Non Oblivious Watermarking Technique for *JPEG*2000 Compressed images using Arnold Scrambling of Unequal Size Watermark Blocks

Geeta Kasana[1], Kulbir Singh[2], Satvinder Singh Bhatia[3]

[1]Computer Science and Engineering Department, Thapar University Patiala, India.
[2] Electronics and Communication Engineering Department, Thapar University, Patiala. India.
[3]School of Mathemetics, Thapar University, Patiala, India.
Email: gkasana@thapar.edu

Abstract:-*In this paper, a watermarking technique for JPEG2000 compressed image is proposed. Scrambling of secret message is performed block-wise using Arnold Transform.Secret message is divided into non-overlapping blocks of unequal size and then Arnold transform is applied on each block and secret key is generated based on the periodicity of each block.Scrambled secret message is embedded into qualified significant wavelet coefficients of a cover image. After embedding the secret message into wavelet coefficients, the remaining processes of JPEG2000 standard are executed to compress the watermarked image at different compression rates. Scaling Factor (SF) is used to embed watermark into wavelet coefficients and the value of SF is stored into COM box of the code stream of JPEG2000 compressed image and this SF value and secret key are used to extract the embedded watermark on the receiver side. The performance of the proposed technique is robust to a variety of attacks like image cropping, salt and pepper noise, and rotation. Proposed technique is compared with the existing watermarking techniques for JPEG2000 compressed images to show its effectiveness.*

***Key-Words*:** *JPEG2000, DWT, Arnold Transform, EBCOT, SF, COM*

I. INTRODUCTION

Recent years have witnessed the rapid development of the Internet and telecommunication techniques. Due to these developments, it has been possible to exchange large amount of data/information over a wide range of public networks. However, information transmitted through these networks may not be safe. For this purpose, information security techniques are used. Information hiding is onebranch of information security, whichhides the existence of information in a media such as digital image, videos and audios, *etc.* and then transmitted to the receiver where the authenticated user can extract the hidden data. Digital watermarking is one branch of information hiding which is used to authenticate the owner of a digital media.

*JPEG*2000 is the new state of art image and video compression standard. It provides excellent performance and novel features such as superior low bit rate compression performance, lossless and lossy compression, progressive transmission, region of interest coding, error resilience and random code stream access etc. as compared to older image compression standards (Taubman and Marcellin, 2000; Christopoulos*et al.*, 2000; Su *et al.*, 2001). Development of techniques for protecting the owner's rights to a *JPEG*2000 compressed images has received devotion from research community. Several steganography and

17

watermarking algorithms for *JPEG*2000 image have been proposed. Hsieh *et al.*, (2001) proposed a watermarking algorithm using wavelet transform. In their approach, an original image is decomposed into wavelet coefficients. Then watermarking scheme based on the qualified significant wavelet tree is used to hide the watermark. Seo*et al.,*(2001) proposed a watermarking scheme in which the watermark is inserted into coefficients obtained from ongoing process of lifting scheme for discrete wavelet transform (*DWT*). Su *et al.*, (2003) proposed a steganography scheme to embed secret data into *JPEG*2000 bit stream. This bit stream is the output of the *Tier*-2 process of the *JPEG*2000 coder.Thomos*et al.*, (2004) presented a sequential decoding of convolutional codes for data hiding in *JPEG*2000 compressed images. Huang *et al.*, (2004) proposed a watermarking technique in which each pixel of watermark is embedded in the wavelet coefficients of the middle and low frequency of a block in an image.The technique casts watermarks in multi-energy level. Chen *et al.,*(2004) proposed a watermark scheme based on *JPEG*2000 codec. The proposed scheme applies torus automorphisms technique to break up and scramble a watermark. The scrambled watermark was embedded into the quantization wavelet coefficients before the *Tier*-1 and *Tier*-2 coding process of *JPEG*2000 coder. Makhloufi*et al.,(2006)* proposed a QIM watermarking combined with *JPEG*2000 images.

