International Journal of Engineering Research in Electronic and Communication Engineering (IJERECE) Vol 3, Issue 3, March 2016

Digital Image Protection and Self Recovery Using Source-Channel Coding

[1] V.G Roja [2] P.Sreekanth [3] N.Pushpalatha
[1] M.Tech Student (DECS), [2][3] [2]Assistant professor,
[1][2][3]Department of ECE, AITS
[1] v.rozzhaa @gmail.com, [2]sreekanth2728@gmail.com, [3]pushpalatha_nainaru@rediffmail.com

Abstract- **Digital imaging has been rapidly developing in last two decades and digital multimedia products are utilized in countless applications. As a consequence popular and low cost access to image editing applications challenges the integrity of digital images. Digital images can be easily tampered with image editing tools. Tampering is intentional modification of images. Forensics applications have been used in digital images. One of the forensics applications is to protect the images against tampering. To fulfill the purpose of image tampering the algorithm should satisfy two cases 1) Detecting the tampered area of the received image 2) Recovering the lost information in the tampered zones. State-of-the-Art techniques perform these tasks by applying watermarks consisting check bits and reference bits. Check bits are used for detecting the tampered area where as information of whole image is stored in reference bits, but the problem of recovery the lost reference bits still exists. To overcome this problem SPIHT technique is used in which if the tampering locations are known then image tampering can be modeled and dealt with as an erasure error. Therefore reference bits are protected against tampering by designing an appropriate channel code. The total water marking bit budget is dedicated into three groups 1) Source-encoder output bits 2) Channel code parity bits 3) Check bits. In watermark embedding phase, the original image is source coded and the output bit string is protected using appropriate channel encoder. For image recovery erasure locations are detected by check bits. Check bits help channel erasure decoder to recover the original source encoded image. This technique significantly outperforms recent techniques in-terms of image quality of water marked and recovered image. The water marked image quality gain is achieved through spending less bit budget on water mark. The quality of recovered image is considerably improved as a result of consistent performance of designed source and channel codes.**

Index terms— **Image watermarking, fragile watermarking, image tampering protection, SPIHT, RS channel codes.**

I. INTRODUCTION

The emergence of digital multimedia products brought drastic changes in electronic world. As a consequence of sudden production of low-cost and reliable storage devices, the digital multimedia products are used in countless applications. With this, the digital imaging and videos have been rapidly developed. At the same time, the popular and low-cost editing applications have led to the widespread of forgeries and unauthorized sharing of digital media. To overcome this problem sophisticated techniques are required for digital media to guarantee its integrity or to protect it against malicious modifications.

This problem can be overcome with the help of digital watermarking. It is useful for fortification of images, video and text. If anyone tries to harm or alter data, it can be retrieved with the help of watermarking. A digital watermark is a code that is embedded in it. It acts as a digital signature, giving the data a sense of ownership or authenticity. Any watermarking algorithm has two parts: embedding algorithm and extraction algorithm. The resent algorithms not only detect the tampered areas, but also recover the lost data.

One common approach is to use the hash of the original image. If the hash outputs of the transmitted and original matches then it is considered as unaltered data[1]-[3]. Authentication watermark can be classified as either fragile or semi-fragile. Any alterations in the pixels can be identified by fragile watermarks; whereas semi-fragile watermarks try to differentiate between content preserving. Inceptive fragile watermarking approach aims to verify only integrity of the image or detect the tampered areas with limited robustness. In the field of tampering detection, the recent methods achieve the perfect localization using watermarks against various attacks. On the other hand, some watermarking algorithm aims to restore information in detected tampered areas. Recently watermark application is extended to self-recovery. It is the process in which the compressed data is embedded as a watermark into itself. This information can protected against tampering using appropriate channel codes. The self-recovery can be modeled as a source-channel coding problem. In this method, the source-coded information is channel-coded using appropriate codes, and embedded into itself. The quality of the restored information depends on the dedicated bit-rate of the source and tolerable tampering rate (TTR) depends on channel bit-rate. In source-channel coding, the

recovery process fails only when the tampering exceeds the tolerable rate applied by the channel-coding.

