Efficient Quality Access Control Scheme for Compressed Gray Scale Image using DWT via Lifting

Amit Phadikar[1], Santi P. Maity [2] Malay K. Kundu[3] ,

[1]Department of Information Technology, MCKV Institute of Engineering, Liluah, Howrah 711204, India.
[2]Department of Information Technology, Bengal Engineering and Science University, Shibpur, Howrah 711 103, India.
[3]Center for Soft Computing Research, Indian Statistical Institute, Kolkata 700 108, India.
(e-mail: amitphadikar@rediffmail.com, santipmaity@it.becs.ac.in, malay@isical.ac.in,)

Abstract—In object oriented and medical images, ROI (Region of Interest) is an area, which contains important information and attracts more attention of an image viewer. Thus protection of ROI at various qualities becomes an important issue for online access of images. This has made ROI as an important site for access control using multi resolution analysis (MRA). An attempt has been made here to serve this purpose through the development of a novel passive data-hiding scheme. The original image is decomposed into tiles by applying *n*-level lifting-based Discrete Wavelet Transformation (DWT). ROI of the image is found in frequency domain using a binary mask supplied by the owner of the image. The coefficients of k -level of detailed subbands, which belong to the ROI, are modulated by a secret key. These operations are collectively called here as passive data hiding in the wavelet coefficients and the necessary information is encrypted in the form of a secret key, which is used at the time of decoding. This results in the degradation of quality in ROI of the original image data, which becomes the key of access control through reversible process. Only the authorized persons having full knowledge of the secret key will be able to restore the full quality of ROI for the image. Simulation results duly support this claim.

Index Terms: Passive Data Hiding, Access Control, Security, Compressed Domain, ROI, Wavelet, Lifting.

1. INTRODUCTION

One of the driving forces for the emergence of World Wide Web (WWW) is due to the tremendous growth in digital technique that allows gross distribution of multimedia signals in digital form. Unfortunately such distribution creates a security problem because digital content can be easily edited or modified by certain software or tools. Moreover, for efficient transmission and storage purposes, digital media such as digital images are generally represented in their compressed form like JPEG, more recently JPEG 2000. Manufacturers and vendors have always two different objectives in their mind. They need to place their large volume of valuable works in the website for wide publicity and at the same time they want to restrict full quality access to the general users in order to maintain their commercial benefits. This has created a pressing demand to the manufacturers and the vendors to develop a quality access control scheme of compressed data, which allows all the receivers of the broadcast channel to display a low quality image with no or little commercial value. But in the meantime, the scheme also allows image access at higher quality levels depending on each receiver's access rights that usually are determined by the subscription agreement.

Research in access control is now in its very early stage and scrambling, cryptography and visual cryptography are the few widely used methods adopted either to deny or partial accessing of the media. Digital data hiding, although originally developed for copyright protection, ownership verification and authentication are now being used for access control due to commercial or security reasons [1]. In literature, active data hiding (popularly known as watermarking) is commonly used for former class of applications while the latter purpose is served by passive data hiding methods. Passive data hiding is a technique used for media identification where it is expected that signal distortions caused due to data hiding can be reverted by the authorized user to enjoy the full quality. Manipulation in the image for controlling its access to the different categories of users are generally guided by the content of the original image. Access control may find an important application in future generation mobile communication system where billing is expected to be performed based on the fulfillment of degree of quality of services (QoS).

We briefly review here few access control methods of digital images and video signals reported in the literature. *Grosbois et al.* [2] propose an authentication and two access control (on image resolutions and qualities) techniques of an image in wavelet domain that can be easily integrated in a JPEG 2000 codec, while remaining compliant with the standard. *Imaizumi et al.* [3] offer a new private-key encryption for JPEG 2000 code streams for flexible access control of layers, resolution levels and color components. *Chang et al.* [4] propose a structure to perform layered access control on scalable media by combining encryption and robust data hiding. *Mark et al* [5] suggest a blind data-hiding scheme in complex wavelet for access control of video where compliant DVD player deny access to the pirated copy of video. *Phadikar et al.* [6] recently propose a quality access control of gray scale image in DCT compressed domain.