Fan *et al.,*(2007) proposed a dual watermarking scheme for *JPEG*2000. The robust pyramid watermark is embedded into the cover image by changing the wavelet coefficients according to the characteristics of wavelet transformation, region of interest, and Embedded Block Coding with Optimized Truncation (*EBCOT*) to protect the watermark. In steganographic algorithm proposed by Hai-ying*et al*., (2008) the secret message is embedded directly into the output of the *Tier*-2 process. Fan *et al.,* (2008) proposed a Region of Interest (ROI) based watermarking method for *JPEG*2000 images in which secret data is embedded into some selected region of the cover image. Zhang *et al.,* (2009) proposed a high capacity steganography scheme for *JPEG*2000 coder which uses bit plane encoding procedure twice to solve the problem due to bitstream truncation. The embedding points and their intensity are determined to increase the hiding capacity. Lim *et al., (*2009)introduced an algorithm that utilizes both *JPEG*2000 and robust watermarking for protection and compression of the medical images.Subramanyam*et a*l., (2012) mainly focused on watermarking of compressed encrypted *JPEG2000* images. In their algorithm, they considered the ciphered bytes from the least significant bit planes of

the middle resolutions, because inserting watermark in ciphered bytes from most significant bit planes degrades the image quality to a great extent. They study the impact on the quality of watermarking in the compressed-encrypted domain.Veni*et al*., (2013) proposed a watermarking scheme for patient medical image. They embed a gray–scale image into a color host image, in both red and blue components.Gayathri*et al., (2013)* proposed a digital watermarking using*RC*5 encryption on *JPEG*2000 images.

In this work, a secure and robust watermarking technique is proposed for *JPEG*2000 compressed images. In all existing techniques, scrambling of secret data is performed on the complete data one time only. Our observation is that if scrambling is performed on blocks of unequal size then it will be difficult for the unauthorized user to extract the real secret data as for each block, the periodicity is different and the user can only unscrambled the secret data if key for the block is known to him. Also, to show the robustness of the proposed technique, different types of attacks are performed on the watermarked images.

II.Overview of *JPEG*2000 Standard and Arnold Transform

Overview of *JPEG*2000 Standard

In image compression technique, the essential step is the domain transformation, which results in the decorrelation of pixels and the energy of the image is compacted into small number of coefficients. JPEG2000 is the new image compression standard (Taubman and Marcellin, 2000; Christopoulos*et.al.*, 2000). The discrete wavelet transform is the domain transform used in *JPEG*2000. *DWT* decomposes the image into *R*-level dyadic wavelet pyramid. For each level, *DWT* is applied twice, once row-wise and column-wise and hence four subbands are produced which are:
1. Horizontally and vertically low-pass (*LL*)subband
2. Horizontally low pass and vertically high-pass (*LH*)subband
3. Horizontally high-pass and vertically low-pass (*HL*)subband
4. Horizontally high-pass and vertically high-pass (*HH*)subband

Let us consider the input image as LL_0 band. When *DWT* is applied on LL_0 band, it is decomposed into LL_1, LH_1, HL_1, and HH_1 bands. At next level, as shown in Fig. 1, $LL_1$is further decomposed into LL_2, LH_2, HL_2, and HH_2 bands. This process is repeated until the image is decomposed upto the required level. A two level wavelet decomposition of the image Lena, given in Fig. 2, is illustrated in Fig. 3.
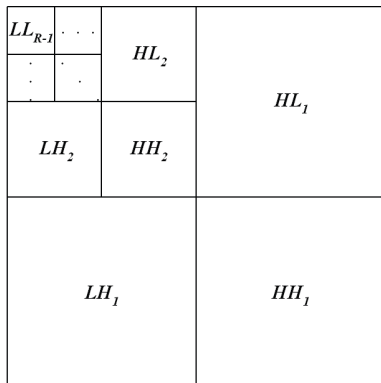
Fig. 1: *DWT* subband structure

Fig. 2: Lena Image

Fig.3: Lena image decomposed at 2 levels

After wavelet transforming an image, it can be represented using trees because of the subsampling that is performed in the transform. A wavelet coefficient in a low subband can be thought of as having four descendants in the next higher subband, as shown in Fig. 4. Each of the four descendants also has four descendants in the next higher subband. Due to this property, there is the quad tree in which each root has four children, as shown in Fig. 5.

