International Journal of
Scientific Engineering and Technology Research

www.ijsetr.com

ISSN 2319-8885
Vol.05,Issue.17
July-2016,
Pages:3544-3548

A New Method for Digital Image Protection and Self-Recovery using Coding Technique

S. HARI PRASAD[1], Y. BASAVA RAJU[2], P. BHANU PRAKASH REDDY[3]

[1]PG Scholar, Dept of ECE, Vaishnavi Institute of Technology, Tirupati, AP, India, E-mail: hariprasadchinna428@gmail.com.
[2]Asst Prof, Dept of ECE, Vaishnavi Institute of Technology, Tirupati, AP, India, E-mail: rajbasavaraj69@gmail.com.
[3]Asst Prof, Dept of ECE, Vaishnavi Institute of Technology, Tirupati, AP, India, E-mail: pbhanuprakash1983@gmail.com.

Abstract: A watermarking scheme to protect images against tampering was proposed. The watermark bit-budget falls into three parts, check bits, source encoder output bits, and channel encoder parity bits. The original image is source coded using SPIHT compression algorithm. The source encoder output bit stream is channel coded using RS code of a required rate and over appropriate field. The main aim of this project tampering location known, image tampering can be modeled and dealt with as an erasure error. In the proposed method introduced, the total watermark bit-budget is dedicated to three groups: source encoder output bits; channel code parity bits; and check bits. In watermark embedding phase, the input image is source coded and the destination bit stream is secured using according channel encoder. For image retrieval, erasure locations detected by check bits help channel erasure decoder to retrieve the original source encoded image. As show the proposed method significantly outperforms recent techniques is improved image quality for both watermarked and retrieval image. The protected image quality gain is achieved through spending low bit-budget on watermark, 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, Prime Fields.

I. INTRODUCTION

In digital image watermarking has been widely applied for image authentication and copy-right protection. However, recently its application is extended to digital image self-recovery, in which the lost content of the original image due to the tampering is recoverable with the help of information embedded into the image itself. The common approach in such techniques is to embed a representation of the original image into itself. This information can be protected against tampering using proper channel codes. However, it has been recently shown that the digital image self-recovery can be modeled as a source channel coding problem. In this approach, the source coded image information is channel-coded using proper codes, and embedded into itself. Therefore, the quality of the restored image and the tolerable tampering rate (TTR) depends on the bit-rate dedicated to the source and channel code bits, respectively. In source-channel coding based approaches, the recovery process fails when the tampering exceeds the rate tolerable by the applied channel coding. 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, has recently attracted growing interest. The problem of image self-recovery has been approached in numerous ways. In conventional error control coding schemes are adopted for localization and restoration.

Several methods embed a representation of an original image into itself for the sake of self-recovery. In discrete cosine transform (DCT) coefficients or reduced color-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, a binary image generated from the difference between the host image and its chaotic pattern, the hash of the original image, watermark derived from approximation coefficients of its wavelet transform, a vector quantized or halftone version of the original image. Fragile watermarks may also be designed for specific purposes, such as binary images, JPEG compressed images, colored images, compression-resistant or cropping resistant applications. 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. 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. The location of tampered areas being identified through check bits, tampering can be modeled as an erasure channel, where the locations of occurring errors are known to the receiver. Erasure modeling of tampering has been recently offered and exploited in [45] and [46], where the authors apply fountain codes [47] 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) [48] 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 [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 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.

II. RELATED WORK

P. Korus and A. Dziech, was proposed “A novel approach to adaptive image authentication,” in Proc.2011. In this paper we address the issue of the trade-off between the tampering rate and the reconstruction quality of image authentication systems. We adopt the fountain coding paradigm and design an adaptive content reconstruction scheme. The scheme conforms the reconstruction quality of individual image fragments both to the local texture properties and to the specified requirements. Experimental evaluation confirms that a framework based on this approach is a valid and convenient model of the performance of the considered reconstruction problem. Z. Qian and G. Feng, was proposed “Inpainting assisted self recovery with decreased embedding data,”in 2010. When hiding information in an image for self recovery, the amount of embedding data affects the embedding influence and the recovery quality. The purpose of this paper is to reduce the amount of embedding data while maintaining good recovery quality. We propose an approach to generate reference data from the original image by encoding different types of blocks into different number of bits. In reconstructing the reference image, a fast inpainting method is used to recover the contents of corrupted regions accompanied with the extracted bits. P. Korus and A. Dziech, “Reconfigurable self-embedding with high quality restoration under extensive tampering,” in 2012. In this paper we analyze the content reconstruction problem with the use of a revised erasure communication channel. Based on this approach, we propose a reconfigurable self-embedding system which can be adapted to different requirements.

