Quality Access Control of a Compressed Gray Scale Image

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

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

Abstract—**In this paper, we present a novel passive data-hiding scheme for quality access control of images in compressed domain. The original image is divided first into non-overlapping blocks. For each block, DCT coefficients are computed after using the standard quantization and normalization procedure of base line JPEG. If the number of nonzero AC coefficients of a block is greater than a predefined threshold (*T*), the coefficients are modulated. The amount of modulation is governed by the sign of the first '*n*' number of the coefficients and the amount of distortion on the quality of image to be allowed. These operations are collectively called here as passive data hiding in the AC 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 of the original image data. The coefficients found after modulation are Huffman coded for efficient storage and transmissions of DCT compressed image data. Only authorized persons having full knowledge of the secret key will be able to restore the full quality of the image. Simulation results duly support this claim.**

Index Terms: **Passive Data Hiding, Access Control, Security, Compressed Domain.**

1. INTRODUCTION

Now a days Internet has become a popular means for wide publicity of creative works and production of individual, government, semi-government, private and multinational organizations. This has been made possible through the revolution of digital techniques where different media can be distributed and transmitted easily and efficiently to the distant places using communication network and World Wide Web. Moreover, for efficient transmission and storage purposes, images are generally represented in their compressed form like JPEG. 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 that want to restrict full quality access to the general users in order to maintain their commercial aspects. This has created a pressing demand to the manufacturers and 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 in multiple levels. 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 discuss 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.

The review of the previous works reveals that it is the multiresolution attribute of wavelets that allows access control of the quality control of image and video signals along with the use of encryption technique. However, the multiresolution decomposition demands high computation complexity irrespective of the length of the wavelet filter coefficients which plays significant role in total computation burden. This computational complexity claims to be lower on DCT

compared to that of conventional DWT based implementation [6]. Moreover, there is one more point which may be mentioned in favor of DCT domain implementation. Although new standard like JPEG2000 has been introduced but in reality more than 80% of image and video data are still available in DCT compressed form. So cost effective access control for DCT compressed data of image and video is an important research issue.

The present work attempts to develop a quality access control scheme of image in compressed domain using discrete cosine transform (DCT). Quantized DCT coefficients of the original image are modulated and the amount of modulation is governed by the sign of the first 'n' number of the coefficients as well as the amount of distortion on the quality of image to be allowed. These operations are collectively called here as passive data hiding in the AC coefficients and the necessary information is 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 get the best copy (100% quality) of the image, while all other users can only access the image up to a certain level of quality.

The paper is organized as follows: Section II describes proposed access control scheme while in section III the performance evaluation of the scheme is demonstrated. Conclusions are drawn in section IV along with the scope of future works.

II. 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. 1 and Fig. 2.

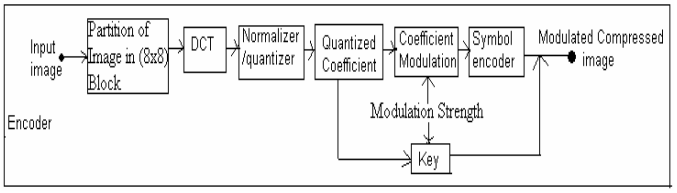

Fig. 1: Block diagram of quality access control encoding process.

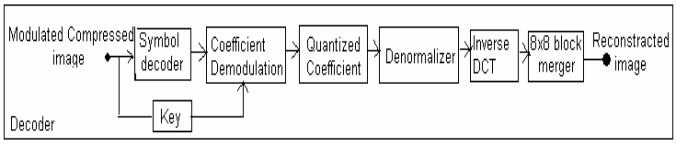

Fig. 2: Block diagram of quality access control decoding process.

II.I IMAGE ENCODING PROCESS

The image encoding process consists of the following steps:

Step 1: Partition of Host Image

Host image is partitioned into non-overlapping block of pixels with size (8x8). This particular block size is chosen in order to make the scheme compliant with the JPEG codec.

Step 2: Image Transformation

Pixel values of each block are level shifted by subtracting 2^{m-1}, where *'m'* is the number of bits required to represent the gray level of images. DCT is then performed over each block.

Steps 3: Quantization and Zigzag *Scanning of DCT Coefficients*

The resulting coefficients are normalized and quantized using standard quantization table used by baseline JPEG. The resulted quantized coefficients are reordered with the zigzag pattern.

Step 4: Bit Symbol Representation of AC Coefficients

Two bits are generated form the first two AC coefficients of each block according to the following rules described in Table-1.