The majority of the conventional DWT and DCT based access control schemes reported in the literature suffers form few shortcomings: (1) Protection of ROI is not taken into consideration during access control. It is to be noted that ROI of an image remains untouched from modification during many applications like coding and compression in order to preserve its essential value or importance. However, with reverse argument this image feature may be modified if the process is reversible leading to its application in access control. (2) Computational complexity. The other shortcoming is high computation complexity that makes the algorithms unsuitable for faster implementation. It is reported in the literature that compared to DCT (discrete cosine transform), conventional DWT has less computational cost. But in the case of an image having large size, it is still a problem when DWT applied to a whole image [7][8]. The issue becomes important as many algorithms in recent times demanded real time implementation for which hardware realization becomes a viable alternative. Lifting scheme is an effective method to improve the computation speed of conventional DWT as well for digital design. Integer wavelets transform allows to construct lossless wavelet transform, which is important for quality access control scheme. On the other hand though 80 % of image and video data are still available in DCT compressed form but future generation relies on DWT based coding technique. So development of cost effective access control for DWT compressed image and video become an important research issue.

The present work attempts to develop a quality access control scheme using ROI of an image in compressed domain by applying lifting based discrete wavelet transformation (DWT). Lifting technique is used to achieve lower computational complexity. The detailed DWT coefficients that lie within the area of ROI in an image are modulated by a key supplied by the user/owner. Those operations collectively are called here as passive data hiding in the DWT coefficients and the necessary information are encrypted in the form of a secret key which is used at the time of decoding. The simulation results show that the user having full knowledge of the key can recover ROI fully, while all other users can only access the ROI up to a certain level of quality.

The rest of the paper is organized as follows: Basic principles and key features of lifting are outlined in section II. Section III describes proposed access control scheme while in section IV the performance evaluation of the scheme is demonstrated. Conclusions are drawn in section V along with the scope of future works.

II. BASIC PRINCIPLES AND KEY FEATURES OF LIFTING BASED DWT

The lifting scheme is a technique for both designing fast wavelets and performing the discrete wavelet transform. The technique was introduced by Wim Sweldens. The discrete wavelet transform applies several filters separately to the same signal [9]. In contrast to that, for the lifting scheme the signal is divided like a zipper. Then a series of convolution-accumulate operations across the divided signals is applied. Generally speaking, lifting scheme includes three steps that are splitting, prediction and update. The basic idea of lifting is described here briefly[10]:

Split: The original signal is divided into two disjoint subsets. Although any disjoint split is possible, we will split the original data set $x[n]$ into $x_e[n]= x[2n]$, the even indexed points and $x_o[n]= x[2n+1]$, the odd indexed points.

Predict: The wavelet coefficients $d[n]$ is generated as error in predicting $x_o[n]$ from $x_e[n]$ using prediction operator P.

$$d[n] = x_o[n]-P(x_e[n]) \tag{1}$$

Update: $x_e[n]$ and $d[n]$ are combined to obtain scaling coefficients $c[n]$ that represent a coarse approximation to the original signal $x[n]$. This is accomplished by applying an update operator U to the wavelet coefficients and adding the result to $x_e[n]$:

$$c[n]=x_e[n]+ U(d[n]) \tag{2}$$

These three steps form a lifting stage. Iteration of the lifting stage on the output $c[n]$ creates the complete set of DWT scaling and wavelet coefficients $c^j[n]$ and $d^j[n]$. At each scale we weight the $c^j[n]$ and $d^j[n]$ with k_e and k_o respectively as shown in Fig. 1. This normalizes the energy of the underlying scaling and wavelet functions.

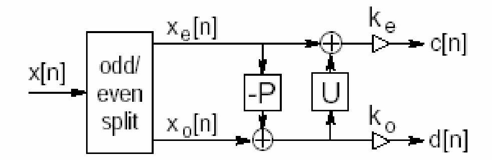

Fig. 1: Lifting steps

The lifting steps are easily inverted even if P and U are nonlinear, space-varying, or noninvertible. Rearranging equation (1) and (2) we have

$$x_e[n]=c[n]-U(d[n]),\ x_o[n]=d[n]+ P(x_e[n]) \tag{3}$$

The original signal will be perfectly reconstructed as long as the same P and U are chosen for the forward and inverse transforms. The inverse lifting stage is shown in Fig. 2.

