isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 4, Issue: 3,Special Issue: 2 ,Apr,2016 ,ISSN_NO: 2321-3337

Detecting And Recovering The Tampered Digital Image Using The Source Channel Coding Algorithm

D.Suma[1],N.Swathilakshmi[2] ,Mr.S.Prakash[3]

Student, Department of Computer Science and Engineering, Agni College of Technology, India[1, 2].

Assistantt Professor, Department of Computer Science and Engineering, Agni College of Technology, India [3].

ABSTRACT

Source channel coding algorithms have been widely applied to the field of image forensics recently. One of these very forensic applications is the protection of images against tampering. For this purpose, we need to design a Source channel coding algorithm fulfilling two purposes in case of image tampering: 1) detecting the tampered area of the received image and 2) recovering the lost information in the tampered zones. State-of-the-art techniques accomplish these tasks using watermarks consisting of check bits and reference bits. Check bits are used for tampering detection, whereas reference bits carry information about the whole image. The problem of recovering the lost reference bits still stands. This paper is aimed at showing that having the tampering location known, image tampering can be modeled and dealt with as an erasure error. Therefore, an appropriate design of channel code can protect the reference bits against tampering. In the present proposed method, the total bit is dedicated to three groups: 1) source encoder output bits; 2) channel code parity bits; and 3) check bits. In embedding phase, the original image is source coded and the output bit stream is protected using appropriate channel encoder. For image recovery, erasure locations detected by check bits help channel erasure decoder to retrieve the original source encoded image. Experimental results show that our proposed scheme significantly outperforms recent techniques in terms of image quality for both detected and recovered image. The image quality gain is achieved through spending less bit while image recovery *quality is considerably improved as a consequence of consistent performance of designed source and channel codes.*

keywords- **Tampering, Imageprotection, Selfrecovery, Detection, DWT algorithm, WaterMakering**

1. INTRODUCTION

Image processing is a method to convert an image into digital form and perform some operations on it, in order to get an enhanced image or to extract some useful information from it. It is a type of signal dispensation in which input is image, like video frame or photograph and output may be image or characteristics associated with that image. Usually Image Processing system includes treating images as two dimensional signals while applying already set signal processing methods to them.

2. EXISTING SYSTEM

- The existing method both authentication of the received image and localization of tampered zone in case of malicious modifications (tampering localization), and recovering the image information in the lost area (error concealment).
- Watermarking techniques aim only to verify the integrity of image or locate the tampered area with limited robustness against image processing modifications.
- Another class of watermarking techniques takes one step further and aims to accomplish both tasks of tampering localization and error concealment via a single watermark.
- Watermark bits in self-recovery method.
- After receiving the image, the receiver wants query to sender. In query receiver asked to send image again, after receiving that image, receiver check one by one bit to another image like that compare these images.

3 PROPOSED SYSTEM

- In our project we develop a scheme to detecting the tampered area of the received image and recovering the lost information in the tampered zones.

- Check bits are used for tampering detection, whereas reference bits carry information about the whole image. Image tampering can be modeled and dealt with as an erasure error.
- In watermark embedding phase, the original image is source coded and the output bit stream is protected using appropriate channel encoder.
- For image recovery, erasure locations detected by check bits help channel erasure decoder to retrieve the original source encoded image**.**

4 SYSTEM IMPLEMENTATION

4.1 Image Compression

In the initial step the image will be uploaded. To design a image to 8-bit form the DWT algorithm will be used .This is a type of wavelet transform. The wavelet transform and set partitioning in hierarchical transforms (DWT) source encoding method [49] to efficiently compress the original image. Therefore, the watermark consists of three parts in our algorithm: source code bits, channel code parity bits and check bits. Source code bits which act as the reference bits are the bit stream of the DWT -compressed original image at a desired rate. In order to survive tampering erasure, the reference bits are channel coded to produce channel code bits. Check bits are used at the receiver to determine the erasure location for the channel erasure decoder. The output of channel decoder is source decoded to find the compressed version of the original image. This work shows that by choosing appropriate parameters for source and channel encoding, our algorithm outperforms existing methods in the same watermark payload of three bits per pixel (bpp).

4.2 Permutation

Image is converted into grayscale image. Permutation means interchange the value of x and y axis. The images is to be changed then bit value is to be inserted into reference bits and then secret key is converted into hash code, those values are stored in reference bits. Channel coding algorithm is to be used to add the reference bits values. Channel decoder having information about this reference bits. The source channel code design and having error locations is to be noted. Repermutation the image then it sends to receiver.

4.3 Tampering

Sender sends the image to receiver. While sending hacker comes intermediately and then hack the image and do some tamper. Then forward the images to receiver. Tampering means some modification in images. Tampering image blocks know the channel decoder algorithm

4.4 Detection and Recovery

Image is to be calculated hash bits and extracted check bits is recorded for each block. For unaltered blocks, this bit stream equals the random key used in the embedding phase. Therefore, comparing these results and spotting the different ones leads to locating the tampered blocks. After locating the tampered blocks, Channel code bits undergo proper inverse permutation. The compressed image bit stream available at the output of the decoder is passed through the source decoder after undergoing proper inverse permutation. The reconstructed image is made by replacing the tampered blocks by their corresponding blocks at the output of the source decoder. Obviously, the content of the received image in preserved blocks will not be replaced with the corresponding information derived from the restored image.

