REVERSIBLE WATERMARKING WITH DENOISING USING SOURCE CODING TECHNIQUE

M.Yuvaraju[1],N.Manju Sunthari[2]

[1] *Assistant Professor, Department of EEE, Anna University Regional Campus, Coimbatore, Tamil Nadu, India*

[2] *PG Scholar , Department of EEE, Anna University Regional Campus, Coimbatore, Tamil Nadu, India*

Abstract -*Watermarking is a widely used technique for image security and authentication. An important application in watermarking is image protection against tampering. This paper proposes an efficient watermarking algorithm that detects the tampered zones and recovers the information lost in those zones. The original image is source coded in the watermark embedding scheme and the output bit stream is protected using appropriate channel encoder. For image recovery, erasure locations that can be detected by check bits help channel erasure decoder to retrieve the original image. The watermarked image quality gain is achieved through spending less bit-budget on watermark. The image recovery quality is being improved well as a consequence of consistent performance of designed source and channel codes. The design is used to protect and provide self recovery for image security applications and can remove the noise in case of noisy image during the recovery. Experimental results show that the proposed scheme outperforms other similar methods in terms of image quality before and after watermarking.*

Keywords: Image watermarking, Source coding, Tampering protection, Noise removal, Self recovery.

1.INTRODUCTION

In the present globalized world, the internet availability and diverse image processing tools reach a greater degree, that there are chances of downloading an image from the internet, and one can manipulate it without the permission of the rightful owner. For such reasons image authentication has become an active and also vital research area. Embedding watermarks in both signals and images may cause distortion. A successful watermarking method satisfies some fundamental requirements. Many number of media specific hash functions have been proposed for multimedia authentication. A multimedia hash is nothing but a content-based digital signature of the media data. Hence to generate a multimedia hash, a secret key is used to extract many features from the data. Those extracted features are further processed to form the hash. The hash is transmitted along with the media by appending or simply embedding it to the primary media data [8]. At the receiver side, the authenticator uses the same secret key to generate back the hash values, which are compared to the ones transmitted along with the data for verifying the authenticity. Also in addition to the content authentication, multimedia hashes are being used in content based retrieval from databases. To search for any multimedia content, some negative methods like sample by sample comparisons are inefficient. Also, these methods are used to compare the lowest level of content representation and they do not offer robustness in such situations as geometric distortions.

Robust image hash functions can be used for the problem solving. Usually the hash is computed for each data entry in the database and is stored with the original data and they are in the form of a look-up table. Hence when it is needed to search for a given query in the database, its computed hash value is compared with the data entry corresponding to the matched item, in terms of certain hash-domain distance that often is responsible for content similarity, is then fetched. The hash has much smaller size than the original media and the hash value matching is more efficient. Image hash functions have also been used in image and video watermarking applications. The hash functions are widely used as image-dependent keys for watermarking. Some techniques called fragile watermarks are used in authentication and image tampered zone location. Even it can be used for recovering lost information in the tempered zones. Also inceptive watermarks can verify the image integrity with robustness. Recent methods achieve 100% localization against many attack varieties. Some watermarking algorithms of error concealment restore information in tampered parts that are previously detected. Further techniques can accomplish the tampering localization [1] and error concealment by a single watermark. The self recovery watermarking trend is being in recent interest [2]. Also some conventional error control coding methods are adopted to solve the above problem.

In the past techniques discrete cosine transform (DCT) coefficients of host image [3] is embedded in least significant bit (LSB) of original image. A binary image generated by the difference between the host image and its chaotic pattern , the original image hash and watermarks derived by the coefficients of wavelet transform, a quantized vector of original image [11].Watermark bits are classified into check bits and reference bits. The check bits localize the tampered bits and reference bits restore the original image in tampered area. For content restoration the reference bits are embedded into other bits. In some blocks when both the bits are detected to be tampered then the content recovery may result in failure. The problem is known as

tampering problem. To overcome the problem of watermark waste where both original data and reference bits are available, some technique suggests a dual watermarking scheme in which watermarked image has two copies of content data for each block to leave a chance of restoration when one copy is lost due to tampering [7].

In the source coding method reference bits are source coded, which includes the data derived from the original image and is scattered. The self recovery problem exists when finding trade off among the watermarked quality, content recovery quality, and tolerable tampering rate (TTR) [9] [12] [15].Usually more watermark bits are needed to gain high TTR and better image quality. Generally recent methods dedicate three LSB of original image for embedding watermark and keeps five remaining most significant bits (MSB) unchanged. For flexible methods reconstruction quality decays when tampering rates increases.

In the proposed algorithm the trade off is approached by i) by modelling image representation and reference bit generation as source coding problem, ii) by modelling the tampering as erasure channel and handling with proper channel coding.

