Secure Digital Image Watermarking Scheme for Copyright Protection and Buyer Fingerprinting

Bedi S. S. Rabia Bano Shekhar Verma

Abstract – **Digital Image Watermarking is a technique for inserting information into an image that can be later extracted for a variety of purpose including identification, ownership authentication, and copyright protections. The goal of this paper is to design a secure watermarking scheme in spatial domain to identify the true buyer and to protect the ownership copyright of digital still images. The scheme inserts a binary watermark in an original image that serves as a fingerprint for a specific buyer. Utilizing the one-way property of the hash function, it generates the unique buyer fingerprint. An image index concept has been used to split the image randomly into disjoint blocks. A threshold is defined for manipulation of pixel intensities of these blocks. The amount of manipulation in pixel intensities absolutely depends upon the buyer fingerprint. The recovery of the watermark not only identifies the buyer but also protects the owner's copyright. The extracted buyer fingerprint identifies the buyer of the original image. The scheme has the ability to trace the buyer involved in forgery. The experimental results show that the watermark can be retrieved from the attacked watermarked image even if the opponent has the complete information of watermarking scheme.**

Index Terms **– Buyer fingerprint, Cryptographic hash function, Digital Watermarking, Image key.**

I. Introduction

INFORMATION security aspects come into role when it is necessary or desirable to protect information as it is being shared during transmission or storage from an immediate future opponent who may present a threat to confidentiality, authenticity, integrity, access control, and availability. The need for information security has been termed as security attack, mechanism, and services [1]. The various data hiding techniques like cryptography, stegnography, digital signatures, finger printing, have been developed to address the information security issues but fail to provide the complete solutions to protect the intellectual property rights of digital multimedia data. The existing basket of technologies like cryptography secures the multimedia data only during storage or transmission and not while it is being consumed [2]. Digital Watermarking provides an answer to this limitation as the watermark continues to be in the data throughout its usage.

Bedi S. S. is with the Institute of Engineering and Technology, MJP Rohilkhand University, Bareilly (U.P.), INDIA (email: erbedi @yahoo.com).
Rabia Bano is with Deartment of C. S. and I.T., MJP Rohilkhand University, Bareilly (U.P.), INDIA (email: rabia.04cs34@gmail.com).
S. Verma is associated with Indian Institute of Information Technology, Allahabad (U.P.), INDIA (email: sverma@iiita.ac.in).

Digital Watermarking (DWM) is the process of embedding information into digital multimedia contents such that the embedded information (watermark) can be extracted later [3]. The extracted information can be used for the protection of intellectual property rights i.e. for establishing ownership right, ensuring authorized access and content authentication. The watermarking system can be implemented using either of two general approaches. One approach is to transform the original image into its frequency domain representation and embed the watermark data therein. The second is to directly treat the spatial domain data of the host image to embed the watermark.

According to Hartung [4] most proposed watermark method utilize the spatial domain, this may be due to simplicity and efficiency. The spatial domain method is about embedding watermark information directly into image pixels proposed by [5]. These techniques embed the watermark in the LSB plane for perceptual transparency which is relatively easy to implement but their significant disadvantages includes the ease of bypassing the security they provide [5], [6] and the inability to lossy compression the image without damaging the watermark.

The methods [6], [7] extended the work to improve robustness and localization in their technique, in which watermark is embedded by adding a bipolar M-Sequence in the spatial domain and detection is via a modified correlation detector. But these schemes were not very much capable to protect the watermark and also not resist with lossy compression.

Regarding security and content authentication a new method [8] introduce the concept of hash function, in which author insert the binary watermark into the LSB of original image using one-way hash function. The technique is too sensitive since the watermark is embedded into the LSB plane of the image and algorithm also does not very resist with lossy compression. Thus the limitations of spatial domain methods are that, in general they are not robust to common geometric distortion and have a low resistance to JPEG lossy compression. Therefore a scheme is required to fulfill the existing gap in the use of watermarking and cryptographic techniques together.

