State of Art Technique that Accomplishes Digital Image Protection and Self Recovery

Prema C.R1, Megha S2
1Assistant Professor, 2UG Scholar
Dept. of ISE, SKIT, Bengaluru,
meghasrinivas26@gmail.com

Abstract-- Recently watermarking algorithm plays an important role in image forensics. One of the main applications is protect—ion of images against tampering. An algorithm that full-fills two purposes has to be designed that includes: 1) detection of tampered area of received image and 2) information recovery in the tampered zones. These tasks using watermarking are accomplished by state-of-the-art techniques that consist of check bits and reference bits. Check bits are used for tampering detection, while reference bits carry information about the whole image. The problem of recovering the lost reference bits can be modeled and dealt with as an erasure error. The reference bits can be protected against tampering by an appropriate design of channel code. The total watermark bit-budget is dedicated to three groups in the present proposed method: 1) source encoder output bits 2)channel code parity bits and 3)check bits. The original image is source coded and using appropriate channel encoder the output bit stream is protected in the watermark embedding phase. To retrieve the original source encoded image, erasure locations detected by the check bits help in image recovery. The image quality of both the watermarked and recovered image significantly outer-performs recent techniques as shown by the experimental results. By spending less bit-budget less bit-budget the watermarked image quality gain is achieved, where the consequence of consistent performance of designed source and channel codes result in considerably improved quality of recovered image.

Index Terms: Image watermarking, fragile watermarking, self-recovery, SPIHT, RS channel codes.

I INTRODUCTION

Digital multimedia produced are utilized in countless applications and digital imaging has been rapidly developing in last two decades. The integrity of digital images are challenged due to the popular and low cost access to image editing applications. Sophisticated techniques are required to guarantee the integrity of the image and protect it against malicious modifications. Using hash of the original image is a common approach. The image is declared unaltered if the hash output is the same as one transmitted from original image. Each image transmission reuses a secure channel for image integrity verification.

Fragile watermarking can be used for both image authentication and localization of tampered zone and recovering the image information. The integrity and localizing of tampered areas with limited robustness against image processing modifications is aimed by Inceptive fragile watermarking technique. The perfect 100% localization using watermarks robust is obtained by more recent method Watermark bits in self-recovery methods are conventionally fallen into two categories, namely check bits and reference bits. The check bits are used to localize the tampered blocks, while the reference bits are employed to restore the original image in the tampered area. Normally for the sake of content restoration, reference bits of a certain block are always embedded into another one. Nevertheless, in some of these methods content recovery may fail because both the original block and the one containing its reference bits are detected as tampered. This is called **Tampering problem**. To tackle this challenge, recent techniques spread the representation data of one block over entire image. On the other hand, there exists another problem of **watermark waste**, that is, where both original data and its reference bits are available. For instance, suggests a dual watermarking scheme where watermarked image carries two copies of content data for each block, in order to leave a chance of restoration when one copy is lost because of tampering. It should be kept in the mind that when both copies and original data survive the tampering, the watermark budget which could help the restoration of other tampered blocks is wasted. The most recent methods also deal with the watermark waste problem by offering schemes in which the content information is derived from several blocks. In our proposed algorithm, reference bits are the source coded image. This data is derived from and then scattered over the whole image to overcome both tampering and waste problems. The problem of image self-recovery is about finding an appropriate trade-off between these three parameters: the watermarked image quality, content recovery quality, and tolerable tampering rate (TTR). We approach this trade-off in our image self-recovery algorithm using these two key ideas: 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. Erasure modeling of tampering has been recently

offered and exploited in and, where the authors apply fountain codes to deal with it. It should be added that when one block is marked as tampered, all its carrying reference bits are missed. We would suggest Reed-Solomon (RS) codes with large encoding blocks and over large Galva fields to solve the erasure problem. Moreover, we treat the challenge of finding some representation of the original image as a source coding problem. We apply the wavelet transform and set partitioning in hierarchical transforms (SPIHT) source encoding method 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 SPIHT-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). Nevertheless, since the watermark artifacts are significant for embedding in three LSB, we would recommend two-LSB version of our algorithm and show that its performance is still remarkable.

