



Methodology Article

Armor on Digital Images Captured Using Photoelectric Technique by Absolute Watermarking Approach

A. Suresh, A. Reyana

Department of Computer Science and Engineering, Nehru Institute of Engineering and Technology, Coimbatore, Tamilnadu, India

Email address:

prisu6esh@gmail.com (A. Suresh), reyareshmy@gmail.com (A. Reyana)

To cite this article:

A. Suresh, A. Reyana. Armor on Digital Images Captured Using Photoelectric Technique by Absolute Watermarking Approach. *American Journal of Science, Engineering and Technology*. Vol. 2, No. 1, 2017, pp. 33-38. doi: 10.11648/j.ajset.20170201.16

Received: December 14, 2016; **Accepted:** January 14, 2017; **Published:** February 13, 2017

Abstract: Nowadays digital image captured through Photoelectric Technique have undergone with malicious modifications. The proposed paper tells on a high quality recovery of digital document using absolute watermarking approach. The recoveries of lost informations are identified using bit values. Whereas the problem on recovering scaled, rotated and translated images exist still. Thus the absolute watermarking approach assures the recovery of digital images from any format of manipulations providing high quality pictures. The different sort of bits used for this purpose is classified into audit bit, carrier bit and output bit. Here the consistent feature of the original image is coded and the output bit is protected using a carrier encoder. This enables the audit bit to detect the erasure locations and retrieve the manipulated areas of the image with high quality pictures in low cost.

Keywords: Carrier Encoding, Tamper Proofing, SIFT, Predictive Coding, Spoofing Detection, Compression

1. Introduction

The recent digital culture provides many new opportunities for the rapid and inexpensive distribution of digital content. Various kinds of information can be encoded into digital form, duplicated without loss of fidelity and transmitted to incredible numbers of recipients over worldwide at negligible cost. While offering interesting opportunities, this evolution also poses serious challenges like protecting the authenticity and integrity of the digital image. Digital watermarking is a method to make data set, such image, sound or video. A stego data set consist of the original data, the cover data set and a digital watermark that does not affect the data set's usability but that can be detected using dedicated software or system. Watermarking can be used for marking authorship or ownership of a data set [2]. The paper focuses on the recovery of an image from any means of modifications or manipulations by considering the wavelength coefficient of the original image. There are certain limitations, which includes the detection of slight changes in gray level based on the viewers position. Of all the methods that have been proposed to protect the intellectual property rights of digital images, digital watermarking schemes are the most commonly used. In digital watermarking schemes, some types of digital

data, such as logos, labels are embedded in the image. Generally existing popular image manipulation techniques provokes the integrity of the digital images. Various techniques are required to guarantee the integrity of the image or to safe-guard it from many intentional malicious manipulations. The examples are in video surveillance applications requires to guarantee the snap shot captured were genuine and are not manipulated anyway in between transmission and reception, or in digital content transmission over peer-to-peer network.

2. Related Works

Some common approaches used to guarantee the integrity of the digital images are the use of hash function, fragile watermarking, semi-fragile watermarking and self embedding techniques. In the use of hash function, along with the original image the hashed one is also transmitted. The receiver checks the original image by hashing the original image and comparing it with the received hashed one. If both are same, the receiver declares the image is unaltered [1]. But the hashed image requires a separate secure channel for transmission, which must be reused for each image transmission. Such a channel might not be available in all the cases. Hence we go

for embedding the verification data into the image itself. Fragile watermarking is the process of marking the image which can detect the modifications by comparing the extracted mark with the original image. A scheme proposed for the authentication of image by watermarking, includes the embedding of simple features in compressed form on the image that can locate the tampered areas. Usually the watermarking has been used to embed author and copyright information to the multimedia content. The watermark will not damage even after the intentional attacks and this preserves the stored information [6].