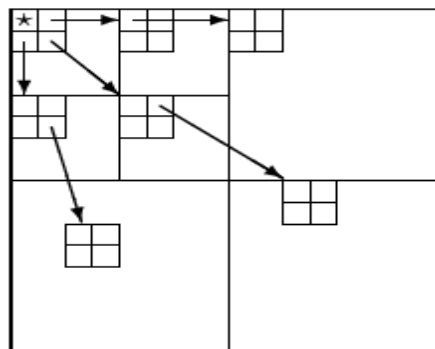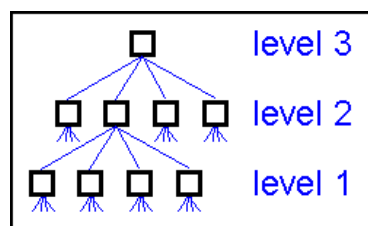**Fig. 4:** Parent child relationship of wavelet coefficients of image subbands.

Fig. 5: Each root has Four children

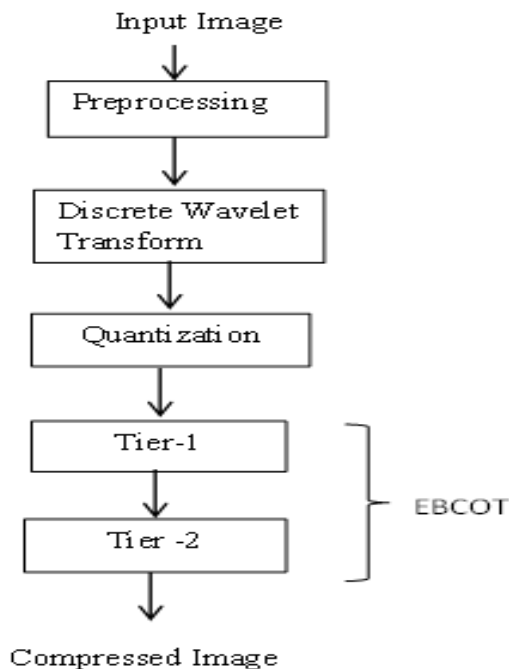*JPEG*2000 encoder consists of the following processes which are illustrated in Fig.6:

Fig. 6: *JPEG*2000 Encoder

19

1. Preprocessing is carried out on the source image. The examples of preprocessing are tiling and shifting of the origin of the image pixels to 0 by subtracting 128(in case of 8 bits image) from its each pixel value.
2. Irreversible or reversible color transform is applied on the preprocessed image to get the transformed image.
3. Lossy or lossless discrete wavelet transform is applied on the transform image. If the lossy compression is required then CDF9/7 wavelet filters are used. If the lossless compression is required then reversible integer to integer 5/3 wavelet filters are used.
4. Then the quantization is applied on the wavelet transformed image which decreases the size of the wavelet coefficients of the transformed image. Quantization is required in case of lossy image compression only.
5. *Tier*-1 coding, in which the quantized wavelet coefficients are partitioned into code blocks. Each code block is encoded using three passes which are significant propagation pass, refinement pass and cleanup pass.
6. *Tier*-2 coding, in which post compression rate distortion (*PCRD*) optimization is applied. The compressed data is converted into packets and these packets are combined to produce the final compressed image in *JPEG*2000 format.

Arnold Transform

Arnold Transform was proposed by V. J. Arnold (Huang and Yang, 2004). It is defined by the following equation:

$$\begin{pmatrix} x^{'} \\ \end{pmatrix}$$

where *mod* is modulo operator, (*x, y*) are the coordinates of the original image pixel, $\begin{pmatrix} x^{'}, y^{'} \end{pmatrix}$ are the coordinates of the scrambled image pixel, *N* is the image size. The transform changes the position of image pixels, and if it is done several times, a disorder image is generated. It preserves the confidentiality of the data.

In proposed technique, Arnold transform is applied on blocks of the secret image where all blocks are of unequal size. In Arnold transform based watermarking techniques, Arnold transform is performed on the complete secret image one time, but it does not make secret message secure as if an unauthorized user

succeed in getting the period of the Arnold transform then he can extract/destroy the whole message if he knows the embedding procedure and this will defeat the objective of watermarking/data hiding. In order to make the embedding of watermark more secure, secret message is divided into unequal size blocks and then each block is scrambled using Arnold transform. Secret key is then generated using the periodicity of each block.

