IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Novel Approach to Protect and Self-Recovery of Digital Images

S. Chandra Mohan Reddy
Professor
ECE Department
JNTUA College of Engineering
Ananthapuramu, India

K.Ravindra Reddy
Assistant Professor (Adhoc)
ECE Department
JNTUA College of Engineering
Pulivendula,INDIA

G.Krishna Murthy
Assistant Professor (Adhoc)
ECE Department
JNTUA College of Engineering
Pulivendula,INDIA

P.G.Varna Kumar Reddy
Assistant Professor (Adhoc)
ECE Department
JNTUA College of Engineering
Pulivendula,INDIA

Abstract— Image forensic in one of the most important applications of Image processing using watermarking. Protection of images against tampering is considered as important applications in Image forensics. In the last few years, researchers have developed many techniques for detecting watermarks that containing check bits and reference bits. State of art techniques are used for detecting watermarks containing check bits and reference bits. Recovering the lost reference bits still hold as problem. This paper is aimed at showing the location of tampering region; image tampering can be identified and considered as erasure error. Therefore, a proper design of channel code has to be designed to protect the reference bits against tampering. In the present proposed approach, the watermark bit-budget is categorized into three groups: a) source encoder output bits; b) channel code parity bits; and c) check bits. In watermark embedding phase, initially, the original input image is source coded and the produced output bit stream is protected with the help of channel encoder. For image reconstruction and recovery, tampered locations are identified with the help of check bits to help channel decoder in order to recover the original source encoded input image. The watermarked image quality gain is achieved through spending less bit-budget on watermark, while image recovery quality is enhanced as a consequence of consistent performance of designed source and channel codes.

Index Terms— Watermarking, Tampering, Self-recovery of digital images, check bits, SPIHT algorithm, RS codes, Fragile watermarking.

I. INTRODUCTION

Due to rapid growth in digital era, there was a scope for growth in image illegal copying and manipulation of images. There are a number of technologies that will help to provide protection from illegal copying; hence, digital watermarking algorithms were developed to solve this problem by providing image authenticity and protection. Watermarking is the process in which carrier signal is utilized to hide digital information; the hidden information should not contain a relation with the carrier signal. Watermarking algorithms embed digital signatures or digital data to prove the owner's identity and stop copyright infringement. So, digital watermarking has been evolved in each and every technical and commercial media. Watermarking has been proven technique for reduction of privacy and capability in identification of faults and managing digital media. Hence, it is found in many applications including remote triggering, filtering and e-commerce. Digital watermarking paved as better patch for content security that enable consumer to adapt the recent trends in digital revolution for reduction of content theft.

Watermarking scheme generally contains two types of media available for transmission that include original transmitter data known as cover/host image and other media include hiding supported media called as watermark. Watermarking system is considered as a system including two parts: one part for embedding and another for detection. Embedding part receives two inputs, one for encoding message (watermark) and other for input (cover/host) image. Second part is for detection that determines the existence of watermark, if exits then decode the embedded image to identify original image. Digital watermarking offers ownership security that includes identification of the copyright owner and protection. Different approaches have made in reconstruction of original image. Among those approaches a common method with the usage of hash of the original image. If transmitted is appeared to be same as hash output receiver then that image is unaltered. Integrity on usage of hash is possible with the help of secure channel that must be used for retransmission every time. As such phenomenon is not carried out, so fragile watermarking scheme is evolved in order to insert verification data to image itself.

Human vision perceives higher sensitivity to smooth regions while compared to textured regions of an image. Thus several watermarking approaches have been evolved in which watermarks are embedded in significant parts of an image. In [1], proposed a watermarking algorithm in which images are transformed into Discrete Cosine Transform (DCT) domain and watermarks were hidden in mid-frequency coefficients. The mid frequencies possess robustness against JPEG

compression and had a less distortion compared to the regions where the variation of intensities gradually changes. Bender, *et al.* [2] developed a secret key for selecting desired wavelet coefficients in order to embedded watermark. This approach is straight forward and is based on statistical changes of an image. This method is only for verifying the existence of watermark.

