International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Enhancing the Protection of Digital Images against Tampering Using Joint Source Channel Coding

Sreeja M.S.[1], Ann Nita Netto[2]

[1]M .Tech student, Sree Buddha College of Engineering for Women, Elavumthitta, Kerala, India

[2]Assistant Professor, Department of Electronics and Communication Engineering, Sree Buddha College of Engineering for Women, Elavumthitta, Kerala, India

Abstract: ***With the rapid development of multimedia products, digital images can be modified easily. This questions the integrity of images. To provide the integrity and authenticity to images, digital watermarking can be effectively used. In addressing the problem of image tampering these algorithms must be enough to accommodate two functionalities such as tampering detection and error concealment. Both these functions can be achieved by using check bits and reference bits as watermark data. Check bits carry information for the tampering detection, whereas reference bits carry information about the whole image which can be used for recovering the lost information. Check bits are MD5 hash output which can detect the tampering that also results in tampering localization. The generation of reference bits can be done by analog joint source channel coding of the image. Analog joint source channel coding directly maps analog image symbols to channel symbols without requiring source coding followed by channel coding. This reduces the computational complexities. This paper presents a novel and effective method for tampering detection and image self recovery.***

Keywords: Joint source channel coding, fragile watermarking, tampering protection, compressed sensing, image self recovery.

1. Introduction

With the ease of editing and perfect reproduction, digital images are subjected to a number of attacks. Thus the protection of ownership, prevention of unauthorized manipulation of digital audio, image, and video materials become important concerns. Digital watermarking has been introduced as a scheme to embed special labels in digital sources, has made considerable progress in providing authentication to these images. A digital watermark can be called "fragile" if it fails to be detectable after some slight modification. Fragile watermarks are commonly used for tamper detection.

The aim of this scheme is to detect those tampered areas of the received image and further to recover the lost information with some amount of quality that can be accepted. In order to ensure the integrity of the images some of the pioneering techniques started to find hash of the image and for tampering detection and transmitted it along with each images that has been transmitted [2]. But it requires a secure channel for the transmission of this hash data. Because of the non availability of such a channel later on studies brought up methods which could effectively hide this hash data within the image itself. This was called watermarking. Fragile watermarks can be used for both authentication of the received image and localization of tampered zone, and recovering the image information in the lost area. Inceptive fragile watermarking techniques aim only to locate the tampered area with limited robustness against image processing modifications [4]. Watermarking algorithms with the purpose of error concealment aim to restore information in the previously detected tampered parts [5]. In [6], discrete cosine transform (DCT) coefficients of the host image are embedded in the least significant bits (LSB) of the original image.

Watermark information namely consists of two parts. Reference bits and check bits. Check bits are used for tampering detection and localization. Reference bits are used to recover lost information due to tampering. Pioneering techniques embed reference bits of one block to another, with a view that even though a block is lost the information can be recovered from the data embedded in the other block. But this scheme fails when both the original block and the one containing its reference data are lost. This condition is called tampering problem. To address this problem there are some other technique where two copies of the reference data are watermarked into image. But when a block and two copies of reference data are received without any lost then the watermark bit budget spent will be in vain. This condition is called watermark waste. To avoid this problem later on techniques evolved where watermarking data is spread throughout the image [7]. Each block contains watermark data. Source channel coding approach for tampering protection is demonstrated in [1]. The image is source coded using SPHIT algorithm and then channel coded using Reed Solomon coding resulting bit stream and hash of input image together is embedded into two LSB of original image as watermark. Having known the locations of error tampering can be considered as an erasure error. In [8] an analog joint source channel coding (AJSCC) technique applied for digital images is described. In contrast to traditional digital systems where zeros and ones are coded and transmitted, analog JSCC takes analog input symbols and generates analog channel symbols without any processing in the digital domain. This paper introduces a novel scheme which combines the concept of AJSCC and fragile watermarking techniques to protect the image against tampering.

2. Tampering Protection Scheme

First the input image is subjected to compressed sensing followed by Analog Joint Source Channel Coding scheme. The resulted encoded data is converted to bit stream which constitute one portion of watermark data. These bits are used as reference bits which can be used for the recovery of lost information in case of tampering. The image is also given to hash algorithm MD5 which calculates the hash data. This bit stream is called check bits which are used for tampering detection. These steps are illustrated in Figure 1.