Some other techniques aim to tampering location detection and error-recovery via single watermark. Depending on the application, the parameter dependency can be considered and adequate performance can be provided as well. The change of quality of watermarked image with tolerable rate happens in flexible watermarking, whereas the constant fidelity watermarks provide stability in parameters [5]. Most recent technique deals the trade-off problems in major parameters of watermarking by certain articulate notions. These include (i) Modeling image representation and reference bit generation as a source coding problem; (ii) Modeling the tampering as an erasure channel while handling it with proper channel coding.

3. Method and Implementation

Like the other systems used, the method uses the algorithm Scale-Invariant Feature Transform (SIFT), that bundles a feature detector and a feature descriptor. The detector extracts from an image a number of attributed regions in a way which is consistent with the viewpoint and the other viewing conditions. The descriptor associates to the regions a signature which identifies their appearance compactly and robustly and is least expensive. Further only few number of bits will be generated on the usage of this algorithm. Predictive encoding is used for the compression of the images. This combines the sequence of identical symbols into single symbol and determines its number of occurrences. RS coding is used for the carrier coding to deal with erasure problem. Audit bits and carrier bits are used for manipulation detection as well as self-recovery of contents. Audit bits are derived from the hash of the MSB bits, which compares with the hash of actual image received. The receiver generates SIFT of the received image and it follows decompression as well carrier decoding. Thus it recovers a high quality image.

The objective of the approach is to recognize the tampered areas of the image and also the reconstruction of the image information in the tampered area. This can be achieved by considering the most significant bits of each pixel as unchanged, and use the remaining bits for the watermarking purpose. This is done by applying Scale Invariant Feature Transform to the original image and then compressing the image using source encoding algorithm, this results in an efficient watermark.

However, there is a chance to lose the content of the image due to manipulations. To overcome this, the Scale Invariant Feature Transform is applied. Compressed image is carrier

coded to exhibit robustness against high level manipulations. To detect tampered blocks at the receiver, audit bits are generated from the parts of the scale invariant feature transformed image which remain unchanged during watermark embedding procedure. These audit bits are included in the total watermark as part of it. As a result, both carrier bits and audit bits of the original image has the least significant bit contained in it. By the usage of audit bits the tampering can be viewed as erasure error. Thus the compressed bit stream is carrier coded using a code that can resist certain level of tampering. At the receiver, the Scale Invariant Feature Transform finds out the received tampered image. The audit bits identify the tampered blocks and in turn, the tampered blocks identifies erasure locations, which helps the RS channel decoder to find the compressed image bit stream despite the occurring erasure. Finally the source coded image will be decoded and the original image is recovered. The steps included here are:

3.1. Watermarking Approach

The gray scale pixel value of the original image is divided into four parts, most significant bit m_b , audit bit m_a , source code bit m_s and carrier bit m_c . The most significant bit remains unchanged throughout the watermarking procedure. The image reproduction and hash value generation is done with the MSB bit. Whereas the other three parameters are used for watermarking procedure. Consider the image pixels being represented as $N_1 \times N_2$. Here N_1 is the number of rows and N_2 is the number columns of the image pixel.

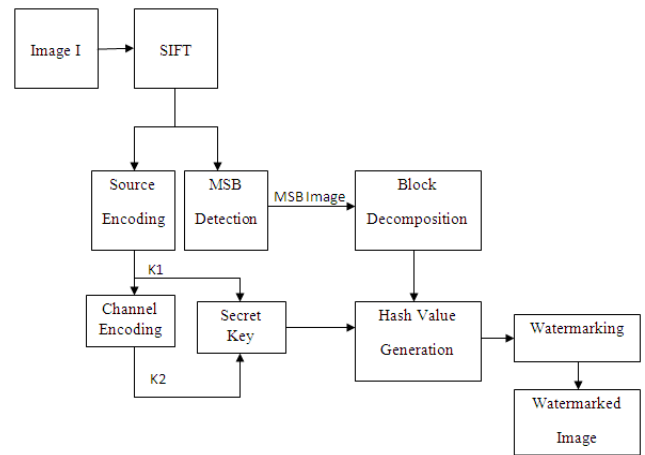


Figure 1. Embedding of Absolute Watermarking.