Organization: The paper is organized as follows. Related works is presented in section II. Our implementation modules are in section III, followed by the experimental results in section IV. We conclude at section V.

II RELATED WORK

The proliferation of digital images creates problems for managing large image databases, indexing individual images, and protecting intellectual property. This paper[1] introduces an image hash function that is a novel image indexing technique. The algorithm uses randomized signal processing strategies for a non-reversible compression of images into random binary strings, and is shown to be robust against image changes due to compression, geometric distortions, and other attacks. This algorithm brings to images a direct analog of message authentication codes (MACs) from cryptography, in which a main goal is to make hash values on a set of distinct inputs pairwise independent.

A fragile watermarking algorithm for image authentication and tamper detection is proposed [9]. A gradient image and its structure is used to achieve localization and security requirements. It provides superior localization with greater security against many attacks including vector quantization attack. In this paper [11], we introduce two techniques for self-embedding an image in itself as a means for protecting the image content. The first method is based on transforming small 8×8 blocks using a DCT, quantizing the coefficients, and carefully encoding them in the least significant bits of other, distant squares. This method provides very high quality of reconstruction but it is very fragile. The quality of the reconstructed image areas is roughly equivalent to a 50% quality JPEG compressed original. The second method uses a principle similar to differential encoding to embed a circular shift of the original image with decreased color depth into the original image. The quality of the reconstructed image gradually degrades with increasing amount of noise in the tampered image. In this study [10], an efficient self-embedding watermarking scheme for color image authentication is proposed. The scheme is designed to achieve tamper proofing and high-quality recovery. The former is used to generate authentication information for obtaining better results of tamper proofing and the latter is used to further improve the neighboring connectivity of the proofing results. The simulation results show that the proposed watermarking scheme can effectively proof the tempered region with high detection rate and can restore the tempered region with high quality.

III IMPLEMENTATION

A. Basics

The goal of our algorithm is to embed a watermark into original image to protect it against tampering. It means that the watermark must be capable of both finding the tampered areas of the received image, and recovering the content of the original image in those zones. For the purpose of image recovery, we compress the image using a source encoding algorithm, and embed the result as watermark.

However, some of compressed image information might be lost because of image tampering; hence the compressed image bit stream must be channel coded to exhibit robustness against a certain level of tampering. In order to detect tampered blocks at the receiver, some check bits are generated from those parts of image which remain unchanged during watermark embedding procedure. These check bits are inserted as a part of total watermark. Having tampered blocks known using the check bits, tampering can be modeled as an erasure error. Therefore, compressed bit stream is channel coded using a code capable of resistance against certain level of erasure. At the receiver, the check bits locate tampered blocks. The list of tampered blocks identifies erasure locations and helps the channel erasure decoder to find the compressed image bit stream despite the occurring erasure. Then source encoded image would be decoded and the estimation of the original image is recovered.

B. Watermark Embedding

Consider the original image I represented as 8-bit gray-scale pixel values.

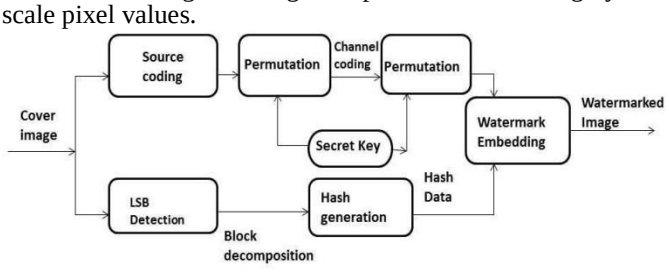

Fig (1). The block diagram of the proposed watermark embedding using two LSB.

These eight bits are divided into four parts: The most significant bits (MSB) that will not change at the watermark embedding phase, check bits, source code bits, and channel code parity bits. MSB bits of each pixel remain unchanged during watermark embedding and will be used later for hash generation and image reconstruction. The remaining bits are used for the purpose of watermark embedding. Block diagram of watermark embedding for 2-LSB algorithm is shown in Fig(1).

