Detecting and Recovering the Tamper Image by using Source Coding and Channel Coding Algorithm

R. Karpagaselvi
IV/CSE
Sri Vidya College of Engineering & Technology,
Virudhunagar,

M. Poonkodi
IV/CSE
Sri Vidya College of Engineering & Technology,
Virudhunagar, Email

S. Seedhanadevi
AP/IT
Sri Vidya College of Engineering & Technology,
Virudhunagar,

Abstract :- In this project, it is need to design a watermarking algorithm fulfilling two purposes in case of image tampering: to detect the tampered area of the received image and to recovery the lost information in the tampered zones. Watermark consist of check bits and reference bits.To detect the tampered area by using check bits , whereas carry information about the whole image by using reference bits .Therefore reference bits against tampering can be protected by an appropriate design of channel code . In the proposed method, the watermark bit-budget is totally dedicated into three groups: source encoder output bits , channel code parity bits and check bits. In watermark embedding phase, the original image is source coded and the output bit stream is protected using appropriate channel encoder.This proposed scheme significantly outperforms recent techniques in terms of image quality for both watermarked and recovered image. To detect the tampered area of the received image using channel RS coding algorithm. To recover the lost information in the tampered zones. while image recovery quality is considerably improved as a consequence of consistent performance of designed source and channel codes.

Keywords — Image watermarking, fragile watermarking, image tampering protection, self-recovery, SPIHT, RS channel codes.

I.INTRODUCTION

Digital imaging has been rapidly developing in last two decades, and digital concealment aim to restore information in the previously-detected tampered parts [14]–[17]. 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. This self-recovery

watermarking trend, initiated by [18],localization and error concealment via a single watermark. This self-recovery watermarking trend, initiated by [18],has recently attracted growing interest. The problem of image self-recovery has been approached in numerous ways. In [19],conventional error control coding schemes are adopted for localization and restoration. Several methods embed a wavelet transform [23], a vector quantized [24] or halftone [25] version of the original image. Fragile watermarks may also be designed for specific purposes, such as binary images [26], JPEG compressed

Detecting the tampered area of the received image. Recovering the lost information in the tampered zones. Image tampering protection for self-recovery.

images [27], coloured images [28], [29], compression-resistant [30].Significance of this project is representation of an original image into itself for the sake of self-recovery. In [18], discrete cosine transform (DCT)coefficients or reduced colour-depth version of the host image is embedded in the least significant bits (LSB) of the original image. This representation of the original image can also be the first few DCT coefficients of each block [20], a binary image generated from the difference between the host image and its chaotic pattern [21], the hash of the original image [22], watermark derived from approximation coefficients of its multimedia products are utilized in countless applications nowadays. As a consequence of this expansive development, popular and low-cost access to image editing applications challenges the integrity of digital images. On the other hand, sophisticated techniques are required to guarantee the integrity of an image or protect it against malicious modifications. One common approach is to use the hash of the original image. The receiver declares the image as unaltered if the hash output is the same as the one transmitted from the original image [1]–[3].

Image integrity verification through hash requires a secure channel that must be reused for each image transmission. Since such a channel might be unavailable, a more applicable approach is to embed the verification data into image itself, which is referred to as fragile watermarking. Fragile watermarks can be used for 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). Inceptive fragile watermarking techniques aim only to verify the integrity of image or locate the tampered area with limited robustness against image processing modifications[4]–[9]. More recent methods in the field of tampering detection achieve the perfect 100% localization using watermarks robust against wide variety of attacks [10]– [13].On the other hand, watermarking algorithms with the purpose of error. This paper proceeds as follows. Section II briefly reviews architecture diagram. Section III briefly reviews image compression. Section IV presents permutation. Section V introduces tampering. Section VI presents detection mechanism.