The original image is compressed and the compressed bit streams are permuted by using secret key K. Reed-Solomon algorithm is an error correcting algorithm, which is used for carrier coding here. The bit streams are permuted before and after the carrier coding and the secret key K is generated. These keys are known to both transmitter and receiver end to ensure the security of the system. The image I which has to be watermarked is divided into block sizes of $M \times M$, so the each image block will host $b_c = m_a \times b_2$ channel code bits. The b_c bits are originally derived from some other blocks. The rows and

indices of these blocks are turned to binary streams, which are called position bits. The derived binary bits and most significant bits used for the hash generation. This will result in $b_h = m_h \times b_2$ hash bits. At the watermark embedding phase, we randomly generate a binary key which is fixed over the whole image. The b_h audit bits are generated by XOR the derived binary key with hash bits. The least significant bits of the actual image are replaced with the check mw stands for indicating the number of bits for watermark embedding.

3.2. Spoofing

The received image might be tampered due to the interference of various types of noises or due to some other intentional manipulations. Trace the local feature coordinates of the received watermarked image, which is decomposed into blocks of size $B \times B$. Here m_w is the watermarked one which contains whole information about the image. The MSB bits

are decomposed to produce MSB bits. Record the extracted audit bits and generated hash bits, and compare them can find out the tampered blocks. The result shows tampering, if the generated and extracted hash bits are different.

3.3. Recovery

After the tampered blocks detected, the carrier coded bits of the whole image are found out and stored from the LSB watermark. Carrier coded bits undergo inverse permutation by using the secret key K_2 . Then these bits and the list of tampered blocks are given as the input to the RS decoder. The compressed image bits streams are obtained at the output of the RS erasure decoder, which is again inverse permuted by the secret key K_2 . Then the compressed image bit stream is source decoded. The reconstructed image is made by replacing the tampered blocks by their corresponding blocks at the output of the source decoder.