Various techniques are introduced to approach self-recovery. In self-recovery method, the watermark bits falls into two categories: check bits and reference bits. The check bits are used to locate the tampered blocks and reference bits helps to restore the original data in the tampered area. For content restoration, the reference bits of certain block are embedded into another block. But, the content recovery fails in these methods if both the original block and the block containing its reference bits are detected as tampered[4],[5]. It is referred as tampering problem. To overcome this problem, recent techniques spread the representation information of one block over entire data. If both the original data and its reference bits are available then it is considered as "watermark waste".

The watermark waste problem is dealt by deriving the content from several blocks. In this method, the reference bits are source-coded which overcomes both tampering and tampering waste problems. The self-recovery finds trade-offs between three parameters: quality of the watermark, recovered content quality and tolerable tampering rate (TTR). The size of the watermark determines the amount of distortion and quality of the watermark. More watermark bits are required to achieve higher TTR or better quality of recovered data. The five most significant bits (MSB) remains unchanged while the three least significant bits (LSB) of the original are used for embedding watermark. Some methods provide almost error free restoration with very limited TTR or very low quality watermark. Some other techniques sacrifice the restoration quality to deal with tampering rate. The self-recovery algorithm trade-off these two key ideas: 1) The representation and reference bit generation as a source-coding problem 2) Modeling the tampering as an erasure channel. The major advantage of the erasure channel is, if the receiver gets a bit, it is 100% certain and correct. The confusion arises only the bits are missed or erased. The check bits identify the tampered areas, tampering can be modeled as erasure channel, where the locations of tampering are known to the receiver. The erasure modeling can be dealt with fountain codes[6], but when one block is marked as tampered; all its carrying reference bits are missed. So, to overcome this problem Reed-Solomon codes[7] with large encoding blocks over Galva fields are suggested. The original data is efficiently compressed by applying wavelet transform and set partitioning in hierarchical transforms (SPIHT) source encoding method[8]. Therefore the watermark consists of three parts: 1) Source-code bits 2) Channel-code parity bits and 3) Check bits. Source-bits act as reference bits. The reference bits are channel-coded to produce channel –code bits, in order to survive tampering erasure. The check bits are used to determine erasure locations at the receiver. The output of channel decoder is source decoded to find the compressed version of the original image.

II.RELATED WORK

In [9] based on the reference sharing mechanism, two novel self-embedding watermarking schemes have been proposed to recover the original content in the tampered area. The original content of different regions is distributed over and embedded into the entire image, and it used as reference data of the watermark. As long as the tampering is not too severe, the original data can be recovered from the tampered areas. Which in-turn refers that reference sharing does not suffer tampering co-incidence. In the first scheme, the original data in the 5MSBs layers are recovered along with original watermark. In the second scheme, different restoration capabilities are employed to protect the data at different levels.

In [10] self-embedding systems, for an erasure communication channel, a new model was proposed for content restoration. It is an alternative approach to spread the reference information over the entire image. A theoretical analysis of the inherent restoration trade-offs was studied and analytically derive formulas for reconstruction of success bounds. It does not impose any specific watermark embedding strategy, reference generation or hash calculation algorithm. Only a small set of necessary requirements is given, and compared with five state-of arts, which shows that high-quality reconstruction is still possible regardless of the amount of tampered region.

X. Zhang et al. [11] proposed a novel watermarking scheme with flexible self-recovery quality. For content recovery, the embedded watermarked data was calculated from the original discrete cosine transform(DCT) coefficients of host image. They do not contain any additional redundancy. When image is tampered the watermark can be extracted from the area without any modifications. The coefficients can also be retrieved by employing compressive sensing technique in DCT domain. If the tampered region is small, quality of recovered watermarked data results better.

X. Zhang et al.[12] proposed a self-embedding scheme, where the reference data is derived from most significant bits of the host image. The localization data derived from MSB and reference data is embedded into the LSB of the cover. At authentication side, localization data detects the substitute information and reference data detects the other blocks. The principal content in tampered area is recovered by spatial correlation in pixel-by pixel manner. Lower the tampered area, higher the quality of the recovered content.

In [13] the digital video watermarking is required for authentication and tampering detection in compressed videos. An efficient and low-complexity method is designed for embedding and extracting the watermarks. They are integrated with coding and decoding routines. The authentication method provides detection of spatial, temporal, and spatiotemporal tampering. To distinguish malicious attacks from common video processing operations, such as H.264/AVC recompression, noise, and brightness increasing, analysis of the error is used to detect tampering.