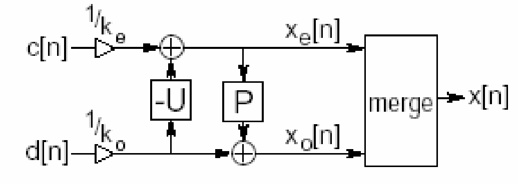

Fig.2: Typical inverse lifting steps

Lifting scheme has several advantages over classical wavelet based transform and are described below [11].

- Easy to understand and implement.
- Faster(x2, but still O (n), where n is length of signal).
- Inverse transform is easier to find.

- Inverse transform has exactly the same complexity as the forward transform.
- Transforms signals with an arbitrary length (need not be 2^n, where n is length of signal)
- Requires less amount of memory.
- All wavelet filters can be implemented using the lifting scheme.
- Simple extensions to an integer transform possible.

In recent section describe lifting based low complexity quality access control scheme of an image developed here.

III. PROPOSED ACCESS CONTROL SCHEME

The proposed access control scheme consists of two modules, namely, image encoding and image decoding. The encoding module basically performs *compression, modulation* and *symbol encoding* while the decoding module does the reverse operations i.e. *symbol decoding, demodulation* and *decompression*. The detailed block diagram representation of the image encoding and image decoding are shown in Fig. 3 and Fig. 4.

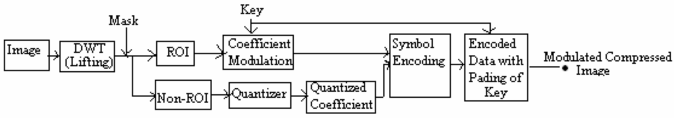

Fig. 3: Block diagram of quality access control encoding process.

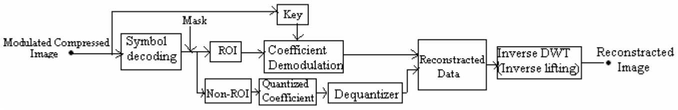

Fig. 4: Block diagram of quality access control decoding process.

A. *Image Encoding Process*

The image encoding process consists of the following steps:

Step 1: Image Pre-processing

The pixel values of the original image are level shifted by subtracting 2^{m-1}, where *'m'* is the number of bits required to represent the gray level of the image.

Step 2: Image Transformation

Lifting-based *n*-level 2D-DWT is performed on the original image and on the binary mask supplied by the owner/user. Fig 7(d) shows the mask generation in wavelet domain.

Step 3: ROI coding

Depending on the mask supplied by the user, ROI is calculated using Generic ROI Mask Generation method, which is used in JPEG2000.

Steps 4: Quantization of Wavelet Coefficients

Each of the transform coefficients $a_b\ (u,\ v)$ of subband *'b'*, which lies outside of the ROI, is quantized to the value $q_b\ (u,\ v)$ using the following rule [12].

$$q_b(u,v) = \text{sign}(a_b(u,v)) \left\lfloor \frac{|a_b(u,v)|}{\Delta_b} \right\rfloor \qquad (4)$$

The quantization step size Δ_b is

$$\Delta_b = 2^{R_b - \varepsilon_b}\left(1 + \frac{\mu_b}{2^{11}}\right) \qquad (5)$$

Where R_b is the nominal dynamic range of subband b, ε_b and μ_b are the number of bits allotted to the exponent and mantissa of the subband's coefficients

Step 5: Owner/User Define Key and its Significance

Owner/user of the image has to give a master key (*K*) of length *'L'* bit to the system, which implies the number of level of wavelet subbands coefficients to be considered and the type of modulation to be performed on all detail subband's coefficients which are with in the ROI. Fig. 5 shows the key where *'k'* number of MSB (i.e. bit 2^{L-1} to 2^{L-k}) represent the number of levels of the detail subbands to be modulated. The rest of the bits in the key are used to denote the type of modulation to be performed on the coefficients, which lie in the ROI.

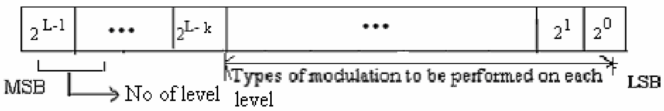

Fig. 5: L bit binary key used for modulation.