In this paper, the robust and secure digital invisible watermarking scheme in spatial domain is proposed. The proposed scheme combines the advantages of cryptographic concept and imperceptibility feature of digital image watermarking. The security and perceptual transparency are achieved by using cryptographic one-way hash function and

computation of threshold value respectively. For the robustness the proposed technique does not depend upon perceptually significant regions; rather it utilizes the concept of image key and buyer fingerprint generator. The unique binary sequence serves as the buyer authenticator of a particular image. The recovery of watermark also protects the copyrights.

The rest of the paper is organized as follows. Section II describes the concept of generation of image key and buyer fingerprint. Section III explains the proposed watermarking scheme with watermark insertion and extraction process. Experimental results with discussion and conclusion are given in section-IV and section-V respectively.

II. IMAGE KEY AND BUYER FINGERPRINT

The image key and generation of buyer fingerprint used in proposed scheme are described as below.

A. Image Key

An Image key, I for any grayscale image, I_m of size $X \times Y$ pixels (let, $X = 2^x$ and $Y = 2^y$) is of the same size as of image. The original image is spatially divided into $z = 2^n (= 2^x = 2^y)$ disjoint blocks. Each block is denoted by an index k, for $1 \leq k \leq 2^n$ and for every block $B(k)$, $B_i(k) \cap B_j(k) = \varnothing$ for $1 \leq k \leq 2^n$, $i \neq j$. The length of blocks which contains different number of locations may vary from each other. Each location for two-dimensional image key, I is represented as (i,j), where i corresponds to row for $1 \leq i \leq 2^n$ and j corresponds to column for $1 \leq j \leq 2^n$. The image key, I store the index numbers of image pixels. As the indexes are random, so it is not possible for attacker to guess the image key. The pixel value of blocks in the image is modified corresponding to the indexes of the image key. Now even if the attacker knows the factor by which manipulation is done, he/she will not be able to locate the pixels whose values are modified. The image key is stored with the owner of the image and is used during the extraction of the watermark.

B. Buyer Fingerprint

The Buyer fingerprint, F is a binary sequence of length 2^n and will be equal to the number of blocks. Each location of buyer fingerprint is denoted by index, k for $1 \leq k \leq 2^n$. The unique buyer fingerprint, F is generated using cryptographic hash function. A cryptographic hash function $H(S) = \{f_1, f_2, \ldots, f_p\}$ where S is string of data of arbitrary length, f_i is binary output bits of the hash function, and p is a size of the output bit string, has the two important properties [1]. First property it is computationally infeasible to find any input which maps to pre-specified output. Second is computationally infeasible to find any two distinct inputs that map to same output referred as collision-resistant. The generation of Buyer fingerprint is discussed in Section III.

III. PROPOSED TECHNIQUE

A. Basic Idea

In this watermarking scheme, the original image, I_m is divided into blocks based on the image key. The intensity value of pixels in each block is modified depending upon the bit of watermark to get the watermarked image. Only those pixels are modulated whose value is greater than the threshold, $T(k)$ for $1 \leq k \leq 2^n$. The motivation for selecting the threshold is to increase the perceptual transparency as it filters out the pixels having intensity values less than threshold. The threshold is calculated for each block. The arithmetic mean of pixels for each group is calculated separately which is taken as the threshold. In the extraction phase watermarked blocks are compared with the original image block and the buyer fingerprint is generated.

B. Generation of Watermark

The watermark is generated through the creation of unique Buyer fingerprint, F of an original image using one-way hash function. The Buyer fingerprint is created as $F=H(X, Y, I, M)$ where X is an image height, Y is an image width, I is an image key and M is a MSB array of block. The two parameters image key and MSB array of block makes the Buyer fingerprint unique. The MSB of pixels at index, k are summed together to form the k_{th} element of array M. The image key, I store the index numbers of block of image pixels. As the indexes are generated randomly, so it is not possible for the attacker to guess the image key. The generated Buyer fingerprint is of length 2^n and shall be equal to the number of blocks of original image.