Table-1: Generated bits depending on polarities of the first two AC coefficients

1st AC coefficient	2nd AC coefficient	Generated bits (binary representation)
Negative	Negative	00
Negative	Positive	01
Positive	Negative	10
Positive	Positive	11

The amount of the percentage coefficients to be modulated in a block is governed by the generated bits shown in Table-1and are of four categories denoted here by 15%, 30%, 45% 60% respectively. If the number of category of percentage (%) is increased, then more number of bits will be needed to represent and polarity of more number of AC coefficients need to be considered.

Step 5: Determination of Modulation Strength

Modulation strength is determined on the amount of distortion to be allowed on the quality of image. This is represented here by 3 bits, although one may use more number of bits in order to have a better access control. Modulation strength is determined by the decimal equivalent of these bit patterns. If modulation strength is increased, then amount of distortion on the quality of images are expectedly increased.

Step 6: Key Formation

A key is formed using bit patterns generated in step-4 and step-5. In the present scheme, the key is of 20 bits in length and is described in Fig. 3., where the value of *'a', 'b'* and *'c'* is either 0 or 1. However, the value of *'c'* can't be zero when both *'a' and 'b'* are '0' at a time.

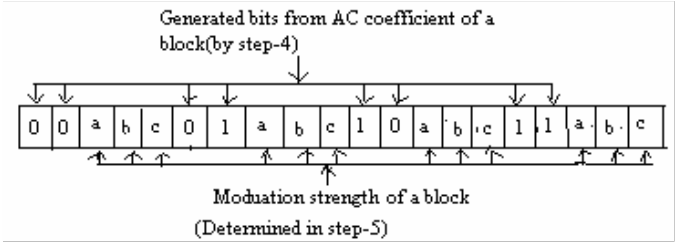

Fig. 3: 20 bit binary key used for modulation.

Step 7: Block Based Modulation

Depending on the bits generated from a bock (using step-4), percentage of coefficients *(say x)* are selected from the end-of-block (EOB). If the number of coefficients in a block is greater than a predefined threshold *(T),* then the selected coefficients are modulated pseudo randomly depending on locally generated key based on *'x'*. The modulation is described by the following rule.

$$X^e = (-1)*X* k \quad (1)$$

where, X and X^e are the quantized DCT coefficients before and after modulation. In the present scheme, the value of *' T'* is taken as 4. This means, if the number of AC coefficient in a block is less than 4, modulation is not done on that block. If we take the value of '*T*' below 4, then this will cause greater distortion in the images, as most of the energy of a block is concentrated near the DC coefficient. After block base modulation, the coefficients are Huffman coded and the key (found in step-6) is padded at the end of the bit sequence.

II.II IMAGE DECODING PROCESS

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

Step 1: Key Extraction and Huffman Decoding

Key is extracted from the end of the bit sequence and Huffman decoding is done on the rest of the bits, to get the modulated quantized DCT coefficient.

Step 2: Block Based Demodulation

Depending on two bits found form a block (as describe in step: 4 of encoding process) and the key extracted, percentage of coefficients*(x %)* and modulation strength *(k)* are determined. If the number of the coefficients in a block is greater than a predefine threshold *(T)*, *'x' % of the* coefficients are selected starting form the end-of-block (EOB) and is demodulated pseudo randomly depending on locally generated key based on *'x'*. The demodulation is described by the following rule.

$$X^{e1} = (-1)* X^e / k \quad (2)$$

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

Step 3: Inverse Transformation

Then reverse zigzag scan, denormalization and inverse DCT is performed on the resulted quantized coefficients found in step -2 to reconstruct the image.

III. PERFORMANCE EVALUATION

The performance of the proposed algorithm is tested over large number of bench mark images [7][8]. All of the test images are of size (512x512), 8 bit/pixel gray scale image and some of them are shown in Fig. 4. The present study uses Peak Signal to Noise Ratio (PSNR)[9] and Structure Similarity Index (SSI)[10] as a distortion measure for the image under inspection with respect to the original image.

Fig. 5(b) shows the decoded 'Lena' image (PSNR 35.7965 dB, SSI 0.9189, bit rare 0.63979 Bits / pixel, compression ratio 12.504:1), without quality access control mechanism. Table 2 lists the bit rate, compression ratio, PSNR and SSI values for three images.

Table 2: Results of images without quality control mechanism.