Step 6: ROI Coefficients Modulation

Depending on the key (*'K'*) supplied by the owner, the respective level of modulation is determined. The coefficients that lie in the area of ROI are modulated pseudo randomly according to the locally generated key based on *'K '*. The modulation is described by the following rule.

$$X^e = (-1)*X \qquad (6)$$

Where, X and X^e are the quantized DWT coefficients before and after modulation.

Step 7: Symbol Encoding

For efficient storage and transmission, all resulting coefficients (both within ROI and non-ROI) are Arithmetic and Huffman coded and the secret key *'K'* is padded at the end of the bit sequence.

B. *Image Decoding Process*

The decoding process is just reverse to that of the encoding process where input is the modulated compressed bit sequence. The steps for decoding process are described below.

Step 1: Key Extraction and Symbol Decoding

Key (*K*) is extracted from the end of the bit sequence and then both Huffman and Arithmetic decoding is done on the rest of the bits, to get the modulated quantized DWT coefficient.

Step 2: Separation of Coefficients into ROI and Non-ROI

Using the knowledge of the mask, DWT coefficients are separated into two group i.e ROI and non-ROI coefficients.

Step 3: ROI Coefficients Demodulation

Depending on the key extracted, the number of level to be demodulated is determined. The coefficients, which are within the ROI, are demodulated pseudo randomly according to locally generated key based on 'K '. The demodulation is described by the following rule.

$$X^{e1} = (-1) * X^{e} \qquad (7)$$

Where, X^{e} and X^{e1} are the quantized DWT coefficient before and after demodulation.

Step 4: Inverse Transformation

The image is reconstructed by performing the operations such as dequantization (only on the coefficients which are out side of the ROI), lifting-based inverse *n*-level 2D-DWT and inverse level shifting on the resulted quantized coefficients.

IV. PERFORMANCE EVALUATION

The performance of the proposed algorithm is tested over large number of bench mark images [13][14]. All of the test images are of size (512x512), 8 bit/pixel gray scale image and some of them are shown in Fig.6. The present study uses Peak Signal to Noise Ratio (PSNR)[12] and Structure Similarity Index (SSI)[15] as a distortion measure for the image under inspection with respect to the original image.

We decompose the test images into 3-level during our experimentation (see Fig.7(c)). Fig. 7(e) shows the decoded 'Lena' image (PSNR: 36.0286, SSI: 0.9271, bit rate 2.5241 bits / pixel, compression ratio 3.1695: 1), without quality access control mechanism. Table 1 lists the bit rate, compression ratio, and PSNR and SSI values for other test images.

Table1: Results of images without quality control mechanism.

Name of image	Bit rate(Bits / pixel)	Compression ratio	PSNR(dB)	SSI
Perer	2.4779	3.2285 : 1	35.2795	0.9025
Babbon	2.9558	2.7065 : 1	28.0731	0.8739
F161	2.5918	3.0866 : 1	35.5881	0.9438

A. Test With Key Having Different Level of Detail Subband Modulation

First two MSB of the key (*K*) represent the number of levels of detailed subbands used for modulation. Table-2 represents the respective type of modulation corresponding to each combination.

Table 2: List of different level of subband modulated for experiment.

First two MSB of the key	Type of modulation of coefficients in ROI	
00	No modulation	
01	Only detail coefficient of level-1	Case-1
10	detail coefficient of Level -1 and 2	Case-2
11	detail coefficient of Level 1,2 and 3	Case-3

Figs. 7(f), 7(h), 7(j) and 7(g), 7(i), 7(k): show the 'Lena' image, if ROI is decoded without and with the true key respectively for the different cases as mentioned above. It is seen that in all cases decoded ROI of 'Lena' images with the true key are of ultimate quality and images without the proper key produce a lower level of quality. In other words, images of Figs. 7(f), 7(h), and 7(j) will be available to all users but images of Figs. 7 (g), 7(i), 7(k) will only be available to the true users who have subscription agreement.

Table 3 lists the bit rate, compression ratio, PSNR and SSI values for various test images under different cases. Results show that in all test cases, modulation process do not increase any bit rate and is reverted completely so that full quality restoration of ROI in the inspected images is achieved.

Table 3: Results of images for different test cases if decoded without and with the true key.