When making digital images scrambling by Arnold transformation, it is important to know the periodicity of transformation. It is more secure due to more randomness. The decryption of an image depends on transformation periodicity. Periodicity changes in accordance with size of image/blocks.

III. Proposed Technique

Proposed technique has two algorithms- one is used to embed secret data and other is used to extract the embedded secret data. Steps of the embedding algorithm are also shown in Fig. 7.

Embedding Algorithm

1. The original image is decomposed using *DWT*upto*r* levels. This decomposition produces $3 \times r + 1$ subbandsof the original image.
2. Apply Arnold transform on the unequal size blocks of watermark image to get the scrambled blocks of the secret image and generate the secret key using the periodicity required for each block.
3. Take the median of all subbands of original image and stored into$T_1, T_2, ..., T_{3\times +1}$.
4. For i = 1 to 3×(*r*-1*)* +1
   Compare the wavelet coefficients of subband*i* with*T* .
   If a coefficient is greater than T then find the largest child of this coefficient and store it into an array along with its spatial location. (Children of a wavelet coefficient are present in the next higher subband).
   End if.
   End of for loop.

5. Embed the confused Arnold data into the largest child coefficient of cover image using the following
   $B (m, n) = A (m, n) + \alpha * W (m, n)$;
   Where α is the scaling factor (SF), $W (m, n)$ is the scrambled secret image pixel, $A (m, n)$ is the array of largest child and $B(m, n)$ is the pixel of the watermarked image.
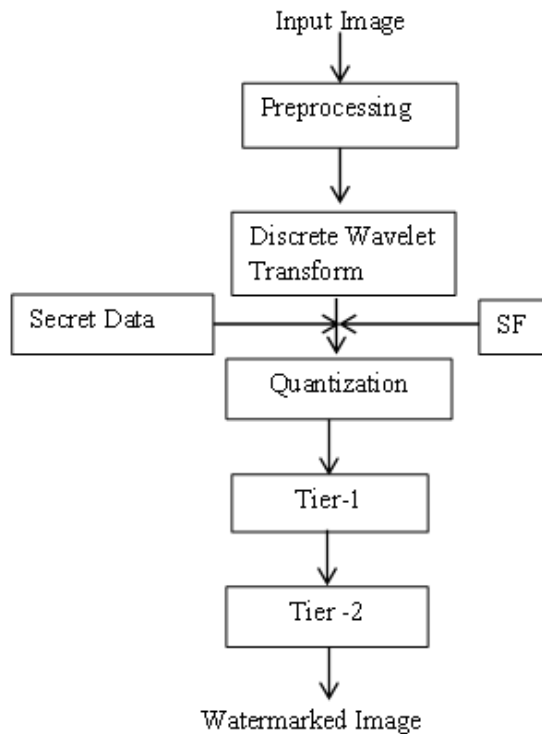
Fig. 7: Flowchart of Proposed Technique

Usage of Comment Marker:
*JPEG*2000 code stream is structured as a main header followed by a sequence of tile streams. There are many boxes in the main header which are used by the encoder as well as by the decoder. One of the boxes is Comment (*COM*) marker box which provides a facility for including unstructured comment information in the code stream of a compressed image when this image is compressed using *JPEG*2000 encoder. The *COM* marker segment is shown in Fig 8.*TY* parameter is a two byte unsigned integer. *TY*=1 indicates that the Comment Data comprises a sequence of bytes in the form of IS 8859-15:1999(Latin) character data. *TY* = 0 indicates general library Comment Data. No other values for *TY* are allowed in *JPEG*2000. The *COM* marker segment length satisfies 5<=L_{COM}<=65535. Here L_{COM} is the length of the box.

COM	L_{COM}	TY	Comment Data

Fig 8: *COM* marker of *JPEG*2000 Standard

In proposed technique, *COM* marker is used to store the value of *SF*and secret key which are used to extract on the receiver side. If user knows the exact values of *SF* and secret key then only he can extract the embedded data.This *COM* box is not used by the decoder so any value can be stored in this box.