The tampered area location can be identified through check bits and tampering as erasure channel. The technique uses Reed-Solomon codes with large encoding blocks and over large Galva fields to solve the erasure problem. For compressing the original image the wavelet transform is applied and set partitioning in hierarchical transforms (SPIHT) is used as source encoding method.

2. RELATED WORKS

The image self-embedding method based on DCT coefficients of image. The sparse DCT coefficients are under sampled for compressive sensing and sparse processing. The tampered data lost is recovered at receiver using compressive sensing [16]. The reference data is generated by least square quantization of DCT coefficients [4]. The embedding capacity is dedicated to the reference data and the data lost will be recovered with higher quality and tampering rate being low. Also least square quantization method is used in some schemes to achieve low TTR and high quality image.

3. PROPOSED SCHEME

Efficient methods include the algorithm design such that the watermark is embedded into the original image to avoid tampering. The watermark is designed to find the tampered areas of received image and to recover the content in tampered zones. For this purpose 'n_m' MSB of each pixel is unchanged and 'n_w' bits are used for watermark embedding.

In order to recover the image, source coding algorithm is used for compressing the image and hence embeds the result as watermark. Any compressed information may be lost due to tampering [6]. For this purpose, the bit stream is channel coded to exhibit robustness. The tampered blocks are detected by means of check bits and they can be inserted in the watermark part. Thus 'n_w' bits (LSB) comprises both check bits and channel coded bits. The tampering can be modelled as erasure channel [5]. The check bits at receiver side are capable of locating tampered blocks. These blocks identify erasure locations and channel erasure decoder and thus can find the compressed bit stream. Thus source encoded image can be decoded and the original image estimation is recovered.

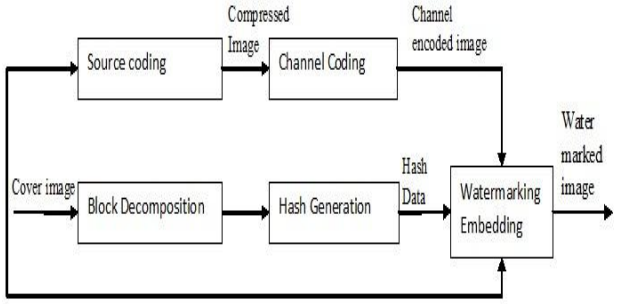

Fig -1: General encoder

3.1. Source Coding

Set Partitioning in hierarchical trees (SPIHT) is used as the source coding scheme [11]. This is an embedded compression method used for truncating output. Discrete wavelet transform bits are used. And sorting among DWT bits is then performed. Hence DWT bits with high magnitude are sent earlier. The sorting pass is also available for the receiver. SPIHT uses self similarities across the sub bands of wavelet transforms. Sophisticated sorting method with least required bit budget is possible from self similarities on spatial orientation trees from root downwards to leaves. Compression quality at 'n_s' determines the constant restoration performance. This would also provide different compression rates for different purposes. Further the output bit stream is subjected to channel coding.

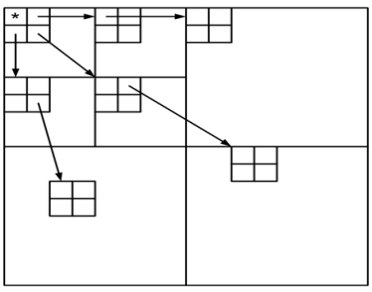

Fig-2: Examples of root-leaves dependencies

3.2 Channel Coding

To protect the image against tampering channel codes are used. The tampered blocks can be found using check bits. Hence error locations are available known to the decoder. It is assumed that all the embedded channel code bits are erased when the blocks are detected to be tampered.

Hence Rs codes with large code words are used for the above problem. This takes the advantage of using one symbol for large code words and is hence less affected by tampering. Image is compressed at the rate of '$n_{s'}$, bits per pixel, and '$n_{c'}$ is dedicated to channel code where $n_c = n_s + n_p$.

When k represents bit symbols for codes over Galva Fields GF (2^k), the method can generate up to $2^{(k-1)}$ symbols in single iteration. The main technique is based on dividing the image into 64x64 pixel small blocks. Every block is watermarked by means of frequency spread spectrum technique.