Cases	Name of image		Lena	Perer
Case-1	Without key	PSNR(dB)	33.938	33.1159
		SSI	0.8993	0.8561
		Bit rate(bit/pixel)	2.5241	2.4779
		Compression ratio	3.1695 : 1	3.2285 : 1
	With key	PSNR(dB)	36.0286	35.2795
		SSI	0.9271	0.9025
Case-2	Without key	PSNR(dB)	30.5907	30.6199
		SSI	0.8509	0.8225
		Bit rate(bit/pixel)	2.5241	2.4779
		Compression ratio	3.1695 : 1	3.2285 : 1
	With key	PSNR(dB)	36.028	35.2795
		SSI	0.9271	0.9025
Case-3	Without key	PSNR(dB)	26.622	27.2310
		SSI	0.7909	0.7805
		Bit rate(bit/pixel)	2.5241	2.4779
		Compression ratio	3.1695 : 1	3.2285 : 1
	With key	PSNR(dB)	36.028	35.2795
		SSI	0.9271	0.9025

Cases	Name of image		Babbon	F161
Case- 1	Without key	PSNR(dB)	26.209	32.8751
		SSI	0.7989	0.9254
		Bit rate(bit/pixel)	2.9558	2.5918
		Compression ratio	2.7065 : 1	3.0866 :
	With key	PSNR(dB)	28.073	35.5881
		SSI	0.8739	0.9438
Case- 2	Without key	PSNR(dB)	24.875	28.7572
		SSI	0.7307	0.8777
		Bit rate(bit/pixel)	2.9558	2.5918
		Compression ratio	2.7065 : 1	3.0866 :
	With key	PSNR(dB)	28.073	35.5881
		SSI	0.8739	0.9438
Case- 3	Without key	PSNR(dB)	23.890	24.9368
		SSI	0.6883	0.8220
		Bit rate(bit/pixel)	2.9558	2.5918
		Compression ratio	2.7065 : 1	3.0866 :
	With key	PSNR(dB)	28.073	35.5881
		SSI	0.8739	0.9438

Fig 7(l) shows the 'Lena' image if it is decomposed by 4-level lifting transformation and all of the detail subband coefficients of ROI are modulated by the key. Figs. 7(m) and 7(p) show the decoded images respectively if the coefficients of ROI for different level of detail subbands are demodulated by the true key.

B. *Having No Knowledge of Key*

We also study our scheme under the consideration that if a user has no knowledge (brute force attacker) of the key and attempts to decode the entire detail subbands of the image with a random key. Figs. 7(q) and 7(t) show the respective images if the RIO of the picture is decoded using a random key. It is seen that in all cases the quality of ROI of the decoded picture is of poor quality than the picture if decoded by the true key. It means that only authentic user can avail better quality of the original one.

C. *Computational Complexity*

We examine the time that is taken in one whole procedure of encoding and decoding for quality access control of image to depict the computational complexity and also compare the computational load with the previous methods. We know that the computational load of conventional DCT and DWT are of O(n.log n) and O(n) respectively having a signal of length n. Feig [16] also pointed out, it only takes 54 multiplications to compute DCT for a block of size (8x8), unlike wavelet calculation depends upon the length of the filter used, which is at least one multiplication per coefficients. As all the previous access control schemes are based on conventional DWT or DCT, required high computational load. Our scheme is based on lifting-base DWT method that is two times faster (though complexity is O (n)) and requires less amount of memory. So the scheme is efficient for real-time implementation of quality access control scheme.

V. CONCLUSIONS AND SCOPE OF FUTURE WORKS

In this paper, a passive data-hiding scheme in compressed domain is proposed using lifting-base DWT and the method may be used as the access control of ROI at various qualities of an image. Experimental results show that valid users having the full knowledge of the key can restore the ROI, where all other users can access the ROI to a certain level. The scheme is simple, fast, cost effective and easy to implement. All these characteristics make the scheme a possible solution for digital right management. Future work will be concentrated on real time VLSI implementation of the scheme for image and video.

REFERENCES

[1]F.A.P.Petitcolas and H.J.Kim, Digital Watermarking, ISBN: 3540012176.

[2]R. Grosbois, P. Gerbelot and T. Ebrahimi, Authentication and Access Control in the JPEG2000 Compressed Domain, In Proceeding of SPIE 46th Annual Meeting, Applications of Digital Image Processing XXIV, San Diego, July 29th -August 3rd, 2001.