Our approach eliminates two major problems with the design of efficient content reconstruction algorithms and allows for theoretical analysis of the reconstruction performance. The presented theoretical results are verified using Monte Carlo simulations. The proposed scheme is experimentally evaluated in a number of possible configurations, and allows to achieve high reconstruction quality even with high tampering rates. Z. Qian, G. Feng, X. Zhang, and S. Wang, “Image self-embedding with high-quality restoration capability,” in 2011. A method of self-embedding capable of restoring large-area contents is proposed in this paper. We present a table for encoding the DCT coefficients that would help compressing each block to a fixed length of 32 bits. Two schemes are designed to improve the restoration ability. In the first scheme, we embed the information of two remote blocks into the least significant bits (LSB) of the current block. In the second scheme, two LSBs are used for embedding information as well as the authentication bits. Both schemes have the ability of large-area restoration, 66.7% and 75% on the upper bound. X. Zhang, S. Wang, Z. Qian, and G. Feng, “Self-embedding watermark with flexible restoration quality,” in 2011. When a document or a sequence of characters is tampered, watermarking should be able to not only detect the tampering but also restore it. Towards this goal, self-embedding is used where the watermark is a copy of the sequence itself. Restoration algorithms for substitution attack are proposed for two variants of self-embedding. These algorithms are analyzed to show where they fail and how to avoid these failures. Strategies to cope with deletion/insertion attacks are also mentioned.

IV. MAGE WATERMARKING

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication. The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal. Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. While the modification may not be malicious, the term attack arises from copyright protection application, where third parties may attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data (in which resolution is diminished), cropping an image or video, or intentionally adding noise. Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted. In robust digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. In fragile digital watermarking, the extraction algorithm should fail if any change is made to the signal.

V. FRAGILE WATERMARK

Fragile watermarks are intolerable to both malicious and content preserving operations. Fragile watermarking techniques are designed with a goal to identify and report every possible tampered region in the watermarked digital media. Semi-fragile watermarks are intermediate in robustness between the two and are also used for image authentication as shown in Fig.1. Some critical applications like medical imagining and forensic image archiving also requires the fragile watermarks to be reversible. The different quantitative parameters such as PSNR, True and false positive may be used for the evaluation of the method of watermarking schemes.

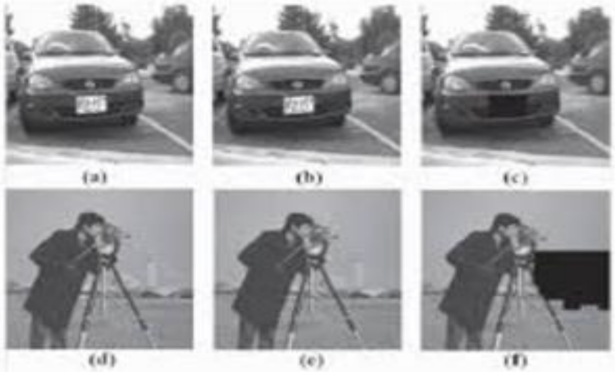

Fig.1. Fragile watermarks.

VI. SPIHT ALGORITHM

Set partitioning in hierarchical trees (SPIHT) is an image compression algorithm that exploits the inherent similarities across the sub bands in a wavelet decomposition of an image. The algorithm codes the most important wavelet transform coefficients first, and transmits the bits so that an increasingly refined copy of the original image can be obtained progressively.