III.EXISTING SYSTEMS

Table 1 summarizes the results of Dynamic Programming (DP) optimization for 512×512 Lena images for tampering rates varying from 0.1 to 0.85. It can be seen that for higher expected tampering rates, the UEP optimizer sacrifices less significant bit-planes to provide better protection for more important bit-planes. On the other hand, it allows more bit-planes to be included in the protection process for lower risks. the original grayscale 512× 512 Lena image after being protected against $\bar{\alpha}$ = 0.5 using a 3-LSB scheme and then being tampered at the rate of α = 56%. As shown in Table 1, 13 SPIHT biplanes are included in UEP and channel coded. Since a 3-LSB scheme is applied, PSNR of the watermarked image equals 37.9 dB. Image quality of the re- stored area compared to the original image equals 35.61 dB. According to Table 1, this value means that 12 bit-planes have survived tampering as it was expected.

		TTR of bit-planes for different $\bar{\alpha}$ designs						
Bit-Plane	PSNR	0.1	0.2	0.3	0.5	0.6	0.75	0.85
1	13.25	0.92	0.92	0.92	0.92	0.99	0.99	0.99
2	14.27	0.92	0.92	0.92	0.92	0.92	0.92	0.97
3	14.5	0.92	0.92	0.92	0.92	0.92	0.92	0.97
4	15.02	0.92	0.92	0.92	0.92	0.92	0.92	0.97
5	16.37	0.92	0.92	0.92	0.92	0.92	0.92	0.97
6	18.27	0.92	0.92	0.92	0.92	0.92	0.92	0.97
7	20.96	0.92	0.92	0.92	0.92	0.92	0.92	0.97
8	23.16	0.92	0.92	0.92	0.92	0.92	0.92	0.95
9	25.95	0.87	0.87	0.87	0.87	0.87	0.87	0.93
10	29.1	0.85	0.85	0.85	0.85	0.85	0.85	0.9
11	32.37	0.71	0.71	0.71	0.71	0.81	0.81	0.88
12	35.61	0.45	0.45	0.64	0.64	0.73	0.78	0
13	38.8	0.28	0.28	0.46	0.46	0	0	0
14	43.02	0	0	0	0	0	0	0
15	48.86	0	0	0	0	0	0	0
16	55.23	0	0	0	0	0	0	0

Table 1:: Reconstruction Profile for Lena 512 × 512 3-LSB protection

IV.DIGITAL WATERMARKING

Digital watermarking[14] is a technique which allows an individual to add copyright notices or other verification messages to digital media. The term "Digital Watermark" was coined by Andrew Tirkel and Charles Osborne in December 1992.

- It should be perceptually invisible to the naked eye to prevent obstruction of the original image. So that it cannot be detected or erased.
- It should be fairly simple; else the detection of watermark requires lot of time.
- Watermark must be accurate, and produced in numerous numbers.
- The watermarks should be robust to filtering, additive noise, compression and other forms of image manipulation

There are two types of watermarking: visible and invisible. The watermarking should be capable of detecting the tampered regions and recover them. Applications of watermarks include finger printing, copyright protection, bank notes, passports, broadcast monitoring and data authentication.

V.SPIHT ALGORITHM

Set partitioning in hierarchical trees (SPIHT) is an image compression algorithm. It is used as source encoder. It can truncate its output bit stream at the desired rate and come to a certain reconstruction of the original image. Better quality of reconstruction is achievable for more output rate. 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. The sorting order must be available at the decoder. SPIHT exploits the self-similarities across different sub bands of wavelet transform. These similarities can be found through wavelet transform spatial orientation trees. Beside the low computational complexity, SPIHT algorithm produces adaptive output rate, which makes it suitable for different application. Channel coding is applied to source encoder output bit stream to protect it against tampering.

VI.REED SOLOMON CODES

Reed solomon codes are error-correcting codes. They are widely used in cds, dvds, blu-ray discs etc. They are also used in satellite communications. Reed-solomon codes are non-binary cyclic error-correcting codes. They are based on univariate polynomials over finite fields. They are able to detect and correct multi symbol errors. By adding t check symbols to the data, a reed–solomon code can detect any combination of up to t erroneous symbols, or correct up to ⌊t/2⌋ symbols. Reed-solomon codes are block codes. If during transmission a block of data is missing or completely erased, there is still hope to recover the data, as long as the remaining blocks are received. In a channel if a block of

data is erased, then it is referred as erasure channels. The codes designed for this channels are named as erasure channel. 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 cannot 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).