[3]S. Imaizumi, O. Watanabe, M. Fujiyoshi, and H. Kiya, Generalized Hierarchical Encryption of Jpeg 2000 Code streams for Access Control, In Proceeding of IEEE International Conference on Image Processing, 2000, Volume 2, 11-14 Sept. 2005 Page(s): II - 1094-7

[4]F.C. Chang, H.C. Huang and H.M. Hang· ,Layered Access Control Schemes on Watermarked Scalable Media, the Journal of VLSI Signal Processing(Springer Netherlands), ISSN-0922-5773, Published online: 28 June 2007.

[5]M. Pickering, L.E. Coria and P. Nasiopoulos, A Novel Blind Video Watermarking Scheme for Access Control Using Complex Wavelets, In proceeding of IEEE International Conference on Consumer Electronics, Jan. 2007, Las Vegas, NV.

[6]A. Phadikar, M.K. Kundu and S.P. Maity, Quality Access Control of a Compressed Gray Scale Image, In Proceeding of IEEE National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG 08), Gandhinagar, Gujarat, India. (Accepted).

[7]X. Wu, J. Hu, Z. Gu, J. Huang , A Secure Semi-Fragile Watermarking for Image Authentication Based on Integer Wavelet Transform with Parameters, In Proceeding of the 2005 Australian Workshop on Grid Computing And E-Research , Vol-44,New South Wales, Australia,Pp-75-80,2005.

[8] P.Meerwald and A.Uhl, A Survey of Wavelet-domain Watermarking Algorithms, in Proc. of SPIE, Electronic Imaging, Security and Watermarking of Multimedia Contents III, January 22 - 26, 2001, San Jose, CA, USA.

[9] http://en.wikipedia.org/wiki/Lifting_scheme

[10]R. L. Claypoole, R. G. Baraniuk, and R. D. Nowak, Adaptive wavelet transforms via lifting. In Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, 12-15 May 1998, Seattle, WA.

[11] G.Uytterhoeven, D. Roose, and A. Bultheel, Wavelet transforms using lifting scheme. Technical Report ITA-Wavelets Report WP 1.1, Katholieke Universiteit Leuven, Department of Computer Science, Belgium, April 1997.

[12] R.C. Gonzalez, R. E. Woods and S. L. Eddins, Digital Image Processing Using Matlab, Pearson Education, 2005.

[13] http://www.cl.cam.ac.uk/fapp2/watermarking.

[14]http://www.petitcolas.net/fabien/watermarking/image_database/index.html

[15] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, Image Quality Assessment: From Error Measurement to Structural Similarity, IEEE Transactions on Image Processing, vol. 13, no. 1, Jan. 2004.

[16] E., Feig. A fast scaled DCT algorithm, In Proc. SPIE Image Processing Algorithms and Techniques, vol. 1224, pp. 2-13, Feb. 1990.

(a) (b) (c) (d)

Fig. 6: Test images. (a) Lena; (b) Perer; (c) Babbon; (d) F161.