IIARCHITECTURE DIAGRAM

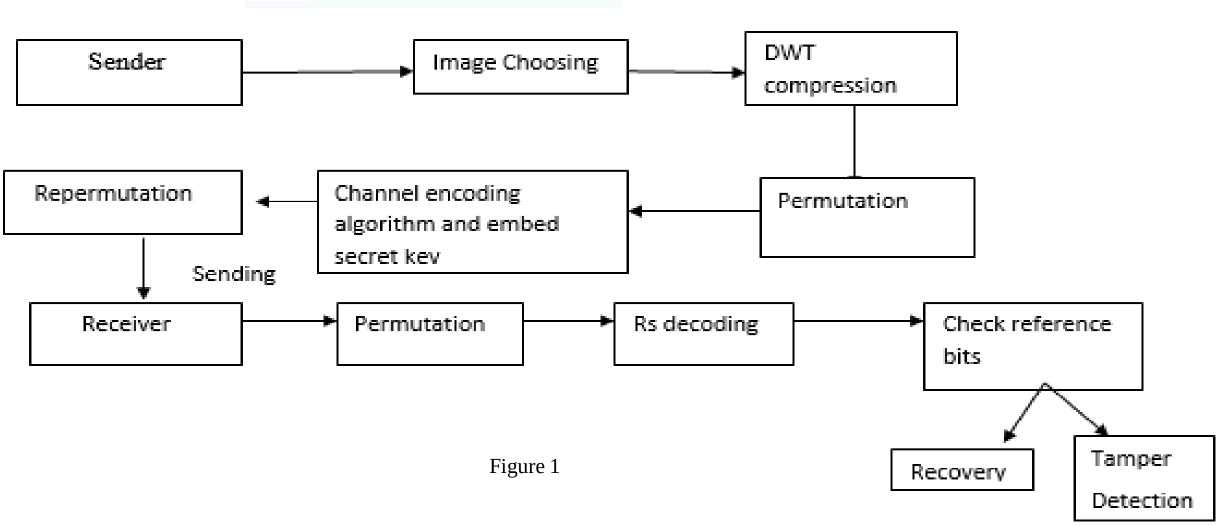


Figure 1

III 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).

IV PERMUTATION

Image is converted into gray scale 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.

V TAMPERING

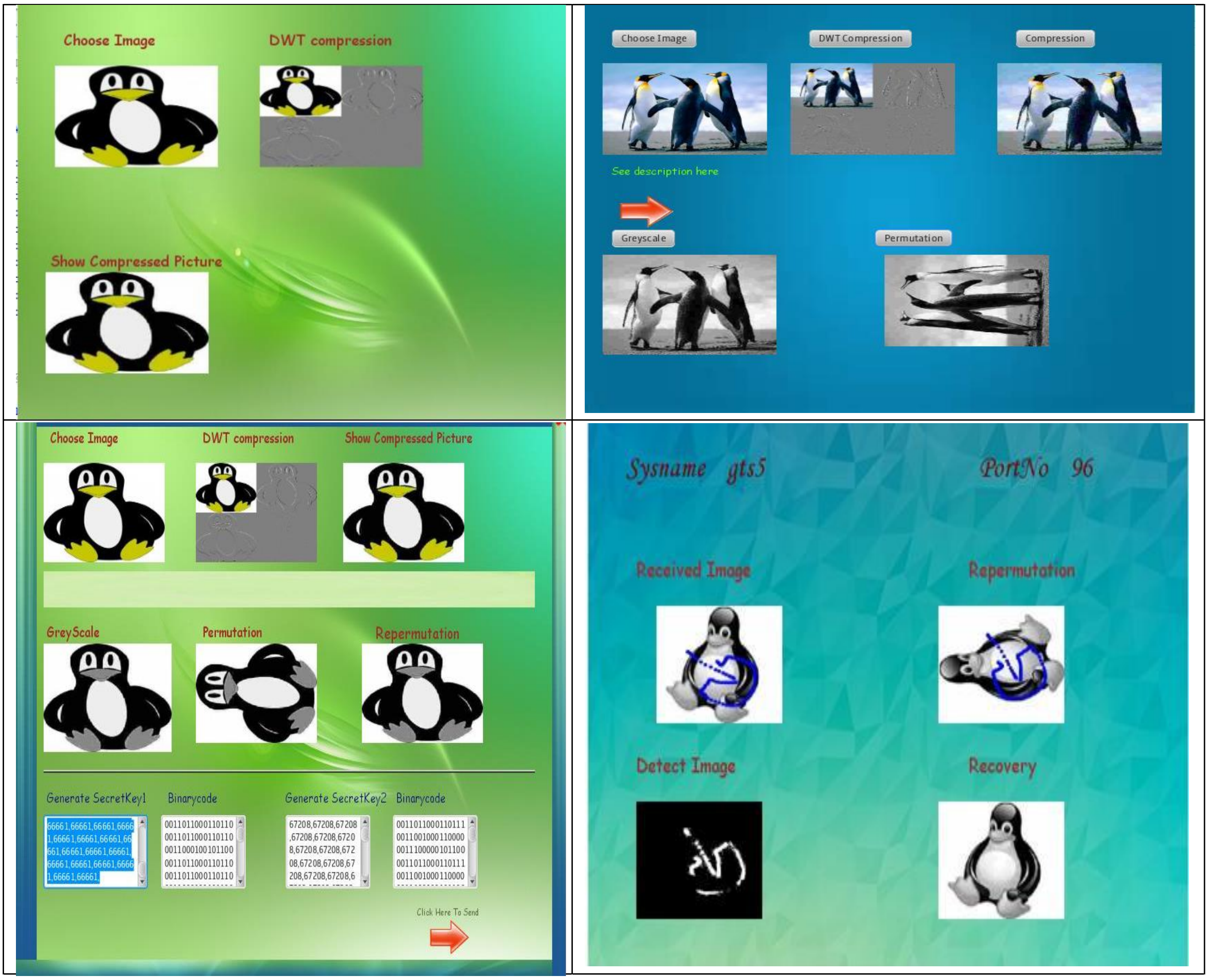
Sender sends the image to receiver. While sending hacker comes intermediately and then hack the image and do some tamper. Then forward the images to receiver. Tampering means some modification in images. Tampering image blocks know the channel decoder algorithm.