Extraction Method
To extract the embedded watermark, original image is required so the proposed technique is non oblivious in nature. Also *SF* and secret key used on the embedding side, are also required to extract the watermark from a watermarked image.

1. To extract the watermark image, decompose the compressed watermarked image and original image upto*r* level.
2. Take the median of all subbands and store into T_1, T_2, ..., $T_{3 \times +1}$.
3. For *i* = 1 to 3×(*r*-1*)* +1
   Compare the wavelet coefficients of subband*i*with T .
   If a coefficient is greater than T then find the largest child of this coefficient and store it into an array along with its spatial location.
   End if.
   End of for loop.
4. Using the below equation, extract the secret data
   W'(m, n) = ((B(m, n) - A(m, n)) /α);
   where*A(m, n)* is the pixel of the original image and *B(m, n)* is the pixel of the watermarked image. The position of these pixels is stored into array constructed in the step 2. *α* is a scaling parameter
5. Divide the secret data *W'(m, n)*into blocks of the same order of different sizes using secret key and then apply Arnold Transform on each block to get the original secret blocks and then combine these blocks to get the secret image.

Three subbands of first level have no children. So the upper limit of *i* in the embedding and extraction is 3×*r* +1 – 3. i.e. 3×(*r*-1*)* +1.

Quality Parameters
PSNR(Peak Signal to Noise Ratio) is taken as a quality parameter in this work to evaluate the quality of the watermarked image. The *PSNR* is defined as

$$PSNR = 10log10 \frac{255^2}{S}$$

Where MS is the mean square error and is defined as

$$MS = \sum_{=1} \sum_{=1} \frac{n^- \quad n}{\times}^2$$

where   is the pixel of reconstructed image and   is the pixel of original image, ⏄ and w is the height and width of the images, respectively.

SIM (Similarity Index Modulation) between the original watermark image and extracted watermark

image is taken as an objective measure in this research work. *SIM* is defined as

$$SIM = \frac{\sum \sum_n , \times '(,)}{\sum \sum_n (,)^2}$$

where*W* is the original watermark image and *W'* is the extracted watermark image.
Correlation is given by the

$$r = \frac{\sum \left((x - \bar{x}) \times (y - \bar{y}) \right)}{\sqrt{\sum (x - \bar{x})^2 \times \sum (y - \bar{y})^2}}$$

IV. Experimental Results

For experimentation purpose, we considered few 512 × 512 gray images,Lena, Barbara, Boat and Pepper. Some of the watermarked and original images are shown in Fig. 9. The watermark image is logo gray image of size 32× 32. The watermark is embedded into these cover images using proposed technique. After embedding watermark, these cover images are compressed at different bit rates using KAKADU software. The *PSNR* of the watermarked images and *SIM*, correlation between original and extracted watermarkat different compression rates are given in Table 1.

Table 1:*PSNR* of different watermarked images and Correlation, *SIM* between watermark and extracted watermark at different bit rates

Bit rate (bpp)	1	2	3	4
Lena Image				
PSNR	35.6941	37.380	39.6661	39.6661
Correlation	0.9796	0.9921	0.9968	0.9968
SIM	0.8180	0.8778	0.9812	0.9812
Barbara Image				
PSNR	35.1831	38.4908	39.9787	39.9787
Correlation	0.9774	0.9929	0.9972	0.9972
SIM	0.7997	0.8928	0.9905	0.9905
Boat Image				
PSNR	35.1831	38.4908	39.9787	39.9787
Correlation	0.9774	0.9929	0.9972	0.9972
SIM	0.7997	0.8928	0.9905	0.9905
Pepper Image				
PSNR	35.6941	37.380	39.6661	39.6661
Correlation	0.9796	0.9921	0.9968	0.9968
SIM	0.8180	0.8778	0.9812	0.9812

From above table, one can conclude that when compression is higher (*i.e.*bpp is lower) *PSNR*of watermarked image decreases as compared to *PSNR* at lower compress rates. The table also shows that *PSNR* at higher compression ratios are acceptable by human visual system as it is higher than 30 dB(Hsieh, 2010)even at 1bpp. *SIM* and correlation between original watermark and extracted watermark are also acceptable when proposed technique is used to embed secret data.