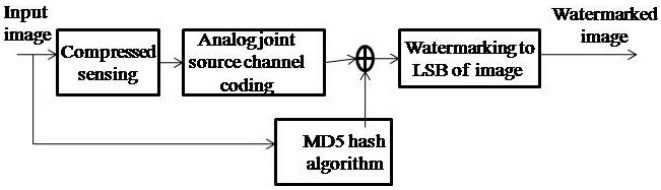

Figure 1: Watermark embedding process

The received watermarked image which is tampered is subjected to watermark extraction. The extracted hash bits are compared with locally generated hash data. This hash data is computed at both transmitter and receiver using only the MSB bits which are not affected by watermarking. The hash check can detect and localize the blocks with tampering. These tampered blocks are then recovered using the reference data that had been watermarked. The other blocks are reproduced as such. These procedures are depicted in figure 2.

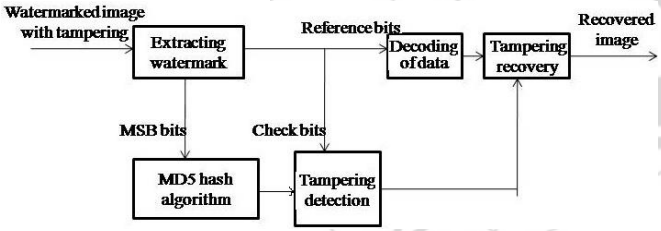

Figure 2: Tampering detection and recovery

3. Watermarking Scheme

3.1 Compressed Sensing

Input image is first subjected to compressed sensing. This is for efficiently acquiring and reconstructing a signal, by finding solutions to underdetermined linear systems. This is based on the principle that, through optimization, the sparsity of a signal can be exploited to recover it from far fewer samples than required by the Shannon-Nyquist sampling theorem. These samples are then subjected to AJSCC.

3.2 Analog Joint Source Channel Coding

According to Shannon "separation principle", optimal communication system can be achieved by cascading optimal source coding and optimal channel coding [9]. But it does not consider the system complexity. Also from Shannon's paper [9], it is clear that approaching optimality requires infinite block lengths, which results in long system delays and high computational complexity. Moreover, if the signal to be sent is analog, quasi-optimal digital systems would require powerful vector quantization and source coding. "Separation principle" does not say anything regarding robustness against change in the channel conditions. In digital systems based on the separation principle, the source encoder first eliminates redundancy in the data, and then the channel encoder adds controlled redundancy in order to protect the data. In JSCC, both procedures are done together.

AJSCC uses the concept of "Shannon Mappings". It uses space filling curves to fill an n-dimensional space with a one dimensional curve to create a mapping of $R^N \rightarrow R$ or $R \rightarrow R^N$. By selecting the direction of mapping, one can achieve N : 1 bandwidth compression or 1 : N bandwidth expansion. It is known that for i.i.d zero mean Gaussian sources 2:1 mappings using the Archimedes' spiral can achieve quasi-optimal performance [10]. The Archimedes' Spiral (single arm for $\theta > 0$) can be described by the following parametric form:

$$\begin{cases} x_1 = \dfrac{\Delta}{\pi}\theta \sin\theta \\ x_2 = \dfrac{\Delta}{\pi}\theta \cos\theta \end{cases} \quad for \theta \rangle 0 \qquad (1)$$

The two source symbols (x_1, x_2) are mapped onto the closest point on the Archimedes' Spiral thereby generating the corresponding channel symbol represented by the angle θ.

3.3 Watermarking

The goal of this algorithm is to embed a watermark into original image to protect it against tampering. Watermark must be capable of finding the tampered areas of the received image and also recovering the lost content in those zones. Keep n_m most significant bits of each pixel unchanged, and use the remaining n_w bits for the watermark embedding. First the input image is resized to 512 x 512. Each pixel is represented by 8 bits. Further the image is divided into blocks. Then its MSB is separated and given to MD5 hash algorithm which generates check bits. The entire image is then subjected to compressed sensing and AJSCC. This result is converted to binary data which constitute the reference bits. The check bits and reference bits are replaced to two LSBs of the image.

4. Tampering Detection and Recovery

Tampering detection can be performed by using reference bits. After receiving the watermarked image possibly containing tampering is subjected to watermark extraction and MSB decomposition. The watermark data extracted contains both reference and check bits. The check bits or hash data is used for tampering detection. The extracted MSB is subjected to hash algorithm and the generated hash and received hash are cross checked. This can detect the tampering and localize the tampered locations. Then reference bits are recovered and subjected to inverse operations of mapping and compressed sensing. This produces estimate of pixel values which can recover lost information. Performance of this scheme can be evaluated by

using Mean Square Error (MSE), the average energy of distortion imposed by watermarking.

$$MSE(n_w) = \frac{1}{2^{n_w}} \sum_{i=0}^{2^{n_w}-1} \sum_{j=0}^{2^{n_w}-1} (i-j)^2 = \frac{4^{n_w}-1}{6} \quad (2)$$

The average peak signal to noise ratio (PSNR) is calculated as:

$$PSNR(n_w) = 10 \log_{10} \left(\frac{255^2}{MSE(n_w)} \right) \quad (3)$$

where n_w is the number of watermarking bits. Since this scheme uses only two bits for watermarking the resulting PSNR is 44.14.