C. Insertion of Watermark

The original image, I_m is spatially divided into $z = 2^n (= 2^x = 2^y)$ blocks. The arithmetic mean of each block is calculated which is taken as threshold for that block. As the length of the generated Buyer fingerprint is equal to the number of blocks of original image. Therefore for each bit of watermark the intensities of the pixels of correspond indexed blocks shall be modified. This modification is based on threshold value of the specific block. If the watermark bit is *'1'*, then the pixels having intensity value greater than threshold are increased by a factor, α. Where as for the watermark bit *'0'*, no modification is recommended. The detailed algorithm of watermark insertion is as given in the following steps:

1) For $1 \leq k \leq 2^n$
   a) Let $T(k)$ be the threshold of the block having index k.
   b) Suppose $F(k)$ is the k_{th} bit of watermark.
2) For $1 \leq i \leq 2^x$, $1 \leq j \leq 2^y$
   a) Let $I_m(i,j)$ be pixel intensity of original image at location (i,j).
   b) Assume that (i,j) belongs to the block $B(k)$.
   c) If $F(k) = 0$, then $W_m(i,j) = I_m(i,j)$.
   d) If $F(k) = 1$, then

e) If $I_m(i,j) > T(k)$, then $W_m(i,j) = I_m(i,j) + \alpha$ and $d(k) = d(k) + \alpha$.

The factor α is taken as positive throughout the insertion. The value of α is chosen so as to maintain the fidelity. The larger values will degrade the quality of the image. From step 2e of algorithm it is clear that the factor $d(k)$ records the increase in the value of intensities for each block.

D. Extraction of watermark

This section illustrates the extraction of watermark form watermarked image, W_m. The extraction procedure requires original image, and image key. The algorithm for the extraction of watermark is as given in the following steps:

1) For $1 \le k \le 2^n$
   a) Set values $s(k) = 0$.
   b) Set bit values $b(k) = 0$.
   c) Let $T'(k)$ be the new threshold of the group having index k.
2) For $1 \le i \le 2^x$, $1 \le j \le 2^y$
   If $| W_m(i,j) - I_m(i,j) | > | \alpha |$, then
   $W_m(i,j) = I_m(i,j) + \alpha$.
3) If (i,j) belongs to the block $B(k)$ and $W_m(i,j) > T'$, then
   $s(k) = s(k) + (W_m(i,j) - I_m(i,j))$.
4) If $\beta s(k) \le d(k)$ and $s(k) \ne 0$, then $b(k) = 1$
   Else $b(k) = 0$
5) The retrieved watermark is $b(k)$.

The value of α is used to reduce the watermarked pixel intensities (may be attacked) to optimum value. As the value of α is known, the limits of pixel values can be determined after watermarking. This fact can be used to rectify the values of attacked pixels. The value of α is utilized for the calculation of the new value of threshold in step 2 of algorithm 2. For the smaller value α there will smaller change in the value of threshold. The difference of watermarked and original pixel is found for every block in step 3 of algorithm 2. The damping factor β (< 1) decreases the value of $s(k)$ in step 4 of algorithm 2 so as to satisfy the inequality. The value of $s(k) = 0$ for unaltered watermarked image. The extracted watermark, b is obtained which is equal to inserted watermark; F as there is exact bit-wise match.

IV. Results and Discussion

The proposed scheme is applied on different grayscale original images of size 128 × 128 pixels. The unique watermark of 128 bits and the unique image key of size 128 × 128 pixels are generated. The threshold is computed for every block and the watermark is inserted in the spatial domain. The different watermarked images of size 128 × 128 pixels are obtained for different buyer fingerprint. The common image processing operations like modification, low pass filter, medium pass filter, cropping, combination of rotation and scaling and compression are imposed on watermarked image. The Normalized Cross Correlation (NCC) values between original image and the attacked watermarked image is computed to demonstrate the robustness and fidelity of the proposed scheme.