a

b

c

d

Fig. 9 (a) Lena (rate=4bpp, *PSNR* 39.661 dB, extracted secret image *SIM* = 0.9812). **(b)**Lena (rate=2bpp, *PSNR* 37.380 dB, extracted secret image *SIM*=0.8778). **(c)** Barbara (rate=4 bpp, *PSNR* 39.97 dB, extracted secret image *SIM*=0.9905). **(d)** Barbara (rate=2bpp, *PSNR* 38.4908 dB, extracted secret image *SIM*=0.8928)

To study the robustness of the proposed technique, the following attacks are performed on the watermarked images.

Cropping attack: To perform this test, some portion(s) of the watermarked image are cropped. In the extraction process, the cropped part of an image was replaced by zero values. The cropped watermarked image is shown in Fig. 10(a). The watermark image is extracted from watermarked image after cropping

Fig. 10(a)cropped watermarked image attackat different compression bit rates. Calculated*SIM* and correlationbetween extracted watermark image from watermarked image after cropping attack and original watermarkimage at different compression bit rates are shown in Table 2.

Table 2: Correlation and *SIM* between extracted watermark from different watermarked images after cropping attack and original watermark at different compression bit rates

Rate	2	2	2	4	4	4
Crop	32x32	64x64	128x128	32x32	64x64	128x128
Lena Image						
Correlation	0.8833	0.8753	0.8038	0.8827	0.8722	0.9956
SIM	0.9456	0.9228	0.8582	0.9326	0.8673	0.8086
Barbara Image						
Correlation	0.9924	0.9656	0.8390	0.9962	0.9691	0.8152
SIM	0.9342	0.8592	0.8019	0.9802	0.7947	0.7407
Boat Image						
Correlation	0.8834	0.8890	0.8238	0.8478	0.8889	0.8867
SIM	0.9234	0.9121	0.9021	0.9001	0.8747	0.8546
Pepper Image						
Correlation	0.9956	0.9473	0.9065	0.8809	0.8629	0.8544
SIM	0.9923	0.9956	0.9023	0.8956	0.8902	0.8438

Fig. 10(b) watermarked image after noise attack

pepper noise. The watermarked image after noise attack is shown in Fig. 10(b).The watermark image is extracted from watermarked image after salt and noise pepper attack at different compression bit rates.*SIM and* correlation between extracted watermark image from watermarked image after salt and pepper noise attack and original watermark at different compression bit ratesis calculated and results are shown in Table 3. The extracted watermark image isvery much similar to its original version. The different noise ratios are used to distort the watermarked image.

Salt and pepper noise attack: To perform this test, the watermarked image was attacked by salt and

Table 3: Correlation and *SIM* betweenoriginal watermark and extracted watermark from watermarked image after salt and pepper noise attack at different compression bit rates

Rate	1	2	3	4	1	2	3	4
Noise	0.02	0.02	0.02	0.02	0.03	0.03	0.03	0.03
Lena Image								
Correlation	0.8995	0.9543	0.9070	0.9437	0.8837	0.9143	0.9110	0.8902
SIM	0.9336	0.8488	0.8678	0.8236	0.9366	0.9499	0.9192	0.8523
Barbara Image								
Correlation	0.9373	0.9282	0.9294	0.9651	0.8674	0.8896	0.8658	0.8938
SIM	0.9609	0.9988	0.8881	0.9392	0.9138	0.9766	0.8900	0.8563
Boat Image								
Correlation	0.9256	0.9132	0.9187	0.9589	0.8876	0.8789	0.8723	0.8954
SIM	0.9721	0.9987	0.8887	0.9343	0.9156	0.9745	0.8945	0.8569
Pepper Image								
Correlation	0.9123	0.9545	0.9167	0.9645	0.8670	0.9054	0.9003	0.8925
SIM	0.9487	0.9980	0.8898	0.9267	0.9254	0.8996	0.8965	0.8678

Rotation Attack: To perform this test, thewatermarked image was rotated by different angles at different compression bit rates. The watermark image is extracted from watermarked image after

rotation attack at different bit rates and calculated *SIM* and correlation between extracted watermark image and original watermark image are shown in Table 4.

