Volume 3, Issue 10, October 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# An Secure Technique for Image Watermarking Scheme

**G.Yamini, G. V.Arunavaranasi**
*Department of Computer Science and Engineering*
*Sreenidhi Institute of Science and Technology (SNIST), India*

***Abstract—in this paper, a robust watermarking scheme using optimization watermarking technique is proposed. In the presented scheme, the watermark image is embedded in the SCS transform domain. The experimental results indicate that superiority of the proposed method against common attacks such as JPEG compression, Gaussian noise addition, median filtering, salt and pepper noise, etc., compared with the existing watermarking schemes using multi-scale transformations***

***Keywords— Digital watermarking, RC4, DWT, SCS-QIM, JPEG***

## I. INTRODUCTION

Digital watermarking is a covert security feature for identity documents that enables trusted authentication of host image like the image of PAN card and other IDs. Watermarking involves the transformation of a digital artifact into another token of the same type. Watermarking is done at the object-level. Almost all watermarking methods, which have been proposed today, can provide robust and secret watermark and against various attacks such as filtering, data compression, warping, cropping etc. Along with the rapid development and widespread use of multimedia and computer network technologies, various multimedia products such as image, audio, video are increasingly exposed to illegal possession, reproduction, and dissemination. Unrestricted copying and convenient digital media manipulation cause considerable financial loss and show up an issue of intellectual property rights [2]. Digital watermarking provides a way to perceptibly embed digital information into both digital (images, video, audio) and conventional (printed material) media contents. By extracting this secret digital data, the copyright of digital media can be protected and authentication to digital media can also be provided as well [3, 4].Robustness and imperceptibility are two fundamental but contradicting properties in robust digital watermark-king. Robustness means that the watermarked data can withstand different image processing attacks and imperceptibility means that the watermark would not introduce any perceptible artifacts [1]. Watermarking systems can be classified to three main types which are non-blind, semi-blind, and blind according to whether the original media is required or not during the extracting processes [5]. Non-blind technique requires the original image; semi-blind technique only needs the watermark; and blind technique requires neither the original image nor the watermark. Majority of watermarking schemes are implemented in spatial domain or in frequency domain. Large numbers of literatures show that the performance of watermarking schemes based on frequency domain is far better than those operating in the spatial domain. Digital watermarking technology is emerging as a solution to a broad class of challenges. There has been great interest in applying watermark to digital multimedia data for copyright protection, image authentication and proof of ownership etc. Image watermarking is finding more and more support as a possible solution for the protection of intellectual property rights

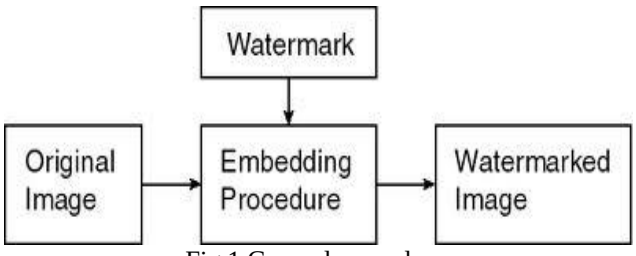



Fig 1 General procedure

For this reason, large numbers of transformation-based watermarking algorithms are proposed using discrete cosine transform (DCT) [6], discrete Fourier transform [7], and wavelets [8] in the past few decades. It is known that natural images do not simply include 1D piecewise scan-line, and have many discontinuity points. In fact, wavelet as a separable 2D multi-resolution transform does not possess directional property and simply follows the curves as horizontal–vertical lines and essentially cannot represent 2D directional discontinuity which is common in as image edges [9]. In 1999, Candes and Donoho [10] introduced a new multi-scale transform called the curvelet transform which can use a few samples to represent edges and other singularities along curves much more efficiently than traditional transforms like wavelet [11]. After this, certain watermarking schemes based on curvelet domains have been proposed [12, 13].