5 ARCHITECTURE DIAGRAM

5. 1 Architecture Diagram

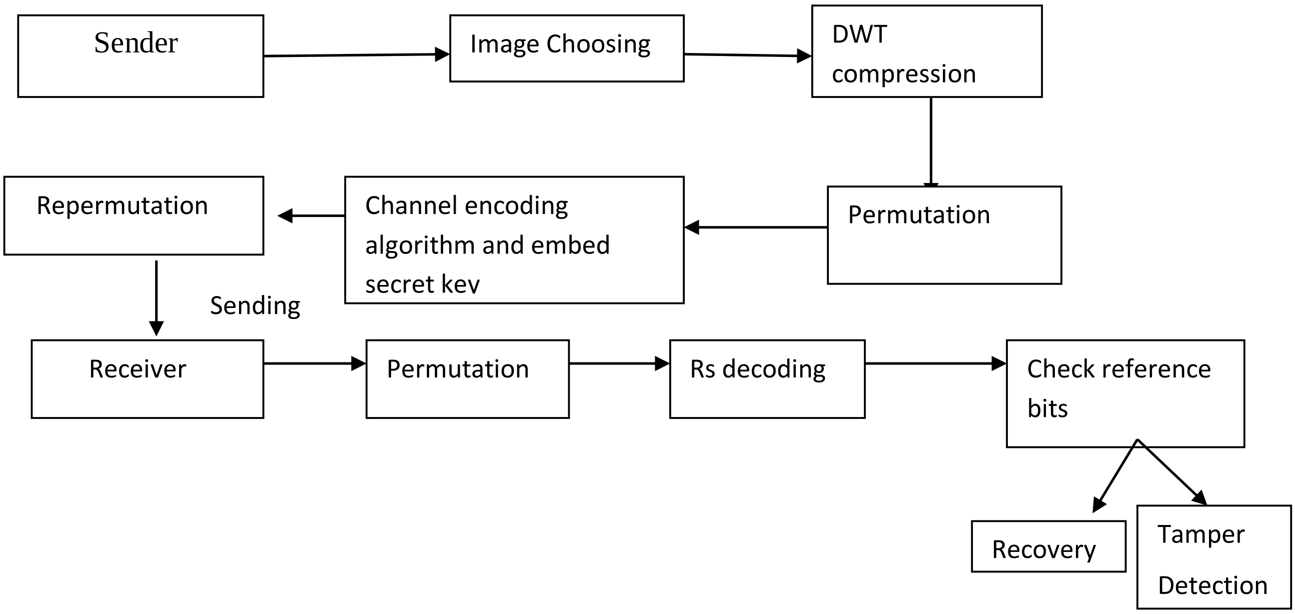

Figure 5.1 System Architecture

6 CONCLUSIONS

In this project, we introduced a watermarking scheme to protect images against tampering. The original image is source coded using Rs encoding algorithm, in this we use reference bits and check bits. Image is tampered by hacker. The RS codes know about the value reference bits. Therefore, the receiver knows the exact location of erroneous bits. So that we can detect the tampered image and recovered the original image.

REFERENCES

[1] A. Swaminathan, Y. Mao, and M. Wu, “Robust and secure image hashing,” IEEE Trans. Inf. 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] M. Wu and B. Liu, “Watermarking for image authentication,” in Proc. Int. Conf. Image Process. (ICIP), vol. 2. 1998, pp. 437–441.

[5] J. Fridrich, “Image watermarking for tamper detection,” in Proc. Int. Conf. Image Process. (ICIP), vol. 2. Oct. 1998, pp. 404–408.

[6] D. Kundur and D. Hatzinakos, “Digital watermarking for telltale tamper proofing and authentication,” Proc. IEEE, vol. 87, no. 7, pp. 1167–1180, Jul. 1999.

[7] C.-S. Lu, S.-K. Huang, C.-J. Sze, and H.-Y. M. Liao, “Cocktail watermarking for digital image protection,” IEEE Trans. Multimedia, vol. 2, no. 4, pp. 209–224, Dec. 2000.

[8] P. W. Wong and N. Memon, “Secret and public key image watermarking schemes for image authentication and ownership verification,” IEEE Trans. Image Process., vol. 10, no. 10, pp. 1593–1601, Oct. 2001.

[9] M. U. Celik, G. Sharma, E. Saber, and A. M. Tekalp, “Hierarchical watermarking for secure image authentication with localization,” IEEE Trans. Image Process., vol. 11, no. 6, pp. 585–595, Jun. 2002.

[10] S. Suthaharan, “Fragile image watermarking using a gradient image for improved localization and security,” Pattern Recognit. Lett., vol. 25, no. 16, pp. 1893–1903, 2004.