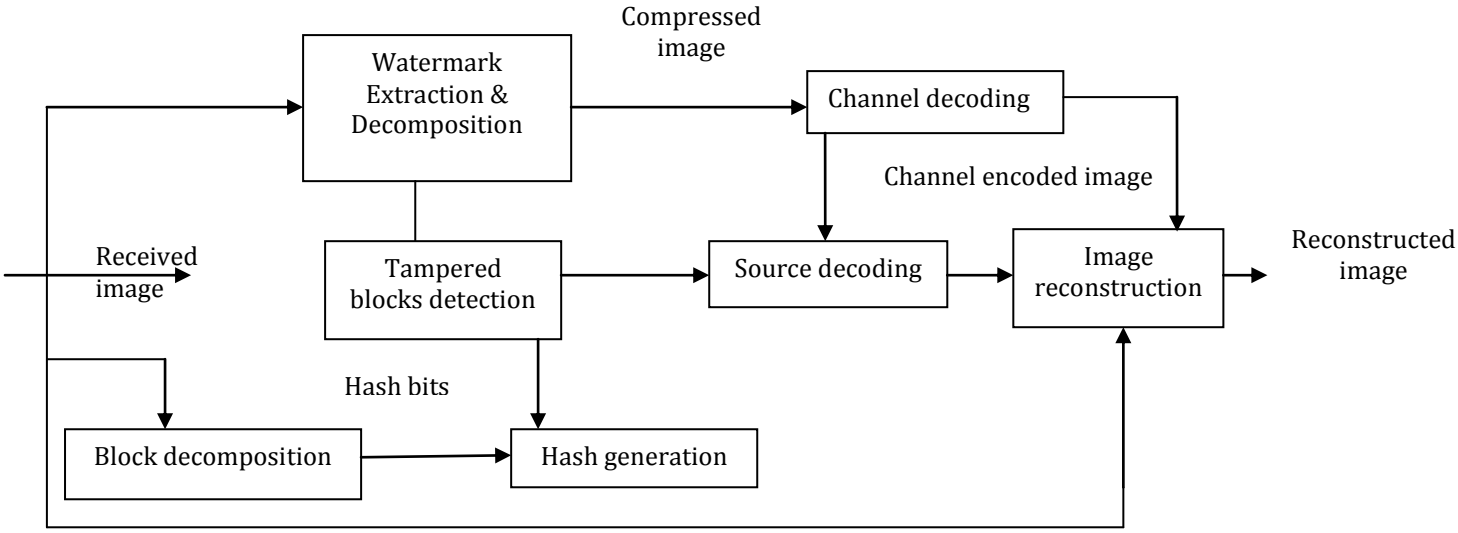

Fig-3: General decoder.

4. NOISE REDUCTION

Salt and pepper noise is introduced in the input side image and is processed to ensure noise removal at receiver side. Since the median filter is the best suited filter for salt and pepper noise. This can improve the later processing steps and the edges can also be preserved. Median filter runs through each entry of signal and replace each with median of its neighbour entries. These patterns are therefore called windows that could slide over every signal.

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

5. EXPERIMENTAL RESULTS

The proposed system is implemented in the software MATLAB.A cameraman image of size 512x512 is chosen as an input image (a) and is watermarked using the proposed method.

Salt and pepper noise is applied to the input image and is shown in (b) the watermark image (c) is the image that is to be hidden inside the original input image which can be recovered and detected in further steps.

The histogram image (d) is nothing but detecting the noise in terms of least squares which would be used for tampering protection of the image. Hence is mentioned in the form of histogram. The image is attained for reconstruction of the image that can be obtained by using the principle of compressive sensing as shown in (e).

Fig-4(a): 8 bit gray scale input cameraman image is of size 512x512.

Fig-4(b): Salt and pepper noise is introduced in the input image that can be further reduced at the receiver side.

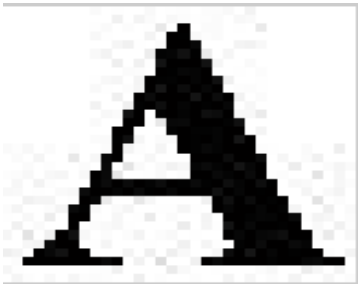

Fig -4(c): The above watermark image is hidden inside the input cameraman image.

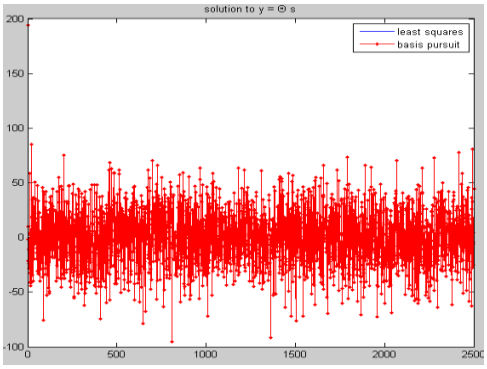

Fig -4 (d): Histogram image for tampering protection.