Name of image	Bit rate(Bits / pixel)	Compression ratio	PSNR(dB)	SSI
Perer	0.63291	12.64: 1	34.8166	0.8817
Babbon	1.3211	6.0557: 1	28.8383	0.8778
F161	0.68934	11.6053: 1	35.9814	0.9189

A. Test with Key Having Different Modulation Strength

We have tested all the images with a key having five different modulation strengths (*k*). Table-3 lists the different modulation strengths of the above five cases where case-1 and case-5 represent the lowest and the highest modulation strength respectively. Now let us explain how the different Cases are worked. Say for case-3 (table-3), if first two AC coefficients are negative i.e. generated bits are '00' (table-1) then value of *'k'* in equations (1) and (2) will be 2 (i.e. decimal equivalent of '010').

Table 3: List of different modulation strength used for experiment.

Watermark bits of a block	Modulation strength of the key				
	Case 1	Case 2	Case 3	Case 4	Case 5
00	001	001	010	011	100
01	001	010	011	100	101
10	001	011	100	101	110
11	001	100	101	110	111

Fig. 5(c, e, g, i, k) & (d, f, h, j, l): show the 'Lena' images, if they are decoded without and with the true key respectively for the different cases as discussed above . Fig. 6 & Fig. 7: show variation of PSNR and bit rate, graphically for the same.

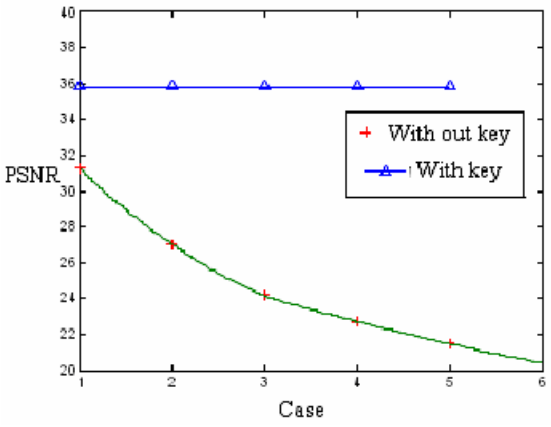

Fig. 6: Results of PSNR for different cases of a test image (Lena).

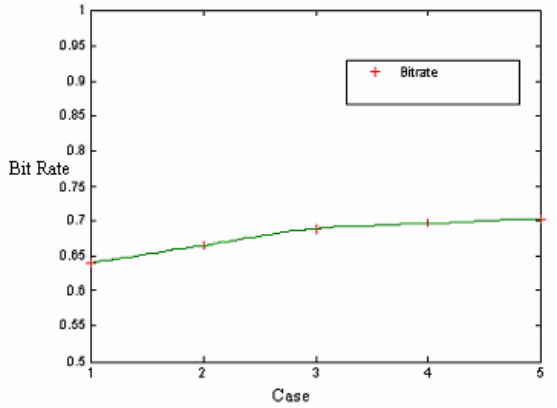

Fig. 7: Results of Bit rate for different cases of a test image (Lena).

It is seen from Fig. 6 that in all cases decoded 'Lena' images with the true key are of ultimate quality and images without the proper key produce a lower level of quality. That is images of Fig. 5(c, e, g, i, k) will be available to all users but images of Fig.5 (d, f, h, j, l) will only be available to true users who have subscription agreement.

From Fig. 7 it is seen that quality control process increase some bit rate in the coded data and the rate of growth depends on the rate of increase of modulation strength. So our aim will be to get the best modulation strength that will not cause large amount of increase in bit rate but performs the quality access control efficiently.

Table 4 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 is reverted completely and the full quality of images is achieved.

Table 4: Results of images modulated by key with different strength and decoded without and with the true key.