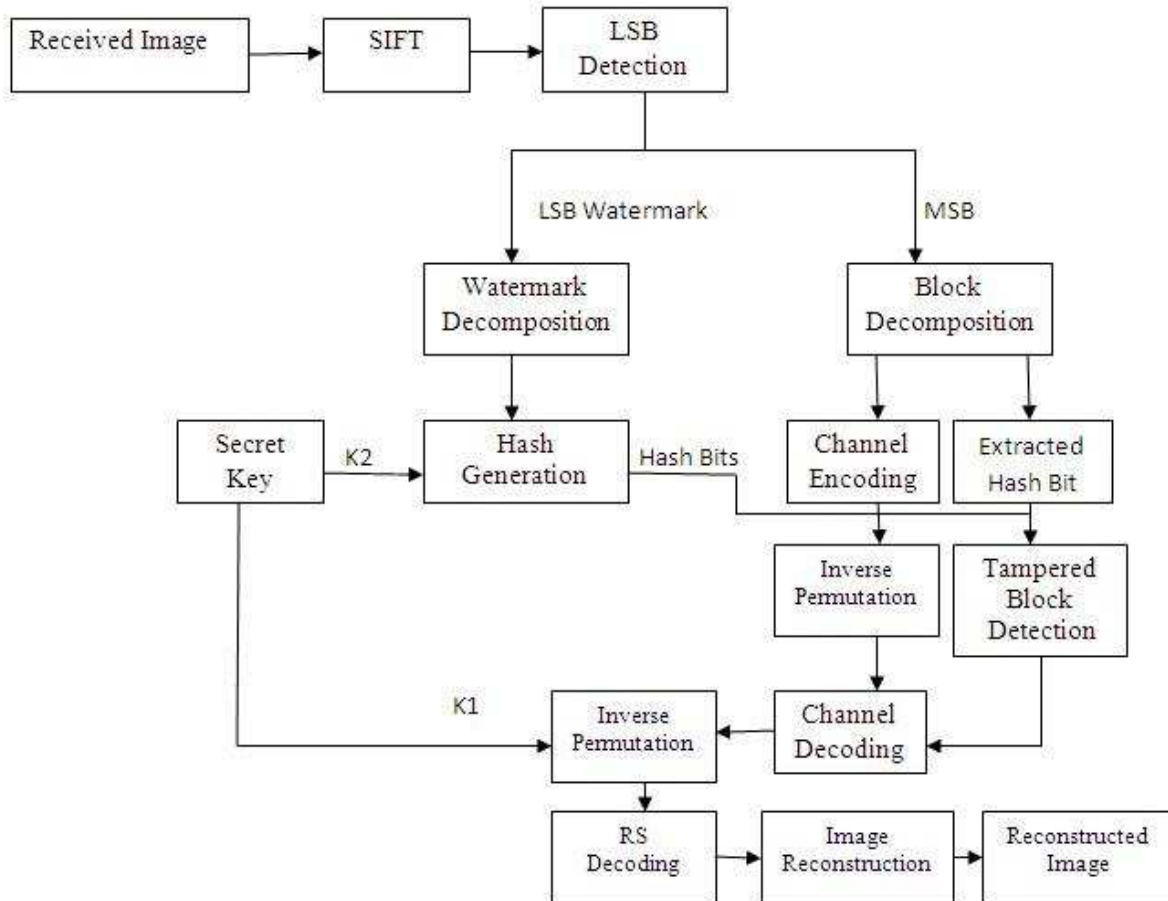


Figure 2. Detection and Recovery of Manipulated Image.

3.4. SIFT - Scale Invariant Feature Transform

SIFT is applied in the proposed method to convert the original image as well the received image into set of local feature coordinates. These feature vectors of the image stands invariant and distinctive to any types of scaling, rotation or translation. These invariant features are also robust across a substantial range of affine distortion, addition of noise, and

change in illumination. The proposed method implement the SIFT as in the following steps 1) Creating the Difference of Gaussian Pyramid; 2) Extrema Detection; 3) Noise Elimination; 4) Orientation Assignment; 5) Descriptor Computation; and 6) Key points Matching. First, take the convolution of the original image I with Gaussian function G_0 of width σ_0 . This would result in blurred image L_0 as the primary image in the Gaussian pyramid. For creating the

i^{th} image in the image pyramid, incrementally convolve L_0 with a Gaussian G_i , of width σ_i . This is equivalent to the original image filtered with Gaussian G_k of width $k\sigma_0$.

Gaussian Pyramid. Each point is compared with all its 26 neighbors of the pixels to get the local maxima and minima of $D(x,y,\sigma)$. If the algorithm finds out that this point is maximum or minimum, then the obtained point is an extreme. By using Taylor series expansion, localization of the key point is improved to sub pixel accuracy. The key point elimination stage attempts to eliminate some points from the list of candidate key points by finding those that have low contrast or poorly localized on an edge. The poorly localized extrema is eliminated by use a large principle curvature across the edge but a small curvature in the perpendicular direction of the Difference in Gaussian functions. Based on local image properties, the orientation step assigns a consistent orientation to the key points. An orientation histogram is formed from this, the peaks of it defines dominant direction of local gradients. The image gradient magnitudes and orientations are sampled around the key point location in the descriptor. Finally, the key points in the transformed image are compared with the key points in the original image and the feature is picked for the comparison.

3.5. Compression

Compressing an image is to avoid redundancies in data. Here, the color value of pixel is estimated by using the color value of neighboring pixels. The first step is the color quantization with some region of the image input. The centroid of the regions can get from the first task. The color value prediction is the next step and it starts from the left to right column and top to bottom row by taking one pixel bit at a time. Then the residual error is calculated for each pixel. The final step is the encoding of errors and the calculation of some parameters such as value and the number of centroid.

3.6. Carrier Coding

The RS codes add redundant parity symbols to the end of a message. When the signal to noise ratio is low, the bits could get flipped during transmission. The use of redundant parity bits (p) can recover the original message up to certain point. The value of p is chosen to be 2 when applied to a digital system, so its values can be expressed in a binary representation. The symbol size is m bits where m is an integer and at least 2. RS codes are denoted as RS (m, k) where k is the number of symbols that is encoded and m is the total number of symbols in the encoded block.