VI DETECTION MECHANISM

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.

RESULT AND DISCUSSION:

Figure2 describes Image is chosen from database. DWT Compression is performed- Here encryption and decryption process is completed. The resultant image is shown after encryption and decryption process. Compressed image is converted into gray scale image. Gray scale image is permutated .Gray Scale image contains X direction is converted to Y direction and vice Versa. Permutation process is completed .Secrete keys are generated. Then secrete key is converted into binary code format. Repermutation is completed. Repermutate image is send to receiver. Tampering the image is done by hackers. Tampered image is saved. Receiver get the tampered image . Receiver repermutate the received image. Receiver is done the decoding process. By using RS channel coding algorithm for detecting the tamperedarea of the image and recovery the lost information of the original image.



```
66661,66661,66661,6666
1,66661,66661,66661,66
661,66661,66661,66661,
66661,66661,66661,6666
1,66661,66661,
```

```
0011011000110110
0011011000110110
0011000100101100
0011011000110110
0011011000110110
```

```
67208,67208,67208
,67208,67208,6720
8,67208,67208,672
08,67208,67208,67
208,67208,67208,6
```

```
0011011000110111
0011001000110000
0011100000101100
0011011000110111
0011001000110000
```

Figure2

CONCLUSION:

The project introduce watermarking scheme to protect images against tampering. The original image is source coded using Rs encoding algorithm, in this project reference bits and check bits are used. 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 .Its application is Military application.

REFERENCE:

[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.

[11] 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.

[12] 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.

[13] X. B. Kang and S. M. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in *Proc. Int. Conf. Comput. Sci. Softw. Eng.*, vol. 3. Dec 2008, pp. 926–930.

[14] 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.

[15] 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.

[16] G. Gur, Y. Altug, E. Anarim, and F. Alagoz, "Image error concealment using watermarking with subbands for wireless channels," *IEEE Commun. Lett.*, vol. 11, no. 2, pp. 179–181, Feb. 2007.

[17] A. Yilmaz and A. A. Alatan, "Error detection and concealment for

[28] N. Wang and C.-H. Kim, "Tamper detection and self-recovery algorithm of color image based on robust embedding of dual visual watermarks using DWT-SVD," in *Proc. 9th Int. Symp. Commun. Inf. Technol. (ISCIT)*, Sep. 2009, pp. 157–162.

[29] K.-C. Liu, "Colour image watermarking for tamper proofing and patternbased recovery," *IET Image Process.*, vol. 6, no. 5, pp. 445 454, Jul. 2012.

[30] C.-Y. Lin and S.-F. Chang, "SARI: Self-authentication- and recovery image watermarking system," in *Proc. 9th ACM Int. Conf. Multimedia (MULTIMEDIA)*, 2001, pp. 628–629. video transmission using information hiding," *Signal Process., Image Commun.*, vol. 23, no. 4, pp. 298–312, 2008.

[18] J. Fridrich and M. Goljan, "Images with self-correcting capabilities," in *Proc. Int. Conf. Image Process. (ICIP)*, vol. 3. 1999, pp. 792– 796.

[19] J. Lee and C. S. Won, "Authentication and correction of digital watermarking images," *Electron. Lett.*, vol. 35, no. 11, pp. 886–887, 1999.

[20] H.-J. He, J.-S. Zhang, and F. Chen, "Adjacent-block based statistical detection method for self-embedding watermarking techniques," *Signal Process.*, vol. 89, no. 8, pp. 1557–1566, 2009.

[21] S.-H. Liu, H.-X. Yao, W. Gao, and Y.-L. Liu, "An image Fragile watermark scheme based on chaotic image pattern and pixel-pairs," *Appl. Math. Comput.*, vol. 185, no. 2, pp. 869–882, 2007.

[22] V. Mall, K. Bhatt, S. K. Mitra, and A. K. Roy, "Exposing Structural tampering in digital images," in *Proc. IEEE Int. Conf. Signal Process., Comput. Control (ISPCC)*, Mar. 2012, pp. 1–6.

[23] R. Chamlawi, A. Khan, and I. Usman, "Authentication and recovery of images using multiple watermarks," *Comput. Elect. Eng.*, vol. 36, no. 3, pp. 578–584, 2010.

[24] C.-W. Yang and J.-J. Shen, "Recover the tampered image based on VQ indexing," *Signal Process.*, vol. 90, no. 1, pp. 331–343, 2010.

[25] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "A secure and improved self-embedding algorithm to combat digital document forgery," *Signal Process.*, vol. 89, no. 12, pp. 2324–2332, 2009.

[26] 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.

[27] 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.