In [3], proposed a self-embedding method with large area restoration capability. The method can be used for image protection when image authenticity and integrity is highly required. Wang, *et al.* [4] proposed a scheme that helps in embedding watermark with the help of wavelet coefficients in appropriate locations of an image. This method involved in multi-threshold wavelet and successive sub band quantization to identify significant coefficients. All the above watermarking schemes are based on embedding significant parts of an image.

Fragile watermarking approaches are treated as sensitive approach for several kinds of distortions. DCT, quantization index modulation, frequency modulation, block wise dependence and image structure based fragile watermarking approaches are made to protect digital image and identification of tampering. Two schemes are proposed in [5] in which the first scheme is for fragile watermarking to authenticate the digital content present in input, while the second scheme is to reconstruct the region where the integrity verification suffers. The watermark embedding scheme is efficient but lacks in reduction of quality of a recovered image when the strength of attack was increased. Chen *et al.* [6] stated a technique for authentication provided with encrypted hash values and embedding them into image sub bands. This approach involved in three-level wavelet transformation to input image and slicing every sub bands into blocks. A slight variation in watermarked image destroys hash value and variations in block size will not affect detection resolution are considered as pros of the proposed scheme.

Fragile Watermarking schemes possess advantages but found in less use because of sensitive to invalid manipulations and content-preserving operations. But the trend in watermarking technology leading to recovering images even though they are tampered. Li *et al.* [10] presented a technique based on Discrete Wavelet Transform (DWT) to extract information of an image from low frequency components and embedding them in mid-frequency components to achieve tampered region for recovery. Lin and Chang [11] introduced a semi-fragile watermarking scheme in which corrupted blocks are also recovered. The main drawback of this scheme is that system works efficiently until both blocks are uncorrupted. Chang *et al.* [12] proposed a method based on block hierarchical watermarking approach in which image can be reconstructed effectively but problem arises with the authenticity.

Hsu and Wu [16] formulated a scheme based on wavelets to embed a logo as watermark. The proposed technique provides robustness only to image processing attacks. Major consideration regarding this scheme is detection in presence of watermark. Lu *et al.* [17] deals with image fusion driven watermarking in which gray scale image and binary images are used as watermarks. Watermark is embedded using LL, HL, LH and HH sub-band coefficients. Even though this algorithm withstands JPEG, EZW compressions, Blurring but major limitation is regarding its non-blind nature. A systematic approach for image coding and block based tampered detection on usage of watermarking scheme with utilization of two-LSB method is proposed in [1]. This method shows some less effect on tampered rate. In [4], proposed a hiding data algorithm in multimedia documented images. This scheme withstand for compression attacks but fragile against information loss.

From the above literature, it is observed that all those algorithms require original input image to identify the watermark and that is considered to be inefficient during many circumstances. Due to the above drawbacks in the existing literature, this paper proposes a novel approach for protecting and self-recovery of digital images from tampering.

The main objective of proposed method is to protect original image against tampering on usage of watermarking scheme. Watermark derived from encoded side should have a capability to identify the tampered region and recovering original image from those areas of tampering. This scheme utilizes least significant bits of each pixel for watermark generation and secret key based approach for image decryption.

The rest of the work is organized as follows. Section II provides the related works. Proposed scheme and methods associated with it is discussed in Section III. Results are presented in Section IV and finally conclusion is made in Section V.