Table 4: Correlation and *SIM* betweenoriginal watermark and extracted watermark from watermarked images after rotation attack at different compression bit rates

Rate	4	4	4	4	4	4	2	2	2
rotation	3	10	90	120	180	270	10	90	180
Lena Image									
Correlation	0.9157	0.9825	0.9968	0.9814	0.9968	0.9968	0.9620	0.9921	0.9921
SIM	0.8981	0.8993	0.9812	0.8108	0.9812	0.9812	0.8531	0.8778	0.8778
Barbara Image									
Correlation	0.8250	.09260	0.9973	0.9294	0.9973	0.9973	0.9116	0.9890	0.9890
SIM	0.8242	0.8922	0.9777	0.8339	0.9777	0.9777	0.8009	0.8803	0.8803
Boat Image									
Correlation	0.8342	0.9245	0.9968	0.9256	0.9970	0.9923	0.9635	0.9934	0.9934
SIM	0.8436	0.8926	0.9788	0.8479	0.9784	0.9823	0.8487	0.8643	0.8754
Pepper Image									
Correlation	0.9265	0.9762	0.9956	0.9810	0.9975	0.9978	0.9723	0.9821	0.9821
SIM	0.8984	0.8996	0.9823	0.8465	0.9845	0.9845	0.8653	0.8876	0.8876

From the above tables, one can conclude after cropping, salt and pepper noise and rotation attacks on watermarked image at different compression bit rates, one can extract the watermark which is relatively similar to the original watermark as *SIM* and correlation is near to 0.9. This shows that the proposed technique maintains the robustness.Proposed watermarking technique is compared with existing watermarking techniques for *JPEG*2000 compressed images and this comparison is given in Table 5.

Table 5: Comparison of watermark quality *SIM* with conventional methods on Lena image

Methods ⟶ Attacks ↓		Thomos*et al*.,(2004)	Makhloufi*et al.,(2006)*	Fan *et al.,(2008)*	Proposed Technique
Scaling	50%	0.59	0.73	0.71	0.75
Median Filtering	3x3	0.75	0.51	0.85	0.85
	5x5	0.62	0.73	0.74	0.80
Cropping	25%	0.80	0.84	0.89	0.90
	50%	0.68	0.72	0.77	0.80
Rotation	+15°	0.76	0.80	0.84	0.89
	-15°	0.76	0.80	0.84	0.89

To compare proposed technique, *SIM* between original watermark and watermark extarcted from watermarked image after attack, is taken as a paramter. From this comparison, one can observethat robustness is better than existing *JPEG*2000 watermarking techniques under different type of attacks.

V. Conclusion

Anon-oblivious watermarking technique for *JPEG*2000 images has been proposed in this work. The watermark is scrambled block-wise using Arnold transform in order to make it secure and is embedded into significant wavelet coefficients of the subbands of an original image. Experimental results have demonstrated that proposed technique is robust and secure, thus meets the requirements of watermarking. Since wavelet based *JPEG*2000 standard is the new image compression standard, protection of *JPEG*2000 compressed images is becoming important. The owner of *JPEG*2000 images can protect their images by adopting proposed technique.

References:

Chen, T.S., Chen, J. and Chen, J.G., (2004). A Simple and Efficient Watermark Technique Based on *JPEG2000* Codec. Multimedia Systems*,*10: 16-26.
DOI: 10.1007/s00530-004-0133-8
http://link.springer.com/article/10.1007%2Fs00530-004-0133-8
Christopoulos, C., Skordas, A. and Ebrahimi, T., (2000). The *JPEG2000* Still Image Coding System: *An Overview.* IEEE Transaction on Consumer Electronic, 46(4):1103-1127.
http://www.cs.cmu.edu/~guyb/realworld/paper_ieee_ce_jpeg2000_Nov2000.pdf