5. Simulation Results

MATLAB R2013a is used as a simulation platform.

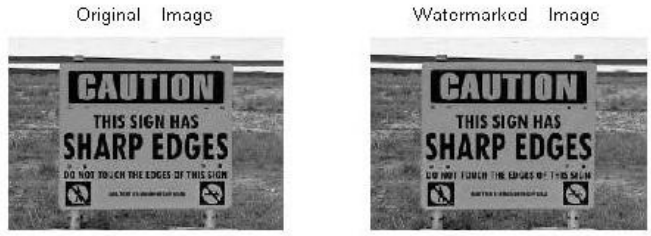

Figure 3: Watermark embedding

Figure 4: Tampering detection

Figure 5: Tampering recovery

6. Conclusion

Fragile watermarking techniques can be effectively used to detect tamper and recover the lost information. Check bits are generated by using MD5 hash algorithm. This helps for tampering detection. Analog joint source channel coding can be used to generate reference bit stream which helps for recovering the lost information. Use of AJSCC reduces the computational complexity. By embedding watermark data into the LSB of image data the PSNR of the watermarked image can be improved.

7. Acknowledgment

I would like to express profound gratitude to our Head of the Department, Prof. Cherian Schariah, for his encouragement and for providing all facilities for my work. I express my highest regard and sincere thanks to my guide, Asst. Prof. Ms. Ann Nita Netto, who provided the necessary guidance and serious advice for my work.

References

[1] S. Sarreshtedari, M.A. Akhaee, "A Source-Channel Coding Approach to Digital Image Protection and Self-Recovery," IEEE Trans. on Image Process., vol.24, No.7, pp. 2266-2276, July 2015.
[2] A. Swaminathan, Y. Mao, and M. Wu, "Robust and Secure Image Hashing," IEEE Trans. on Inf. Forensics and Security, Vol 1, Issue 2, pp.215-230, June 2006.
[3] M. Tagliasacchi, G. Valenzise,and S. Tubaro, "Hash Based Identification of Sparse Image Tampering," IEEE Trans. on Image Process., vol.18, No.11, pp. 2491-2504, 2009.
[4] M. Wu and B. Liu, "Watermarking for Image Authentication," Proc. Int. Conf. Image Process., vol.2, pp. 437-441, 1998.
[5] C.B. Adsumilli, M.C.Q. Farias, S.K. Mitra and M. Carlie "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, Nov. 2005, pp. 1394-1406.
[6] J. Fridrich and M. Goljan, "Images With Self-Correcting Capabilities," Proc. Int. Conf. Image Process. (ICIP), vol. 3, pp. 792–796, 1999.
[7] X. Zhang, S. Wang, and G. Feng, "Reference Sharing Mechanism for Watermark Self-Embedding," IEEE Trans. Image Process., vol. 20, no. 2, pp. 485–495, Feb. 2011.
[8] S.M. Romero, M. Hassanin, J.G. Frias and G.R. Arce, "Analog Joint Source Channel Coding for Wireless Optical Communications and Image Transmission," J. of Lightwave Technology, Vol. 32, No. 9, May 2014.
[9] C.E. Shannon, "A mathematical Theory of Comm-unication," Bell Syst. Technol. J., vol. 27, no. 3, pp. 379–423, 1948.
[10] F. Hekland, G. Oien, and T. Ramstad, "Using 2:1 Shannon Mapping for Joint Source-Channel Coding," in Proc. Data Compress. Conf., Mar. 2005. pp. 1–6

Author Profile

Sreeja M.S. received B-Tech degree in Electronics and Communication Engineering from M.G University, Kerala at Sree Buddha college of Engineering for women in 2014. And now she is pursuing her M-Tech degree in Communication Engineering under the same university in Sree Buddha college of Engineering for women.

Ann Nita Netto is working as Assistant Professor in department of Electronics and Communication, Sree Buddha college of Engineering for women, Elavumthitta, Pathanamthitta.