VII. REED SOLOMON CODE

Reed Solomon codes are used in a wide variety of commercial applications, most prominently in CDs and DVDs, and in data transmission technologies such as DSL, DVB (Digital Video Broadcasting) and WiMAX (Worldwide Interoperability for Microwave Access). One significant application of Reed Solomon coding was to encode the digital pictures sent back by the Voyager space probe of Uranus. Modern versions of Reed Solomon codes with convolutional coding were and are used on the Mars Pathfinder, Galileo, Mars Exploration Rover, etc. Reed Solomon code is a scheme of block coding — that is, if during transmission a block of data is missing or completely erased, as long as enough of the remaining blocks are received, there is still hope to recover the data. The channel in which a block of data might be erased is also named the erasure channel. And codes designed for erasure channels are also named erasure codes. Erasure channels are commonly seen in the applications of Reed Solomon Code. For CDs or DVDs, physical scratches typically destroy one or more data blocks. In storage systems, a hard drive fails with the pattern that a whole block can not be read out. In digital video, it often happens that a data frame is missing or corrupted due to either bursty error or packet drop in the network (because of congestion).

VIII. PRIME FIELD

A prime field is a finite field $\mathrm{GF}(p)$ for p is prime. A finite field is a field with a finite field order (i.e., number of elements), also called a Galois field. The order of a finite field is always a prime or a power of a prime (Birkhoff and Mac Lane 1996). For each prime power, there exists exactly one (with the usual caveat that "exactly one" means "exactly one up to an isomorphism") finite field GF(p^n), often written as $\mathbb{F}_{p^n}$ in current usage. GF(p) is called the prime field of order p, and is the field of residue classes modulo p, where the p elements are denoted 0, 1, ..., $p-1$. $a=b$ in GF(p) means the same as $a \equiv b \pmod{p}$. Note, however, that $2 \times 2 \equiv 0 \pmod{4}$ in the ring of residues modulo 4, so 2 has no reciprocal, and the ring of residues modulo 4 is distinct from the finite field with four elements. Finite fields are therefore denoted GF(p^n), instead of GF(k), where $k=p^n$, for clarity.

IX. 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. 1(a). Fig. 1(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. 1(c), where the same image is watermarked using Zhang's method [36] 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 and results as shown in Figs.2 to 5.

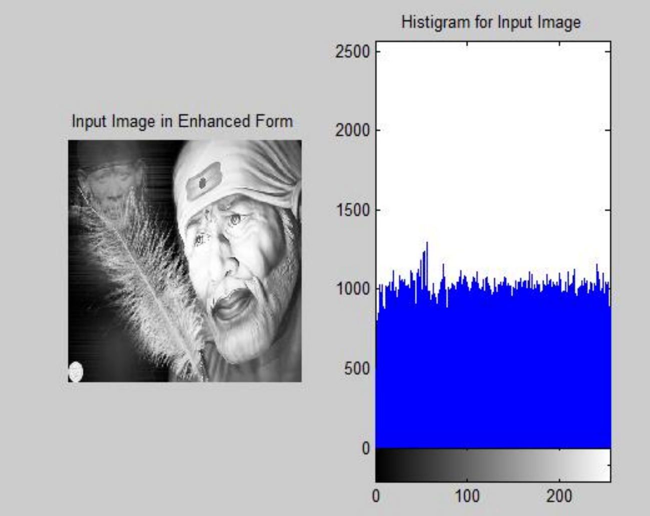

Fig.2. Input Image and its histogram.

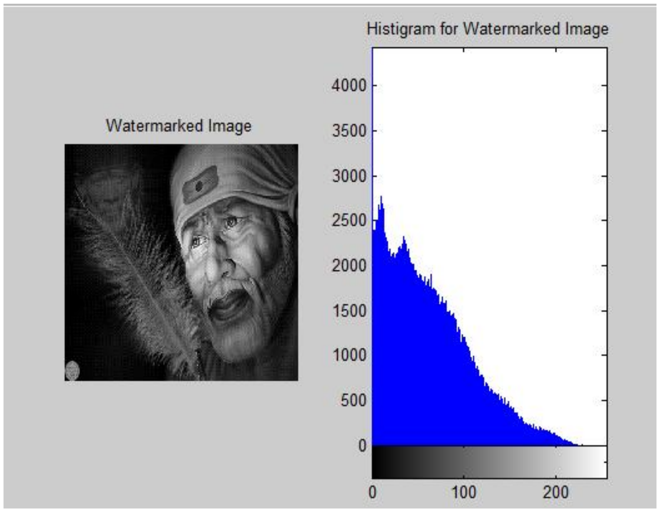

Fig.3. Water Marked image and Histogram.