4. Experimental Results

An image of size 256×256 is watermarked using the proposed method. The original image is shown in Figure. 3 and the Figure. 4 shows SIFT transformed version of the original image. The local coordinate feature is specified in red color. Figure. 5 show the watermarked image by the proposed algorithm. The SIFT algorithm reduces the number of bits

available for watermarking. Only the least significant bit of the SIFT transformed image is used for watermarking. The PSNR of the watermarked image is improved by PE compression algorithm. The quality of the real image is preserved without any noticeable distortion. Hence, in the transparency point of view, this method outperforms the existing method. The PSNR values are constant and independent on the selected host image. The self-recovery performance of the proposed algorithm is investigated by applying variety of tampering in high rate and low rate. Here the original and watermarked images are same as in Figure. 3 and 4. Tampering of the watermarked image and the original reconstructed images are shown in Figure. 6 and 7 respectively.



Figure 3. Original Image.



Figure 4. SIFT Image.



Figure 5. Watermarked Image.



Figure 6. Tampered Image.



Figure 7. Reconstructed Image.

5. Conclusion

The proposed method introduces a new watermarking scheme to protect images against tampering as well as used for the self-recovery of tampered images. The watermark bit-budget falls into three parts, audit bits, source encoder output bits, and channel encoder parity bits. The original image is source coded using PE compression algorithm after scale invariant transformation. The output bit stream of source encoder is channel coded using Reed-Solomon code of a required rate and over appropriate field. Since image tampering affects a burst of bits, the RS codes over large Galva fields are good choices. Audit bits help the receiver to detect the tampered blocks. In this way tampering can be modeled as an erasure error because of the receiver knows the exact location of tampering. The use of SIFT to locate feature coordinates is the major suggestion of this paper that reduce the bit-budget for the watermarking as well as efficient error-recovery. The combination of Predictive encoding scheme along with modified SPIHT for the compression of the image can result in better PSNR and efficiency. The proposed system suggests an efficient method for finding tampered areas of an image and also recovers the lost information. This method can be applied to the field of image forensics. And also can be extent to Security purposes, Copyright protection and Hidden communication. The video tampering detection and retrieval of lost information can also be done with the proposed technique.

References

- [1] Swaminathan, Y. Mao, and M. Wu, "Robust and secure image hashing," IEEE Trans. Information Forensics Security, vol. 1, no. 2, pp. 215–230, Jun. 2006.
- [2] S. Roy and Q. Sun, "Robust hash for detecting and localizing image tampering," in Proc. IEEE Int. Conf. Image Process. (ICIP), vol. 6. Sep./Oct. 2007, pp. VI-117–VI-120.
- [3] M. Tagliasacchi, G. Valenzise, and S. Tubaro, "Hash-based identification of sparse image tampering," IEEE Trans. Image Process., vol. 18, no. 11, pp. 2491–2504, Nov. 2009.
- [4] X. Zhang, Z. Qian, Y. Ren, and G. Feng, "Watermarking with flexible self-recovery quality based on compressive sensing and compositive reconstruction," IEEE Trans. Inf. Forensics Security, vol. 6, no. 4, pp. 1223–1232, Dec. 2011.
- [5] M. Wu and B. Liu, "Watermarking for image authentication," in Proc. Int. Conf. Image Process. (ICIP), vol. 2. 1998, pp. 437–441.
- [6] J. Fridrich, "Image watermarking for tamper detection," in Proc. Int. Conf. Image Process. (ICIP), vol. 2. Oct. 1998, pp. 404–408.
- [7] I. J. Cox, J. Killian, T. Leighton, and T. Shamoan, "Secure spread spectrum watermarking for multimedia," NEC Res. Inst., Princeton, NJ, Tech. Rep. 95-10, 1995.
- [8] K. C. Liu, "Colour image watermarking for tamper proofing and pattern based recovery," IET Image Process., vol. 6, no. 5, pp. 445–454, Jul. 2012.