Fan, Y.C. and Tsao, H.W., (2007). A Dual Pyramid Watermarking for *JPEG2000.* International Journal of High Performance Computing and Networking, 5(2): 84-96.
DOI:10.1504/IJHPCN.2007.015767
Fan, Y.C., Chiang, A. and Shen, J.H., (2008). ROI based watermarking scheme for *JPEG2000*. Circuits System Signal Process*,* 27: 763-774.
DOI: 10.1007/s00034-008-9055-6
http://link.springer.com/article/10.1007%2Fs00034-008-9055-6
Gayathri, I. K. and Anil Kumar, M. N., (2013). Digital Watermarking Using RC5 Encryption on JPEG 2000 Images. International Journal of Engineering Research& Technology, 2(7): 1439-

25

1445.

http://www.ijert.org/view-pdf/4422/digital-watermarking-using-rc5-encryption-on-jpeg2000-images

Hai-ying G, Yin, X. Xu, L. and Guo-qiang, L., (2008). A Steganographic Algorithm for *JPEG2000* Image. International Conference on Computer Science and Software Engineering, pp: 1263-1266.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4723138

Hsieh M.S. Tseng, D.C. and Huang, Y.H., (2001). Hiding Digital Watermarks Using Multiresolution Wavelet Transform. IEEETransaction on Industrial Electronics*,* 48(5): 875-882.

http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=954550

Hsieh, M.S., (2010). A Robust Image Authentication Method Based on Wavelet Transform and Teager Energy Operator. The International Journal of Multimedia and Its Applications, 2(3):1-17.

http://airccse.org/journal/jma/0810ijma01.pdf

Huang, J. and Yang, C., (2004). Image Digital Watermarking Algorithm Using Multiresolution Wavelet Transform.IEEE Int. Conference on Systems, Man and Cybernetics*,* pp. 2977-2982;

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1400786

Kakadu software,

www.kakadusoftware.com

Lim, S.J., Moon, H.M., Chae, S.H., Chung, Y. and Pan, S.B., (2009). SSIR Paper *JPEG2000* and Digital Watermarking Technique Using Medical Image. IEEE International Conference on Secure Software Integration and Reliability Improvement, pp. 413-416.

Makhloufi, A., Zaid, A.O., Boualleg, R.B. and Boualleg, A., (2006). QIM watermarking combined to *JPEG2000* part I and II. 18th International Conference and Pattern Recognition*,* 3 pp: 746-749.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=16996

33

Seo, Y.S., Kim, M.S., Park, H.J., Jung, H.Y., Chung, H.Y., Huh, Y. and Lee, J.D., (2001). A Secure Watermarking for *JPEG*2000. IEEE*,* 530-533.

http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=958545

Su, P.C. and Kuo, C.C.J., (2003). Steganography in *JPEG2000* compressed images. IEEE Transactions on Consumer Electronics*.* 49(4): 824-832.

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1261161

Su, P.C., Wang, H.J.M. and Kuo, C.C., (2001). An Integrated Approach to Image Watermarking and *JPEG2000* Compression. Journal of VLSI Signal Processing,(27): 35-53.

http://mcl.usc.edu/wp-content/uploads/2014/01/200102-An-integrated-approach-to-image-watermarking-and-JPEG-2000-compression.pdf

Subramanyam, A.V., Emmanuel, S. and Kankanhalli, M.S.,(2012).Robust Watermarking of compressed and Encrypted *JPEG*2000 Images*.* IEEE Transactions on Multimedia*,* 14(3:703-716.

http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6112232

Taubman, D. S. and Marcellin, M. W., (2000). *JPEG2000: Image Compression Fundamentals, Standards and Practice,* Kulwer, Boston, MA.

Thomos, N., Boulgouris, N.V., Kokkinou, E. and Strintzis, M.G., (2004). Efficient data hiding in *JPEG2000* images using sequential decoding of convolutional codes. International Conf. Digital Signal Process, 2, pp: 717-720.

http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1028191

Veni, M., Eswaran, P., (2013). Robust Watermarking of Compressed and Encrypted *JPEG*2000 images. International Journal of Computer Trends and Technology, 4(6): 1717-1720.

http://ijcttjournal.org/Volume4/issue-6/IJCTT-V4I6P135.pdf

Zhang, L., Wang, H. and Wu, R., (2009). A High Capacity Steganography Scheme For *JPEG2000* Baseline System. IEEE Transaction on Image Processing, 18(8): 1797-1803.

http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4840534