II. PROPOSED METHOD

Proposed scheme involves a watermarking method to achieve protection of images against tampering. Image authentication and self-recovering of the original image is achieved with help of check bits and reference bits. The block diagram of the proposed watermarking scheme for encoding and self-recovery of digital image is shown in Figure 1 and Figure 2 respectively. The watermark scheme is of three parts: check bits, source encoder output bits, and channel encoder parity bits. Check bits are used for detection of tampered region, whereas reference bits are used for carrying information regarding the whole image. The original image is compressed using Set Partitioning In Hierarchical Transform (SPIHT) algorithm to produce source coded bits. The channel coded bit stream is generated using Reed-Solomon (RS) codes of a required rate and over source encoded bit stream. Check bits helps to locate the tampered region at the receiver section. Therefore, the receiver defines the exact location of tampered bits. Hence, there is a necessity of RS channel erasure decoder at the receiver for image recovery. The length of the channel encoder input and output blocks are considered precisely to achieve the best performance. The flowchart of the proposed algorithm for protecting and self-recovery of images is shown in Figure 3.

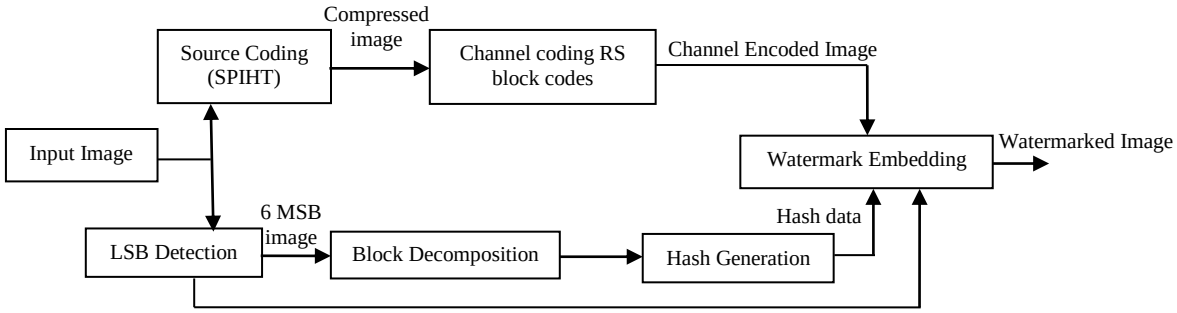


Fig 1: The Block diagram for Proposed watermarking Embedding method.