## II. RELATED WORK

***Encryption background***

Ciphering of images is actually an important issue. One essential difference between text data and image data is that the size of image data is much larger than the text data. The time is a factor very important for the image encryption [15]. Two levels of time are found, the first is the time to encrypt, and the other is the time to transfer images. To minimize it, the first step is to choose a robust, rapid and easy method to implement cryptosystem. In pervious study, we have found some articles on image encryption: In 2000, Tarish [16] proposed image cryptographic system based on stream cipher as a tool for image encryption. In 2003, Pommer [17] two approaches of selective encryption where wavelet-based methods are used for compression. The first attempt was to hide the choice of filters, while the second approach of selective encryption was based on wavelet packets and the decomposition tree are keep secret. In the present work, the RC4 algorithm is developed to encrypt image with wavelet subband images (LL, HL, LH or HH).

## III. PROPOSED METHOD

### A. DWT COMPRESSION

The proposed technique first decomposes an image into coefficients called sub-bands and then the resulting coefficients are compared with a threshold. Coefficients below the threshold are set to zero. Finally, the coefficients above the threshold value are encoded with a loss less compression technique. The compression features of a given wavelet basis are primarily linked to the relative scarceness of the wavelet domain representation for the signal. The notion behind compression is based on the concept that the regular signal component can be accurately approximated using the following elements: a small number of approximation coefficients (at a suitably chosen level) and some of the detail coefficients.

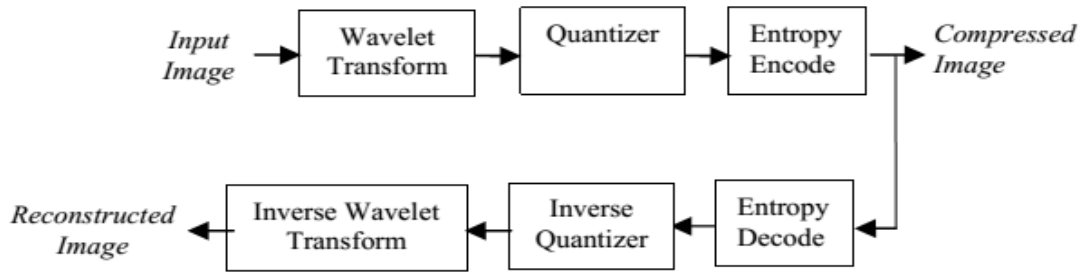



Fig. 2 Wavelet transforms based compression

The steps of the proposed compression algorithm based on DWT are described below:

a) Choose a wavelet; choose a level N. Compute the wavelet. Decompose the signals at level N.

b) For each level from 1 to N, a threshold is selected and hard thresholding is applied to the detail coefficients and

c) Compute wavelet reconstruction using the original approximation coefficients of level N and the modified detail coefficients of levels from 1 to N.

### B. ENCRYPTION ALGORITHM

RC4 Algorithm:

A secret key cryptosystem encrypt image pixel by pixel, with the RC4 algorithm. RC4 convert original image to encrypted image one bit at a time. The simplest implementation of a RC4 is shown in Figure (3) [7]. A key stream generator (sometimes called a running-key generator) outputs a stream of bits:

K1, K2, K3… Ki

. This key stream is XORed with a stream of plaintext bits, P1, P2, P3… Pi to produce the stream of cipher text bits C1, C2 …Ci …….. 1

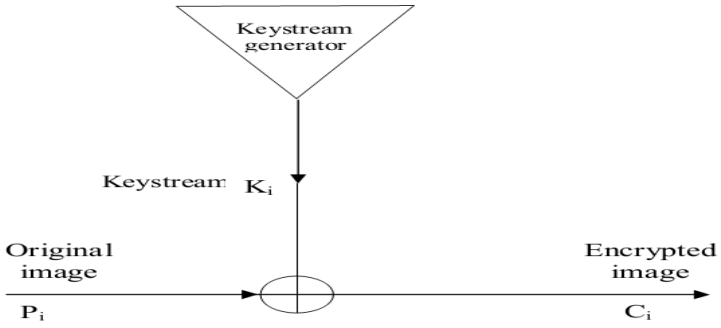



Fig 3: RC4 system

RC4 system consists of two main parts:
1- Algorithm to generate key stream.
2- XOR gate.

C. EMBEDDING ALGORITHM

The encryption algorithm used is an additive privacy homomorphic one, so the watermark embedding is performed by using a robust additive watermarking technique. Since the embedding is done in the compressed ciphered byte stream, the embedding position plays a crucial role in deciding the watermarked image quality.