C .Tampering Detection and Image Recovery

The received image which is probably tampered is decomposed into blocks of size B × B. For each block, position bits are found, derived from shared secret key. The XOR of 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. The channel decoder at the receiver side is Reed-Solomon (RS) erasure decoder. Channel code bits undergo proper inverse permutation. Then, they are delivered as input to RS erasure decoder along with the erasure locations calculated from the list of tampered blocks.

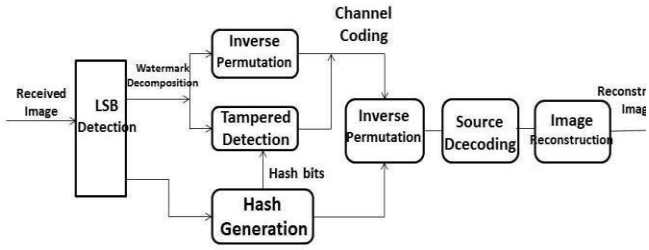

Fig (2). The block diagram of our tampering detection and image recovery scheme using 2 LSB of each pixel.

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. An example of image recovery for 2-LSB algorithm is given in Fig (2).

IV. EXPERIMENTAL RESULTS

8-bit gray scale Cameraman image of size 512 × 512 is watermarked using our proposed method explained in Section VII. The original Cameraman image is shown in Fig. 3(a). Fig. 3(b) shows the watermarked image generated by 2-LSB version of our algorithm. As mentioned, the PSNR of watermarked image generated by 2-LSB version of our algorithm equals 44.15 dB, which is far beyond the HVS threshold of noticeable distortion. State-of-the-art tampering protection algorithms usually use three least significant bits for watermark insertion. This embedding approach degrades the PSNR of watermarked image down to 37.9 dB, which is not suitable for smooth areas. This fact is shown in Fig. 3(c), where the same image is watermarked using Zhang‘s method which replaces three LSB with tampering protection data. Comparing three images in Fig. 4, it is clear that Zhang‘s method has imposed noticeable distortion to the original image, while our watermarked image preserves the quality of the original image.

Therefore, the proposed method outperforms the state-of-the-art techniques from transparency point of view. Note that the values derived for PSNR of watermarked image (37.9 dB and 44.15 dB for those algorithms using two and three LSB for data embedding) are constant and independent of the chosen host image, in spite of the reconstruction PSNR which varies depending on the selected cover image.

Fig (3) (a) Original 8-bit gray scale Cameraman image. (b) Watermarked image generated by 2-LSB watermark artifacts are noticeable in smooth area of sky in this image.

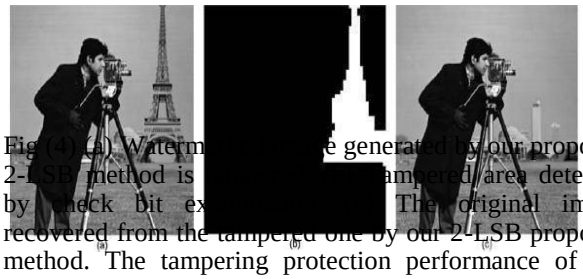

Fig (4) (a) Watermarked image generated by our proposed 2-LSB method is tampered, (b) tampered area detected by check bit extraction. (c) The original image recovered from the tampered one by our 2-LSB proposed method. The tampering protection performance of our algorithm is also investigated in practice. Both ―low-rate‖ and ―high-rate‖ tampering scenarios are applied to Cameraman image. Fig. 4 depicts the result of low-rate tampering protection. In this case, 2-LSB version of our algorithm has been applied. Fig. 4(b) demonstrates the detected tampered areas of image after check bit

examination.

The original image is recovered exploiting the channel coded data located in preserved blocks and the list of tampered blocks as shown in Fig. 4(c). In order to protect the image against high-rate tampering, we need to spend more bit-budget for watermark embedding. Since three LSB are used for watermark data, the watermarked image looks similar to Fig. 3(c). Tampered blocks are recognized and their information is perfectly recovered as illustrated in Figs. 4(b) and 4(c).

As the next step, we compare the general performance of our algorithm with two of the most recent works presented so far. Both of them exploit three LSB for watermark embedding. In this way, regardless of the content of the watermarked image, the maximum PSNR of recovered area is limited to 40.7 dB, as is calculated. The second mode is when the tampering rate exceeds the TTR. In this scenario, the channel code breaks down, source encoder data is not retrievable and the image tampered area will not be recovered.