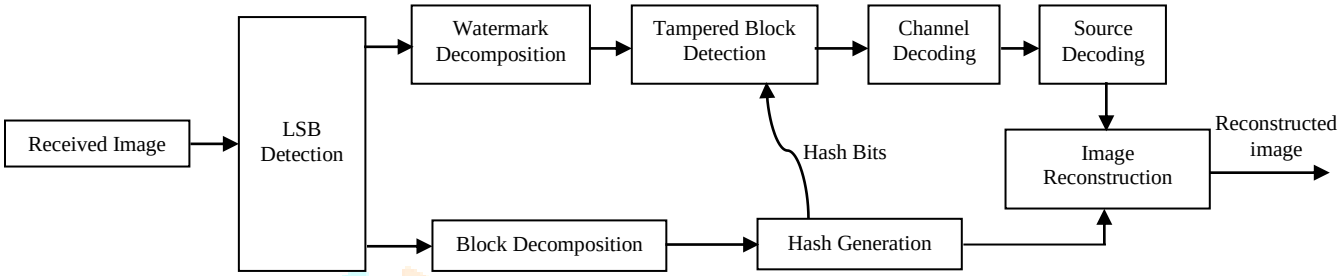


Fig 2: Block diagram Representation for Tampered detection and image recovery

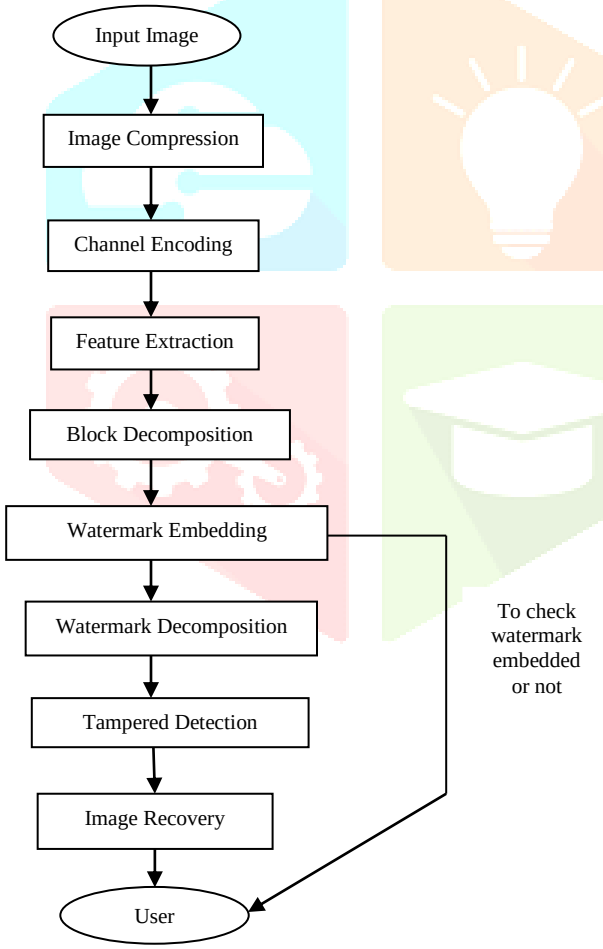


Fig 2: Flow chart of the proposed algorithm for protecting and self-recovery of images

A. Image Compression

The proposed method uses SPIHT algorithm to achieve better Image compression. SPIHT algorithm is based on Embedded Zero-tree Wavelet (EZW) coding method. This algorithm uses set partitioning sorting algorithm and spatial orientation tress. It derives a parent child relationship between similar sub-bands to achieve spatial orientation trees. The important characteristics of an SPIHT algorithm is transforming the entire input to compressed image, thus it takes quite large time and memory for operation. It derives a drawback for not performing efficient operation on small handheld and mobile devices.

B. Channel Encoding

Block codes produces *n* coded bits by accepting block of *k* information bits. During data transmission these are used for identification and correction of errors. RS codes involve a polynomial for generation of block codes based on functional table and is interpreted by *k* symbols of polynomials of degree less than *k* and remaining *(n-k)* symbols are generated by solving the polynomial at that point and dedicated system is formed by the *n* transmitted symbols.

The code rate is derives as $R=n_s/n_c$ for RS channel code, where $n_c= n_s+n_p$. The total channel code is $N_c = N \times n_c$ bits. These bits varied and spread over the whole image, so that every pixel consists of both source bits and channel coded bits. A key is generated before and after channel coding which is assumed to known by both transmitter and receiver. Then the LSB bits replaced with channel coded parity bits along with check bits and secret key in the embedding phase. The encoders and decoders are implemented by the RS code using the equation,

$$m = \overset{\min}{\hat{m}}\left(\hat{m} \mid 2^t - 1 \ \text{and} \ \hat{m} > n\right) \quad (1)$$

C. Feature Extraction

Feature extraction is related to dimensionality reduction. When the input data to an algorithm is too large to be processed and it is assumed to be redundant, then it can be transformed into a reduced set of features. The extracted features are expected to contain the relevant information from the input data, so that the desired task can be performed by using this reduced representation instead of the complete initial data.

D. Tampered Detection

The image received at receiver section is possibly tampered and are decomposed into blocks. Position bits are found using shared secret key for each block. Block bits are decomposed to MSB bits and watermark LSB bits. The watermark bit stream itself is decomposed into check bits and channel code bits. MSB bits are used to generate hash bits and tampered blocks are identified with the use of hash bits. The output bit stream is

passed into channel decoder for further recovery of channel coded bits.