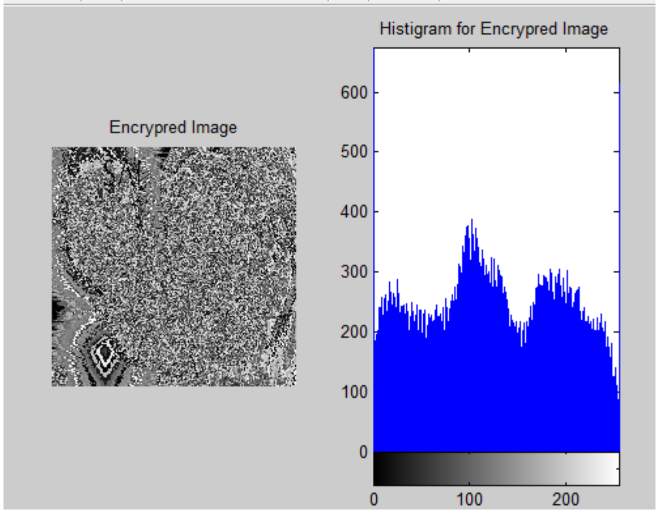

Fig.4. Encrypted image and Histogram.

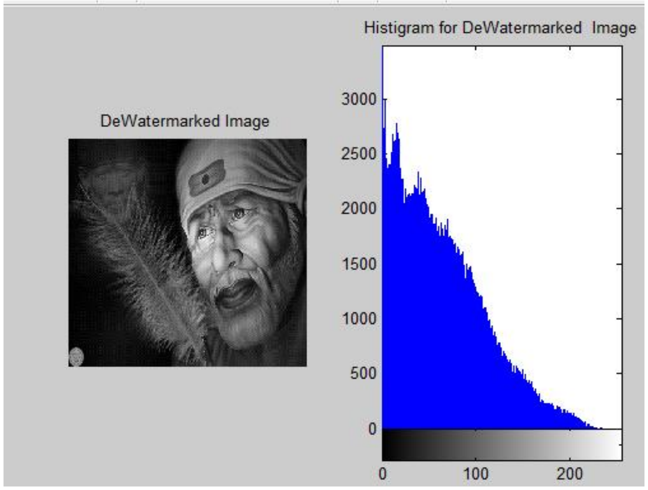

Fig.5. Dewater marking image and histogram.

X. CONCLUSION

In this propose a Source-Channel Coding Approach to Digital Image Protection and Self-Recovery. 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.

XI. REFERENCES

[1]P. Korus and A. Dziech, “A novel approach to adaptive image authentication,”in Proc. 18th IEEE Int. Conf. Image Process. (ICIP), Sep. 2011,pp. 2765–2768. Z. Qian and G. Feng, “Inpainting assisted self recovery with decreased embedding data,” IEEE Signal Process. Lett., vol. 17, no. 11,pp. 929–932, Nov. 2010.

[2]P. Korus and A. Dziech, “Efficient method for content reconstructionwith self-embedding,” IEEE Trans. Image Process., vol. 22, no. 3,pp. 1134–1147, Mar. 2013.

[3]P. Korus and A. Dziech, “Reconfigurable self-embedding with highquality restoration under extensive tampering,” in Proc. 19th IEEE Int.Conf. Image Process. (ICIP), Sep./Oct. 2012, pp. 2193–2196.

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

[5]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,

[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 watermarkingschemes 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] 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.

Author's Profile:

S.Hariprasad did his bachelor of Technology in ECE at Siddharth Institute of Engineering and Technology, Puttur, and doing Master of Technology in Digital Electronics and communication systems at Vaishnavi Institute of Technology, Tiruapti, Andhra Pradesh, India.

Mr.Y.Basavaraj received the B.Tech (ECE) from SRI VIDYANIKETHAN College of Engineering TIRUPATI, JNTU Ananthapur, India, in 2006 and M.Tech from Annamacharya Institute of Technology and Sciences, Rajampeta, India, in 2011.Currently he is working as an Assistant Professor in Vaishnavi institute of Technology, Tirupati, India. He is having 7 years of Teaching Experience.

Mr.PbhanuprakashReddy received the B.Tech (ECE) from Sri Jayam Engineering College, Kadalur, India, in 2006 and M.Tech from Madanapalli Institute of Technology and Sciences, Madanapalli, India, in 2012. currently he is working as an Assistant Professor in Vaishnavi institute of Technology, Tirupati, India. He is having 4 years of Teaching Experience.