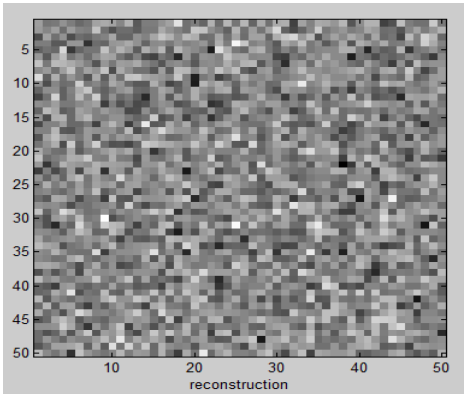

Fig-4(e): The above image is based on compressive sensing for image reconstruction.

The noise removed watermarked image (f) is the watermarked image that is formed after the data is hidden in the original image. The detected watermark is shown in the (g) image. It could also provide a Current plot held PSNR 47.4177.

Fi-.4(f): The resulting noise removed image at the receiver side.

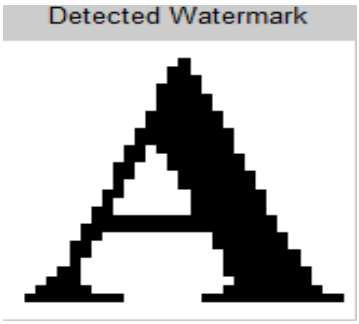

Fig-4(g): Extracted watermark hidden in the original image.

The PSNR comparison graph between the image with salt and pepper noise and the image without noise technique is shown in the Fig.5.

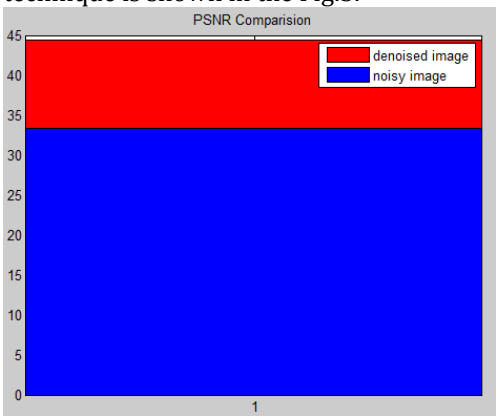

Fig -5: PSNR comparison graph

Table – I: Comparison of noise ratio

S.NO	METHOD	2-LSB	3-LSB
1	Korus method	32.5	34
2	Zhang's method	-	40
3	Existing method	33	41
4	Proposed method	34	45

6. CONCLUSION

Watermarking along with cryptographic techniques could definitely provide an efficient copyright protection. According to the necessary intended requirements and the security level requirements, the suitable watermarking algorithm can be chosen. Experimental results show that the proposed scheme significantly outperforms recent techniques in terms of image quality for both watermarked and recovered image. The proposed method can be further enhanced by considering the noise ratio and reconstruction quality.

ACKNOWLEDGEMENT

The authors would like to extend sincere gratitude and hearty thanks to the Department of Electrical and Electronics Engineering in Anna University Regional Campus, Coimbatore for their valuable support and worthy reviews which helped a lot to improve the paper quality.

REFERENCES

[1] Bravo-Solorio.S,Li.C.T,andNandi.A.K, "Watermarking method with exact self-propagating restoration capabilities," in Proc. IEEE Int. Workshop Inf. Forensics Security (WIFS), pp. 217–222,DEC.2012.

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

[3] Fridrich.J and Goljan.M,"Images with self-correlating capabilities,"in Proc.Int.Conf.Image Process. (ICIP), vol.3.pp.792-796.1999.

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

[5] Korus.P and Dziech.A, "Reconfigurable self-embedding with high quality restoration under extensive tampering," in Proc. 19th IEEE Int. Conf. Image.

[6] Korus.P and Dziech.A, "A novel approach to adaptive image authentication," in Proc. 18th IEEE Int. Conf. Image Process. (ICIP), pp. 2765–2768, Sep.2011..

[7] Lee.T.Y and Lin.S.D, "Dual watermark for image tamper detection and recovery," Pattern Recognit.," vol. 41, no. 11, pp. 3497–3506, 2008.

[8] Mall.V, Bhatt.K, Mitra.S.K, and Roy.A.K, "Exposing structural tampering in digital images," in Proc. IEEE Int. Conf. Signal Process., Comput. Control

[9] Qian.Z, Feng.G, Zhang.X, and Wang.S, "Image self-embedding with high-quality restoration capability," Digital Signal Process., Vol. 21, no. 2, pp. 278–286, 2011.

[10] Said.A and Pearlman.A.W, "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

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

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

[13] Zhang.X, Wang.S, Qian.Z, and Feng.Z, "Reversible fragile watermarking for locating tampered blocks in JPEG images," Signal Process, Vol. 90, no. 12, pp.

[14] Zhang.X, Wang.S, Qian.Z, and Feng.G, "Reference sharing mechanism for watermark self-embedding," IEEE Trans. Image Process., Vol. 20, no. 2, pp.

[15] Zhang.X, Qian.Z, Ren.Y, and Feng.G, "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.