The simulation results have been produced on various sets of images. The original gray-scale image of "Lena" of size 128 × 128 pixels is taken as shown in fig. 1(a). Unique image key of size 128 × 128, and MSB array of 128 bits are taken as input to MD5 hash function. The 128-bit string buyer fingerprint is generated and inserted in original image which produced the watermarked image of size 128 × 128 as shown in fig. 1(b). The result shows that the watermark is invisible. The NCC value between the original image and the watermarked image is 0.99998. However the watermark is extracted from watermarked image. The exact bit-wise match between extracted watermark and the inserted buyer fingerprint identifies the true buyer of the original image.

The effect of some attacks on the watermarked image is also shown in Table I and fig.1. Table II shows the bit-wise match of inserted buyer fingerprint and extracted buyer fingerprint.

In the low pass filter attack, a mask of 3 × 3 is used. The NCC value of 0.96294 is obtained between the original and the modified watermarked image whereas it is 0.98461 for median-pass filter attack. The modified watermarked image is shown in fig. 1(c). An exact match of 128 bits is obtained for both the filtering operations as illustrated in table II. The watermarked image is scaled to twice of its size as shown in fig. 1(d) and the measured value of NCC is 0.9999. For the combined attack of rotation of 17° followed by resizing to the size of 128 × 128 pixels, the NCC value between original and modified watermarked image is 0.9878 (fig. 1(e)). The 126-127 bits are recovered for scaling and combined attack. The cropped and randomly modified images are shown in fig 1(f)-(g). In case of modification, the watermarked image has been tampered at specific locations by changing the pixel values. In case of severe manipulation to pixel intensities, a bit-wise match of 120 to 126 bits is obtained. With the use of damping factor of 0.9, exact 128 bits is obtained for the buyer fingerprint and the value of NCC is 0.68474. In case of cropping the NCC value becomes 0.66389. In a rigorously cropped image 3 to 4 bits of inserted Buyer fingerprint are lost which can be recovered by using a damping factor of 0.9. The robustness against lossy JPEG compression with quality factor 90 is demonstrated in fig 1(h) and the NCC value 0.9843 is obtained with all the 128 bits of Buyer fingerprint are recovered. Therefore results demonstrates that proposed scheme is more robust to geometric attacks and compression, whereas robust to modification and cropping.