- [9] J. J. K. O Ruanaidh, W. J. Dowling, and F. M. Boland, "Watermarking digital images for copyright protection," in *IEE Proc. Vision, Image and Signal Processing*, Aug. 1996, vol. 143, pp. 250–256.
- [10] J. F. Delaigle, C. De Vleeschouwer, and B. Macq, "Digital watermarking," in *Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques*, Feb. 1996, vol. 2659, pp. 99–110.
- [11] E. Koch and J. Zhao, "Toward robust and hidden image copyright labeling," in *Proc. Workshop on Nonlinear Signal and Image Processing*, I. Pitas, Ed., June 1995, pp. 452–455.
- [12] X. B. Kang and S. M. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in *Proc. Int. Conf. Comput. Sci. Software Engg.* vol. 3. Dec. 2008, pp. 926–930.
- [13] G. Voyatzis and I. Pitas, "Applications of toral automorphisms in image watermarking," in *Proc. IEEE Int. Conf. Image Processing*, 1996, vol. 2, pp. 237–240.
- [14] D. Kundur and D. Hatzinakos, "A robust digital image watermarking method using wavelet-based fusion," in *Proc. IEEE Int. Conf. Image Processing*, 1997, vol. 1, pp. 544–547.
- [15] D. Zou, Y. Q. Shi, Z. Ni, and W. Su, "A semi-fragile lossless digital watermarking scheme based on integer wavelet transform," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 10, pp. 1294–1300, Oct. 2006.
- [16] A. Swaminathan, M. Wu, and K. J. R. Liu, "Digital image forensics via intrinsic fingerprints," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 101–117, Mar. 2008.
- [17] C. B. Adsumilli, M. C. Q. Farias, S. K. Mitra, and M. Carli, "A robust error concealment technique using data hiding for image and video transmission over lossy channels," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 15, no. 11, pp. 1394–1406, Nov. 2005.
- [18] M. Chen, Y. Zheng, and M. Wu, "Classification-based spatial error concealment for visual communications," *EURASIP J. Appl. Signal Process*, vol. 2006, pp. 1–17, Jan. 2006, Art. ID 13438.
- [19] G. Gur, Y. Altug, E. Anarim, and F. Alagoz, "Image error concealment using watermarking with sub bands for wireless channels," *IEEE Commun. Lett.*, vol. 11, no. 2, pp. 179–181, Feb. 2007.
- [20] A. Yilmaz and A. A. Alatan, "Error detection and concealment for video transmission using information hiding," *Signal Process, Image Commun.*, vol. 23, no. 4, pp. 298–312, 2008.
- [21] J. Fridrich and M. Goljan, "Images with self-correcting capabilities," in *Proc. Int. Conf. Image Process. (ICIP)*, vol. 3. 1999, pp. 792–796.
- [22] M. Wu and B. Liu, "Data hiding in binary image for authentication and annotation," *IEEE Trans. Multimedia*, vol. 6, no. 4, pp. 528–538, Aug. 2004.
- [23] X. Zhang, S. Wang, Z. Qian, and G. Feng, "Reversible fragile watermarking for locating tampered blocks in JPEG images," *Signal Process.*, vol. 90, no. 12, pp. 3026–3036, 2010.
- [24] X. Zhu, A. T. Ho, and P. Marziliano, "A new semi fragile image watermarking with robust tampering restoration using irregular sampling," *Signal Process., Image Commun.*, vol. 22, no. 5, pp. 515–528, 2007.
- [25] X. Zhang and S. Wang, "Fragile watermarking with error-free restoration capability," *IEEE Trans. Multimedia*, vol. 10, no. 8, pp. 1490–1499, Dec. 2008.
- [26] Lowe, D. G. 2001. Local feature view clustering for 3D object recognition. *IEEE Conference on Computer Vision and Pattern Recognition*, Kauai, Hawaii, pp. 682–688.