E. Image Recovery

Channel coded bits are decoded using a secret key used at encryption end. Once channel coded bits are decoded then they are driven through source decoder to decode the compression of image. This is performed at encoded end using SPIHT algorithm. The Tolerable Tampering Rate (TTR) of the channel coded bits is given as:

$$TTR(n_S, n_C) = \frac{n-k}{n} = 1 - \frac{n_S}{n_C} \quad (2)$$

F. Parameter Calculation

Most probably the parameters associated with image recovery and restorations are Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). The average energy of distortion caused by watermarking measured by MSE is given as,

$$MSE(n_W) = \frac{1}{2^n w} \sum_{i=0}^{2^{n_w-1}} \sum_{j=0}^{2^{n_w-1}} (i-j)^2 \quad (3)$$

PSNR is calculated over MSE and is given as,

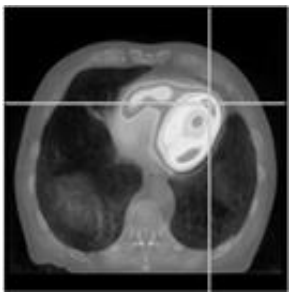
$$PSNR(n_w) = 10\log_{10}\left(\frac{255^2}{MSE(n_w)}\right) \quad (4)$$

III. Simulation Results

The proposed watermarking approach to protect and self-recovery of digital imagesThe experimental results are shown below describing procedural watermarking approach for digital image protection and tampered detection. Input images are considered for evaluation as cover image and secret input image. Cover image undergoes compression based on SPIHT algorithm to produce compressed image which undergoes channel coding on usage of RS codes. On the other hand a secret/original input image is selected and block decomposed. Based on hash generated data secret image is encrypted.

(a) Cover Image

(b) Compressed Cover Image



(c) input Image

(d) Watermarked Image

Feature extraction is carried out on original/secret image. Block decomposed image and channel coded cover undergo watermarking procedure to embed an original image in to the cover image. The produced watermark image is shown below

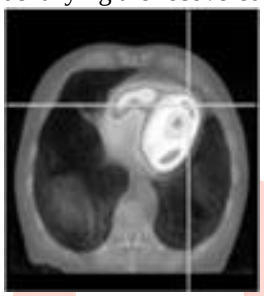
A secure key mechanism is carried out to encrypt a cover image at the encryption end. Thus same key is used to decrypt the cover in order to recover the original encrypted secret image. The decrypted cover is shown below

(e) Decrypted cover Image

(f) Tampered Image

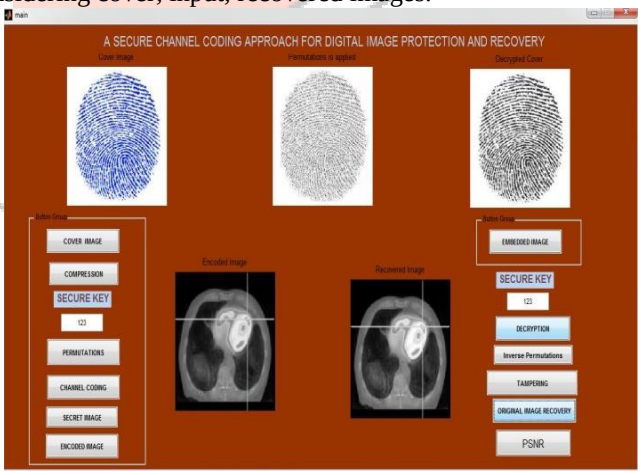
On decryption with proper key, image tampered region can be identified based on MSB block bits and watermarked LSB image. Tampering region is identified and shown below

Once tampered image is detected reference bits are capable of identifying the recovered image as shown below



(g) Recovered Image

Generalized GUI modeled approach is provided on considering cover, input, recovered images.



(viii) GUI Representation for Input-1

Watermarking and channel coded image protection and recovery approach is implemented on different input images to determine ability of proposed scheme as shown below.