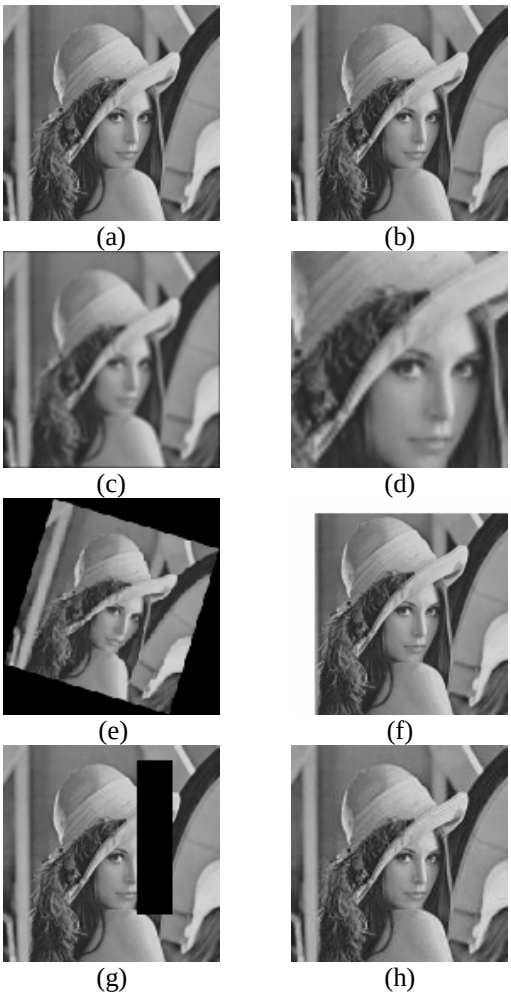

Fig. 1. (a) Original Lena Image; (b) Watermarked Lena Image; (c)-(h) Results of watermarked images with some attacks: (c) Low Pass Filtered (d) Scaled (e) Rotated (17°) (f) Cropped from top and left border (g) random modification (h) JPEG lossy compression (quality factor = 90).

Table I
NCC VALUES OF IMAGES FOR SOME COMMON IMAGE PROCESSING OPERATIONS

Attacks / Images	Scal-ing	Scaling+ Rotation	Compre-ssion	MPF
Lena	0.9999	0.9878	0.9943	0.98461
Cameraman	0.9999	0.9878	0.99523	0.9502

Attacks / Images	LPF	Modify	Cropping
Lena	0.96294	0.68474	0.66389
Cameraman	0.93504	0.71265	0.88474

TABLE II
BIT-WISE MATCH BETWEEN INSERTED AND EXTRACTED BUYER FINGERPRINT (LENA IMAGE)

Attacks / β	Scal-ing	Scaling+ Rotation	Compre-ssion	MPF
1	127	126	128	128
0.9	128	128	128	128

Attacks / β	LPF	Modify	Cropping
1	128	120	123
0.9	128	128	128

V. Conclusion

The proposed watermarking technique is for copyright protection and buyer fingerprinting. The security of algorithm lies in the image key and the unique watermark. The watermark generated is cryptographically secure because it has utilized the property of hash function. The watermark has increased the intensity of an image block when the positive value of α is used. As the attacker knows the watermarking process, he/she may intentionally utilize this fact and try to remove the watermark. For this the attacker must have the knowledge of the image key. But this has been kept secret and since indexes have been generated randomly, so it is not possible for the opponent to guess the secret image key. Now, when the opponent increases or decreases the pixel values, then the step 2 of watermark extraction algorithm rectifies the pixel values. Someone who does not have a valid image key will not be able to forge the watermark. Our proposed technique survives common image transformations as well as intentional attacks, and therefore the objective of buyer fingerprinting and copyright protection has been achieved.

References

[1] William Stallings "Cryptography and Network Security: Principles and Practices," *Pearson Education, Inc.*, 3rd Ed., 2005, ISBN 81-7808-902-5.

[2] S. S. Bedi, and S. Verma, "Digital Watermarking Technology: A Demiurgic Wisecrack Towards Information Security Issues", *Invertis Journal of Science and Technology*, vol. 1, no. 1, pp. 32-42, 2007.

[3] Arun Kejariwal, "Watermarking," Magzine of IEEE Potentials, Oct./Nov., 2003, pp. 37-40.

[4] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques," *Proceedings of IEEE*, vol. 87, no. 7, pp. 1079-1106, July 1999.

[5] M. Yeung, F. Mintzer, "Invisible watermarking for image verification," *Journal of Electric Imaging*, vol. 7, no.3, pp. 578-591, July 1998.

[6] R. Wolfgang and E. Delp, "Fragile watermarking using the VW2D watermark," *Proceedings of the IS & T/SPIE Conference on security and watermarking of multimedia contents*, pp. 204-213, San Jose, California, Jan. 1999.

[7] J. Fridrich, "Image watermarking for temper detection," *Proceedings of the IEEE International Conference on Image Processing*, vol. 2, pp. 404-408, Chicago, Illinois, October 1998.

[8] P. W. Wong and N. Memon, "Secret and Public key Image Watermarking Schemes for Image Authentication and Ownership Verification", IEEE transaction on Image Processing, vol. 10, no. 10, Oct. 2001.