Modulat -ion strength	Name of image		Lena	Perer
Case- 1	With out key	PSNR(dB)	31.2942	29.1392
		SSI	0.8545	0.8568
		Bit rate(bit/pixel)	0.63979	0.86971
		Compression ratio	12.504 : 1	9.1985 : 1
	With key	PSNR(dB)	35.7965	34.8419
		SSI	0.9189	0.9419
Case- 2	With out key	PSNR(dB)	26.9760	23.4895
		SSI	0.7674	0.7232
		Bit rate(bit/pixel)	0.66444	0.9164
		Compression ratio	12.0401 : 1	8.7298 : 1
	With key	PSNR(dB)	35.7965	34.8419
		SSI	0.9189	0.9419
Case- 3	With out key	PSNR(dB)	24.1628	21.7458
		SSI	0.6947	0.6554
		Bit rate(bit/pixel)	0.68833	0.93199
		Compression ratio	11.6223 : 1	8.5838 : 1
	With key	PSNR(dB)	35.7965	34.8419
		SSI	0.9189	0.9419
Case- 4	With out key	PSNR(dB)	22.7242	20.2671
		SSI	0.6433	0.5930
		Bit rate(bit/pixel)	0.69608	0.94278
		Compression ratio	11.4929 : 1	8.4855 : 1
	With key	PSNR(dB)	35.7965	34.8419
		SSI	0.9189	0.9419
Case- 5	With out key	PSNR(dB)	21.4737	18.9901
		SSI	0.5981	0.5379
		Bit rate(bit/pixel)	0.70236	0.94817
		Compression ratio	11.3901 : 1	8.4373 : 1
	With key	PSNR(dB)	35.7965	34.8419
		SSI	0.9189	0.9419
Modulat -ion strength	Name of image		Babbon	F161
Case- 1	With out key	PSNR(dB)	25.0555	27.6226
		SSI	0.7426	0.8525
		Bit rate(bit/pixel)	1.3211	0.93196
		Compression ratio	6.0557 : 1	8.584 : 1
	With key	PSNR(dB)	28.8383	35.9814
		SSI	0.8778	0.9189
Case- 2	With out key	PSNR(dB)	19.9415	21.7850
		SSI	0.5340	0.7287
		Bit rate(bit/pixel)	1.3988	0.97829
		Compression ratio	5.7192 : 1	8.1776 : 1
	With key	PSNR(dB)	28.8383	35.9814
		SSI	0.8778	0.9189
Case- 3	With out key	PSNR(dB)	18.2436	20.0853
		SSI	0.4483	0.6694
		Bit rate(bit/pixel)	1.4216	0.99329
		Compression ratio	5.6274 : 1	8.0541 : 1
	With key	PSNR(dB)	28.8383	35.9814
		SSI	0.8778	0.9189
Case- 4	With out key	PSNR(dB)	16.7879	18.6409
		SSI	0.3782	0.6166
		Bit rate(bit/pixel)	1.4328	1.0037
		Compression ratio	5.5835 : 1	7.9703 : 1
	With key	PSNR(dB)	28.8383	35.9814
		SSI	0.8778	0.9189

Case- 5	With out key	PSNR(dB)	15.5231	17.3906
		SSI	0.3222	0.5708
		Bit rate(bit/pixel)	1.4392	1.0076
		Compression ratio	5.5588 : 1	7.9393 : 1
	With key	PSNR(dB)	28.8383	35.9814
		SSI	25.0555	27.6226

After studying the results of Table 4, we can conclude that the key of case -3 can be used for efficient access control as this compromise between quality control and bit rate, so that the scheme can be easily integrated in a JPEG codec. For the key in case-3, we test our scheme for other test images and various results are shown in Table 5 and Table 6.

Table 5: Results of images without quality access control mechanism.

Name of image	bit rate(Bits / pixel)	compression ratio	PSNR(dB)	SSI
Fishing boat	1.0367	7.7172 : 1	32.4445	0.9190
Cameraman	0.8402	9.5211 : 1	31.6328	0.9116
Kid	0.73772	10.8443 : 1	34.7704	0.9405
Opera	0.8663	9.2346 : 1	34.0795	0.9168

Table 6: Results of images modulated by the key (where modulation strength is as case-3) and decoded without and with the true key.

Name of image		Fishing boat	Cameraman
With out key	PSNR(dB)	20.3936	19.7496
	SSI	0.5935	0.6914
	Bit rate(bit/pixel)	1.1106	0.89359
	Compression ratio	7.2035 : 1	8.9527 : 1
With key	PSNR(dB)	32.4445	31.6328
	SSI	0.9190	0.9116
Name of image		Kid	Opera
With out key	PSNR(dB)	23.1987	22.1528
	SSI	0.6714	0.5822
	Bit rate(bit/pixel)	0.79166	0.9236
	Compression ratio	10.1054 : 1	8.6618 : 1
With key	PSNR(dB)	34.7704	34.0795
	SSI	0.9405	0.9168

B. Having No Knowledge of Key

We also study our scheme if a user has no knowledge (brute force attacker) of the key and attempts to decode the image with a random key. Fig. 8 shows the result if the picture is decoded by a random key. It is seen that in all cases the quality of the decoded picture is poor in than the quality of 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. Our scheme is in DCT domain which is fast and demands computation load in O(n. log n) operations where n indicates the signal length. The computational complexity of DWT is more compared to DCT. As Feig [11] pointed out, it only takes 54 multiplications to compute DCT for a block 8x8, unlike wavelet calculation depends upon the length of the filter used, which is atleast 1 multiplication per coefficients. As all the previous access schemes are based on DWT domain implementation, require more computational complexity compared to the present method which is based on DCT domain implementation.