Hence, for watermarking, we consider the ciphered bytes from the less significant bit planes of the middle resolutions, because inserting watermark in ciphered bytes from most significant bit planes degrades the image quality to a greater extent. Also, the higher resolutions are vulnerable to transcoding operations and lower resolution contains a lot of information, whose modification leads to loss of quality.

We show how the watermark can be inserted in less significant bit planes of middle resolutions without affecting the image quality much. Since the embedding and detection are done on integer domain, the watermark is added after rounding off to the nearest integer for SCS-QIM.SCS-QIM: In [14], Eggers et al.proposed SCS scheme for watermark embedding. In this scheme, given watermark strength, we choose a quantizer from an ensemble of quantizers to embed the watermark.

D. IMAGE QUALITY MEASURES

Peak signal-to-noise ratio (PSNR) is the standard method for quantitatively comparing a reconstructed image with the original. For an 8-bit grayscale image, the peak signal value is 255. Hence the PSNR of an M×N 8-bit grayscale image x and its reconstruction x is calculated as:

**ATTACKS**

An important requirement of watermarking scheme is robustness. However it is important to note that the level of robustness required varies with respect to the application in hand [6]. In today's world, images are sent on internet as well as in transmission from one point to another; in such case, some noise is added to the images. Some of the time attacks on images may be deliberate also to misuse it. Following sections cover different types of attacks and detect logo for each case. Comparative study of logo detection under various attacks is done.

***A. Cropping***

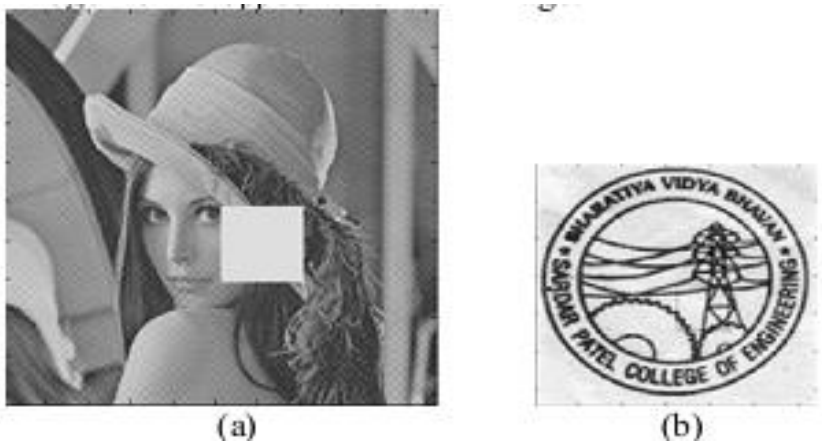
Lena image is the image where face of image is cropped. All the pixel values of particular part are made 255. So if some hidden information is there in that particular part then it will be lost. On one hand image is corrupted and at the same time loss of confidential information also take place. In this situation algorithm detects cropped region very evidently along with usual detection of logo. For experimental verification, face of Lena image is cropped as shown in figure 4.

a) Consider the watermark image as host image or input image having size 512 X 512. Crop the watermark image by making the value of the respective pixel to zero.

b) Decompose the cropped watermark image by using discrete wavelet transform. Then we will get the first level approximation coefficients i.e. LL1, horizontal coefficient LH1, vertical coefficient HL1, diagonal coefficient HH1as first level watermark key coefficients of cropped watermark image.

c) Approximation coefficient of first level is LL1which is further decomposed into new coefficients i.e. LL2, horizontal coefficient LH2, vertical coefficient HL2, diagonal coefficient HH2as second level watermark key coefficients of cropped watermark image.

d) Extract the logo as per the procedure of given algorithm to find the cropped extracted watermark logo from cropped watermark image.