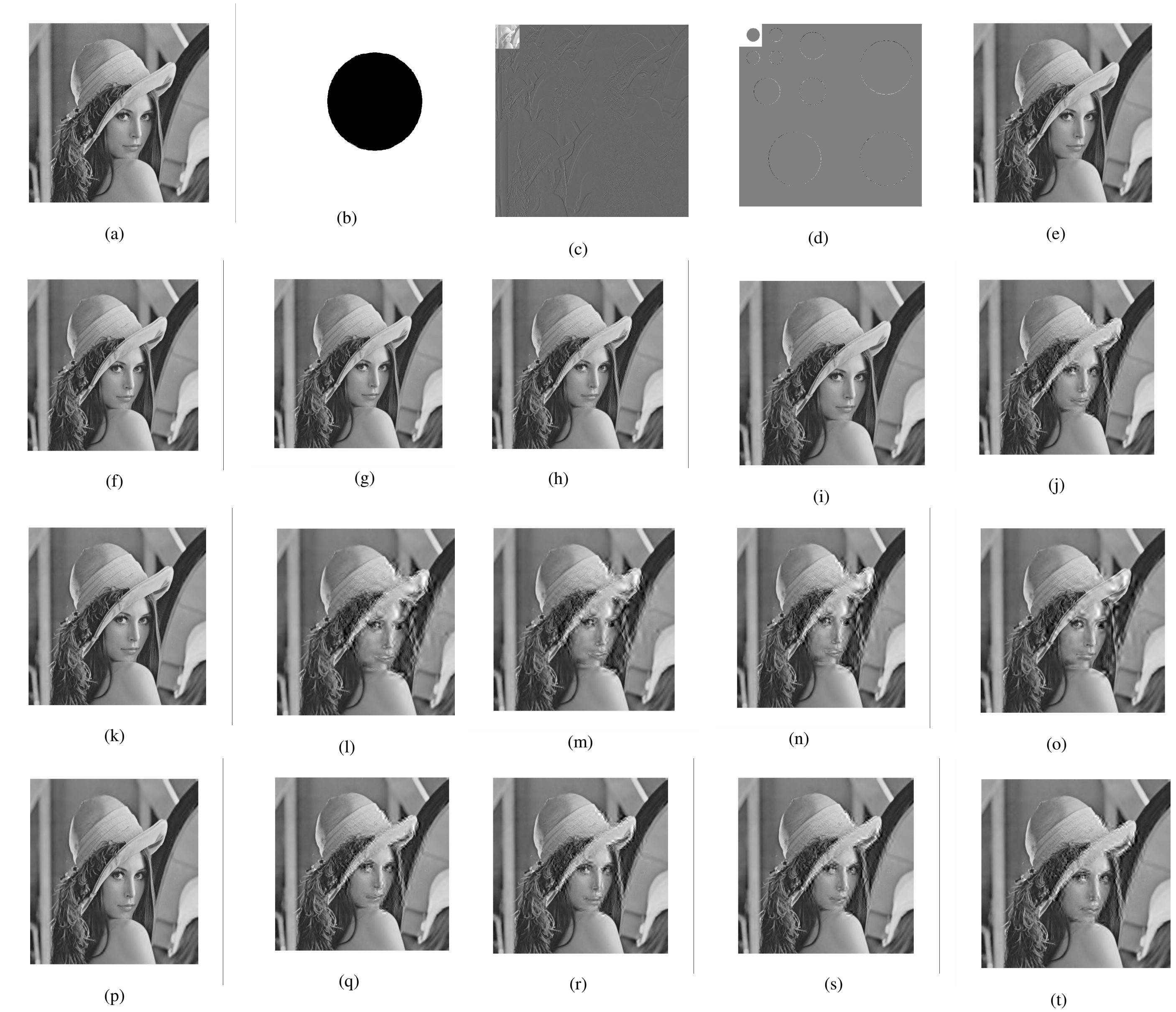

Fig. 7: (a) original image, (b) binary mask, (c) 3-scale lifting transformation of original image (a), (d) 3-scale lifting transformation of binary mask (b) , (e) decoded image without quality control scheme, (f) & (g): quality accesses control for case-1, (f) decoded image without key, (g) decoded image with the true key,(h) & (i): accesses control for case-2, (h) decoded image without key, (i) decoded image with the true key, (j) & (k): accesses control for case-3, (j) decoded image without key, (k) decoded image with the true key, (l)– (p): results when original image goes through 4-scale lifting transformation and all detail subbands are modulated, (l) decoded image without key(PSNR=23.8568,SSI=0.7381), (m) output when detail coefficients of level-1 are decoded with true key(PSNR=24.0257,SSI=0.7598) , (n) output when detail coefficients of level-1and 2 is decoded with true key(PSNR=24.5767,SSI=0.7951) , (o) output when detail coefficients of level-1,2 and 3 are decoded with true key(PSNR=26.6225,SSI= 0.8504) , (p) output when detail coefficients of level-1,2,3 and 4 are decoded with true key(PSNR=34.0996,SSI 0.9079). (q)-(t): Results if "Lena" image is decoded by different false (a random) key (for case-3), (q): decoded image with false key (1st try) (PSNR-26.7177 dB, SSI-0.7910),(r): decoded image with false key (2nd try) (PSNR-26.7145 dB, SSI-0.7898), (s): decoded image with false key (3rd try) (PSNR-*26.6689* dB, SSI-*0.7905*),(t): decoded image with false key (4th try) (PSNR-26.7415 dB,SSI-0.7918).