The results in Fig. 6 confirm the TTR calculated for 2-LSB and 3-LSB versions of the proposed method. In order to have a fair TTR comparison, we must compare the other techniques with 3-LSB version of our algorithm. It is inferred from Fig. 6 that the TTR of our proposed method is higher than that of Koru‘s method. Fig. 6 also confirms that our proposed algorithm dramatically outperforms Zhang‘s method.

The consistent performance of our proposed algorithm compared to the decaying one of Zhang‘s method shows significant gain in image recovery which exceeds 14 dB for high-rate image tampering. Although the notable recovery gain of our 3-LSB algorithm is attractive, since 3-LSB algorithm inherently imposes significant distortion on original images, we recommend our 2-LSB algorithm for practical applications.

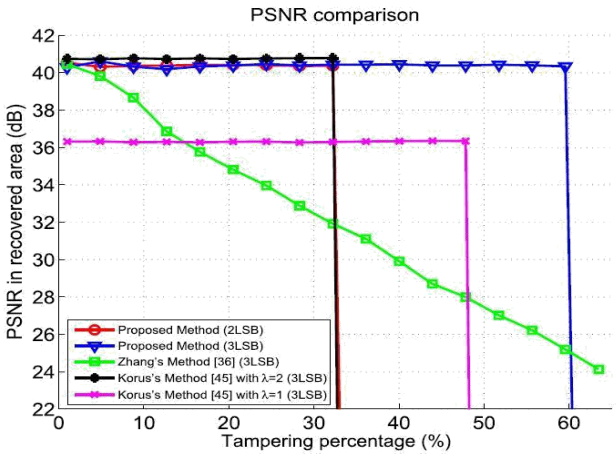

Fig. 6. Simulation results for different methods, expressed as the recovered PSNR in tampered area in terms of tampering rate.

V CONCLUSION

A watermarking scheme to protect images against tampering was introduced in this paper. The watermark bit-budget consists of three parts, check bits, source encoder output bits, and channel encoder parity bits. SPIHT compression algorithm is used for the original image source coding. The source encoder output bit stream is channel coded using RS code of a required rate and over appropriate field. The RS codes over large Galva fields are wise choices since image tampering affects a burst of bits. Check bits support the receiver in locating the tampered blocks. Therefore, the receiver knows the exact location of erroneous bits. In this way tampering is modeled as an erasure error. Thus, at the receiver we need an RS channel erasure decoder for image recovery. The lengths of the channel encoder input and output blocks are also taken as long as possible to achieve the best performance. It is shown that our watermarking scheme which replaces only two LSB of an image, efficiently recovers the tampering up to 33% without leaving any noticeable distortion. However, if we implement our algorithm using 3 LSB, it totally outperforms the state-of-the-art methods using the same three LSB for watermarking. It should be noted that albeit the proposed scheme is just implemented for two certain sets of parameters, it can be flexibly adapted to different applications with different purposes, thanks to adaptive rate adjustment capability of applied source and channel codes.

VI FUTURE ENHANCEMENT

A total of 33% tampering is recovered after the whole process is undergone so in future a whole of 100% or at the maximum of 80% tampering can be done without any distortion done to the image quality.

VII 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. Wu and B. Liu, ―Watermarking for image authentication,‖ in Proc. Int. Conf. Image Process. (ICIP), vol. 2. 1998, pp. 437–441.

[4]J. Fridrich,―Image watermarking for tamper detection,‖ in Proc. Int. Conf. Image Process (ICIP), vol.

2. Oct. 1998, pp. 404–408.
[5]D. Kundur and D. Hatzinakos, ―Digital watermarking for telltale tamper proofing and authentication,‖ Proc. IEEE, vol. 87, no. 7, pp. 1167–
1180, Jul. 1999.
[6]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.
[7]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.

[8]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.

[9] 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.
[10] J. Fridrich and M. Goljan, ―Images with self-correcting capabilities,‖ in Proc. Int. Conf. Image