(a) (b)

Fig 4 Cropping

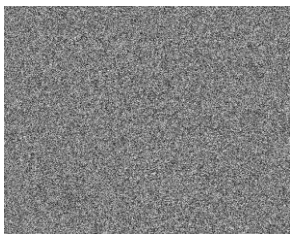
## IV. RESULTS AND DISCUSSION

Input image

**DWT COMPRESSION**

Compressed image

Compressed image → **RC4-ENCRYPTION**



Encrypted image

Encrypted image

Copyright

Watermark

EMBEDDED SCHEME

Final Watermarked image

Final Watermarked image

EXTRACTION SCHEME

Copyright

Extracted watermark

## V CONCLUSION

To determine the best compromise between robustness and imperceptibility, a number of experiments have been conducted. Overall, the experimental results demonstrate that our scheme provides excellent robustness against histogram equalization, Gaussian noises, cropping, luminance, and contrast attacks. Besides, the quality of the watermarked image is satisfactory in term of perceptibility .The comparison results between the proposed method and the

existing watermarking schemes show that the proposed method is comparable in terms of robustness and the processing time. And the security analysis result proved that the proposed method is secure.

**REFERENCES**


1. CI Podilchuk, EJ Delp, Digital watermarking: algorithms and applications. IEEE Signal Process. Mag. 18(4), 33–46 (2001)
2. IJ Cox, ML Miller, JA Bloom, Digital Watermarking (Morgan Kaufmann, San Francisco, 2002)
3. GC Langelaar, I Setyawan, RL Lagendijk, Watermarking digital image and video data: a state-of-the-art overview. IEEE Signal Process. Mag. 17(5), 20–46 (2000)
4. IJ Cox, J Kilian, FT Leighton, T Shamoon, Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Process.6 (12), 1673–1687 (1997)
5. S Katzenbeisser, FAP Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking (Artech House, Boston, 2000)
6. CS Shieh, HC Huang, FH Wang, JS Pan, Genetic watermarking based on transform domain techniques. Pattern Recognit.37, 555–565 (2004)
7. V Solachidis, I Pitas, Circularly symmetric watermark embedding in 2-D DFT domain. IEEE Trans. Image Process.10, 1741–1753 (2001)
8. P Tao, A Eskicioglu, A robust multiple watermarking scheme in the discrete wavelet transform domain. Proc. SPIE5601, 133–144 (2004)
9. MA Akhaee, SME Sahraeian, F Marvasti, Contourlet-based image watermarking using optimum detector in a noisy environment. IEEE Trans. Image Process. 19(4), 967–980 (2010)
10. EJ Candes, DL Donoho, New tight frames of curvelets and optimal representations of objects with C2 singularities. Commun. Pure Appl. Math. 57(2), 219–266 (2004)
11. EJ Candès, L Demanet, DL Donoho, L Ying, Fast discrete curvelet transforms. SIAM Multiscale Model. Simul.5 (3), 861–899 (2006)
12. HY Leung, LM Cheng, LL Cheng, A robust watermarking scheme using selective curvelet coefficients. Int. J. Wavelets Multiresolution Inf. Process. 7(2), 163–181 (2009)
13. P Tao, S Dexterb, AM Eskicioglu, Robust digital image watermarking in curvelet domain, in Proc. SPIE, Security, Forensics, Steganography, and Watermarking of Multimedia Contents, ed. by (, 2008). 6819, 68191B–68191B-12
14. IJ Cox, J Kilian, FT Leighton, T Shamoon, Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Process.6 (12), 1673–1687 (1997)
15 Borie J., Puech W., Dumas M., "Crypto-Compression System for Secure Transfer of Medical Images", 2nd International Conference on Advances in Medical Signal and Information Processing (MEDSIP 2004), September 2004.
16 Tarish A.H., "Designing and implementation a stream cipher cryptography system", MSc. Thesis, Computer Science Department, University of Technology, 2000.
17 Pommer A.,"Selective Encryption of Wavelet-compressed Visual Data", PhD. Thesis, Department of Scientific Computing, Salzburg University, Austria, June 2003.


**BIODATA**

Aruna Varanasi presently working as Professor Head of Department of Computer Science and Engineering(CSE),Sreenidhi Institute of Science and Technology(SNIST),Hyderabad,India.She was awarded "Suman sharma" by Institute of Engineers(India),Calcutta for Securing highest marks among women in India in AMIE course.

G YAMINI Pursuing M.tech in software Engineering from Sreenidhi Institute of Science and Technology(SNIST),Hyderabad, India.