VII.PRIME FIELDS

A field is a commutative ring in which all nonzero elements are invertible. A finite field is a field with a finite number of elements; the number of elements is the order of the field. A prime field is a finite-field. Finite field order is called as Galois field GF(p) for p is prime. The order of a finite field is always a prime or a power of a prime.

VIII.CONCLUSION

A source-channel coding approach shows that watermarking scheme in which only two lsb bits are replaced, and efficiently recovers the tampering up to 33% without any noticeable distortion. However, if this algorithm is implemented using three lsb, then it totally outperforms the state-of-art methods using the same three lsb for watermarking.

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]X. Zhu, A. T. S. Ho, and P. Marziliano, "Image authentication and restoration using irregular sampling for traffic enforcement applications," in *Proc. 1st Int. Conf. Innov. Comput., Inf. Control (ICICIC)*, vol. 3. Aug./Sep. 2006, pp. 62–65.

[5] X. Zhu, A. T. Ho, and P. Marziliano, "A new semi-fragile image watermarking with robust tampering restoration using irregular sampling," *Signal Process., Image Commun.*, vol. 22, no. 5, pp. 515–528, 2007.

[6]D. J. C. MacKay, "Fountain codes," *IEE Proc.-Commun.*, vol. 152, no. 6,pp. 1062–1068, Dec. 2005.

[7] S. B. Wicker, *Reed–Solomon Codes and Their Applications*. Piscataway, NJ, USA: IEEE Press, 1994.

[8] A. Said and W. A. Pearlman, "A new, fast, and efficient image codec based on set partitioning in hierarchical trees," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 6, no. 3, pp. 243–250, Jun. 1996.

[9] X. Zhang, S. Wang, Z. Qian, and G. Feng, "Reference sharing mechanism for watermark self-embedding," IEEE Trans. Image Process., vol. 20, no. 2, pp. 485–495, Feb. 2011.

[10] P. Korus and A. Dziech, "Efficient method for content reconstruction with self-embedding," IEEE Trans. Image Process., vol. 22, no. 3,pp. 1134–1147, Mar. 2013.

[11] X. Zhang, Z. Qian, Y. Ren, and G. Feng, "Watermarking with flexible self-recovery quality based on compressive sensing and compositive reconstruction," IEEE Trans. Inf. Forensics Security, vol. 6, no. 4, pp. 1223–1232, Dec. 2011.

[12] X. Zhang, S. Wang, Z. Qian, and G. Feng, "Self-embedding watermark with flexible restoration quality," Multimedia Tools Appl., vol. 54, no. 2, pp. 385–395, 2011.

[13] Mehdi Fallahpour, Shervin Shirmohammadi, Mehdi Semsarzadeh, and Jiying Zhao, " Tampering detection in compressed digital video using watermarking" IEEE Trans. Instrumentation and measurement, VOL. 63, NO. 5, MAY 2014.

[14] M. Wu and B. Liu, "Watermarking for image authentication," in *Proc.Int. Conf. Image Process. (ICIP)*, vol. 2. 1998, pp. 437–441.

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

[1]**V.G.Roja** received B.Tech Degree in Electronics and Communications from Sri Padamavati Mahila Visvavidyalaym, Tiupathi in 2014 and currently pursuing the M.Tech in Digital Electronics and Communication systems at Annamacharya Institute of Technology and Sciences, Tirupathi.

[2]**P.Sreekanth** received the B.Tech Degree from Sri Sai Institute of Technology and science (SSITS), Rayachoti in the year 2007 and M.Tech from Annamacharya Institute of technology and sciences(AITS), Rajampet in the year 2011. He is currently an assistant professor at Annamacharya Institute of Technology and Sciences, Tirupathi.

[3]**N.Pushpalatha** received the B.Tech Degree from JNTU, Hyderabad in 2004 and M.Tech from A.I.T.S., Rajampet in 2007. Currently she is working as Assistant Professor at, Annamacharya Institute of Technology and Sciences, Tirupati since 2006. Many B.Tech projects has been guided under her presence. Her Research area includes Data Communications and Ad-hoc Wireless Sensor Networks.