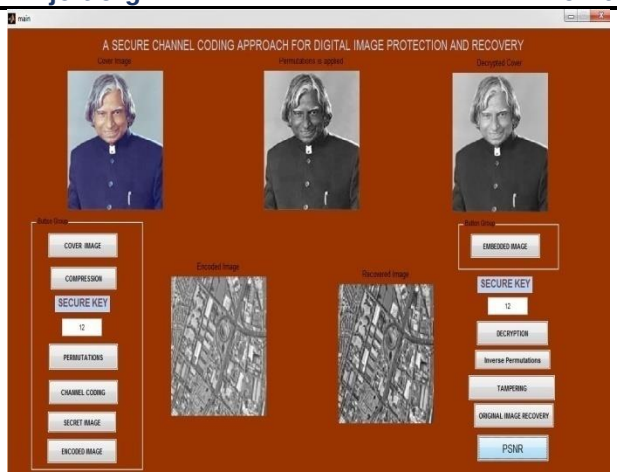


Fig 6: Generalized GUI for Input-2.

Fig 7: Generalized GUI for Input 3.

On evaluating the image parameters for different images a generalized analysis is observed in table shown below.

Table 1: Performance evaluation of proposed scheme.

Input	PSNR (dB)	PSNR (dB)	TTR
1	57.1	50.4	38.0
2	57.9	51.1	38.6
3	81.4	71.8	54.2

Tabulated values represent the performance of coding approach by considering different inputs showing PSNR (Peak Signal to Noise Ratio) and TTR (Tampering Tolerance Rate).

IV. Conclusion

In this paper, we introduced a watermarking plan on dealing with protection of image against tampering. The watermark scheme plan falls into three sections, check bits, source encoder yielded bits, and channel encoder parity bits. The original input image is source coded using SPIHT compression algorithm. The proposed scheme achieved in detecting the location regarding tampering region. Image tampering identification is considered as erasure error with the help of check bits.

Therefore, a proper designing of channel code has been made in order to protect the reference bits against tampering. However, designing an efficient is made possible on using 3 LSB, which increase tampering recovery up to 60%. It completely outperforms the state-of-the-art methods. It should be noted that source and channel codes have adaptive adjustability which help in adjustment capability to various applications.

References

[1]. J. Zhao, lin, and E. Koch, “A general digital watermarking model,” Comput. Graph, vol.22, pp. 397–403, 1,998.

[2]. Bender, J. Lee and C. S. Won, “Authentication using secret key using wavelets for watermarking images,” Electronics Letters., vol. 35, no. 11, pp. 886–887, 1999.

[3]. Zhenxing Qian and Tong Qiao, (2012) “Image Self-Embedding With Large-Area Restoration Capability”.

[4]. Shuozhong Wang, Zhenxing Qian, and Guorui Feng, (2003) “Reference Sharing Mechanism for Watermark Self-Embedding”.

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

[6]. Ting-Wen Chen, Kuo-Ming Hung, Wen-Kai Su, Chia-Nan Kao, (2010) “Automatic Image Authentication and Recovery Using Multiple Watermarks”.

[7]. Li et al. (2001) “DWT Approach for tampered detection and recovery in watermarking,” presented an IEEE transaction on image processing, vol. 14, no. 12, September 2001.

[8]. Lin and Chang (2000-2001),” Semi-fragile watermarking scheme in watermark recovery” in proc, Int, Conf., vol. 2.2001, pp.791-785.

[9]. Chang et al. (2008),”A block-based hierarchical watermarking recovery” presented a paper in International conference in 2008.

[10]. Hsu and Wu (1998)”Wavelet based watermarking scheme embedding logo watermarking,” presented a paper in IEEE transactions on Image & signal processing in 1998.

[11]. Lu et al. (2001),”A robust watermarking scheme based on image fusion and JND threshold,” presented a paper in international conference in 2001.

[12]. Saeed Sarreshtedari, and Mohammad Ali Akhaee, “A Source-Channel Coding Approach to Digital Image Protection and Self-Recovery,” IEEE Transactions on Image Processing, Vol. 24, No. 7, July 2015.

[13]. Campisi, X. B. Kang and S. M. Wei, “Data Hiding Recovery using JPEG in Digital Image Forensics,” in Proceedings of International Conference on Computer Science and Software. Engineering, Vol. 3, December 2002, pp. 926–930.