IV. CONCLUSIONS AND SCOPE OF FUTURE WORKS

In this study, a passive image data hiding scheme in compressed domain is presented, which can control the access of the full quality of images. Experimental results show that valid users having the full knowledge of the key can get the ultimate quality of a picture, where all other users can get the images to a certain level. The scheme is simple and 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 the development of a scheme that can handle all types of color images.

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] 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.

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

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

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

[10] 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.

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

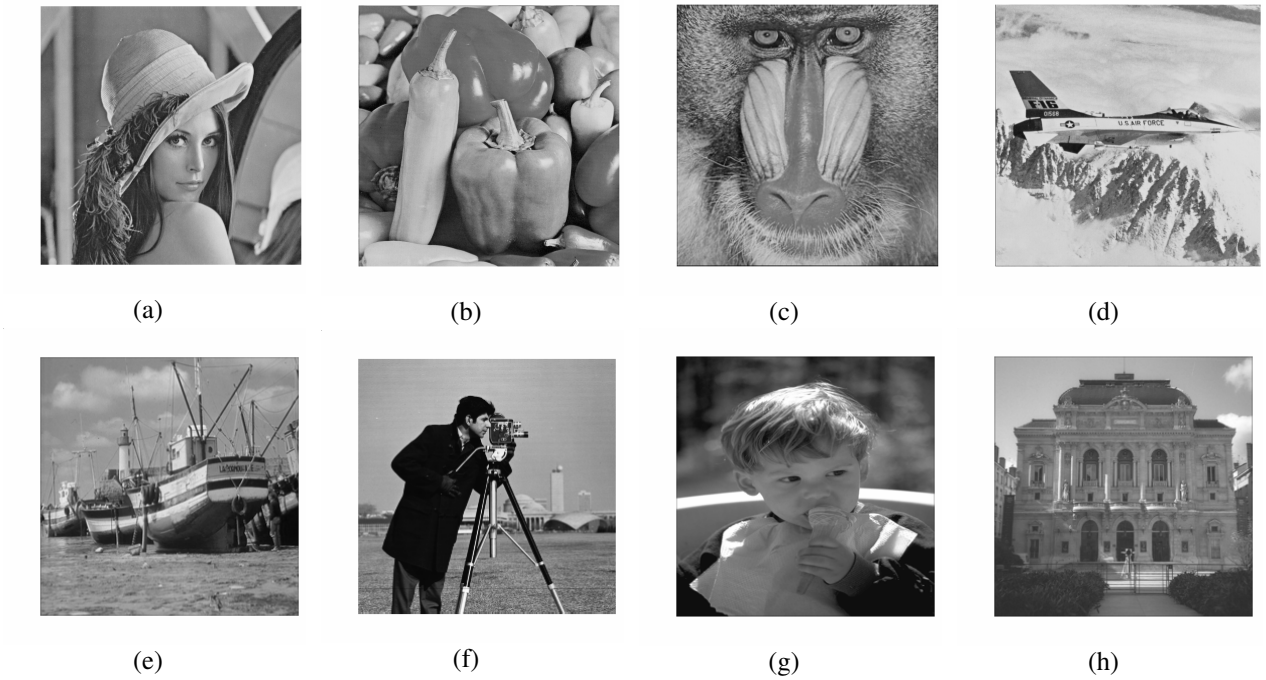

Fig. 4: Test images. (a) Lena; (b) Perer; (c) Babbon; (d) F161;(e) Fishing boat; (f) Cameraman; (g) Kid; (h) Opera.

(i) (j) (k) (l)

Fig. 5: (a) original image, (b) decoded image with out access control, (c) & (d): quality accesses control for case-1, (c) decoded image with out key, (d) decoded image with the true key, (e) & (f): quality accesses control for case-2, (e) decoded image with out key, (f) decoded image with the true key, (g) & (h): accesses control for case-3, (g) decoded image with out key, (h) decoded image with the true key,(i) & (j): accesses control for case-4, (i) decoded image with out key, (j) decoded image with the true key,(k) & (l): accesses control for case-5, (k) decoded image with out key, (l) decoded image with the true key.

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

Fig. 8: Results if "Lena" image is decoded by different false (a random) key (for case-3), (a): decoded image with false key (1st try) (PSNR-14.7515 dB, SSI-0.2773),(b): decoded image with false key (2nd try) (PSNR-14.7185 dB, SSI-0.2808), (c): decoded image with false key (3rd try) (PSNR-14.7096 dB, SSI-0.2771),(d): decoded image with false key (4th try) (PSNR-14.6784 dB,SSI-0.2808),