

Implementation of Transform Based Techniques in Digital Image Watermarking

Akhilendra Yadav
Electrical Engg. Deptt.
College of Engineering Roorkee
Roorkee, Uttarkhand
e-mail: akhil_amu@rediffmail.com

Nitin Chand
Electrical Engg. Deptt.
College of Engineering Roorkee
Roorkee, Uttarakhand
e-mail: nitin289chand@gmail.com

Abstract—Digital image watermarking is used to resolve the problems of data security and copyright protection. In many applications of digital watermarking, watermarked image of good quality are required. But here is a trade-off between number of embedded watermark images and quality of watermarked images. This aspect is quite important in case of multiple digital image watermarking. This project presents a robust digital image watermarking using discrete cosine transform (DCT) method. Compression on a watermarked image can significantly affect the detection of the embedded watermark. The detection of the presence or absence of a watermarked in an image is often affected if the watermarked image has undergone compression. Compression can also be considered as an attack on watermarked images. To show that a particular watermarking scheme is robust against compression, simulation is often relied

Keywords—Image compression, DCT, compression ratio, PSNR

I. INTRODUCTION

(A) IMAGE COMPRESSION

Image compression is an application of data compression that encodes the original image with few bits. The objective of image compression is to reduce the redundancy of the image and to store or transmit data in an efficient form. The main goal of general image storage system is to reduce the storage quantity as much as possible, and the decoded image displayed in the monitor can be similar to the original image as much as can be. The essence of each block will be introduced in the following sections. Image compression is used to minimize the amount of memory needed to represent an image. Images often require a large number of bits to represent them, and if the image needs to be transmitted or stored, it is impractical to do so without somehow reducing the number of bits. The problem of transmitting or storing an image affects all of us daily. Three techniques of image compression are pixel coding, predictive coding, and transform coding. The idea behind pixel coding is to encode each pixel independently. The pixel values that occur more frequently are assigned shorter code words (fewer bits), and those pixel values that are more rare are assigned longer code words. This makes the average code word length decrease. The image compression technique most often used is transform coding. A typical image's energy often varies significantly throughout the image, which makes compressing it in the spatial domain difficult; however, images tend to have a compact representation in the frequency domain packed around the low frequencies, which makes compression in the frequency domain more efficient and effective. Transform coding is an image compression technique that first switches to the frequency domain, then does its compressing. The transform coefficients should be decor related, to reduce redundancy and to have a maximum amount of information stored in the smallest space. These coefficients are then coded as accurately as possible to not lose

information.

(B) IMAGE WATERMARKING

Many watermarking algorithms are proposed in the literature. On the basis of working domains there are spatial domains and transform domains watermarking. Spatial domain method is simple and easy for implementation. These watermarking algorithms modify the pixel values of the original image where the watermarked is to be embedded, while in transform domain, host image is transformed using any transform method the modifications are made to the transformed coefficients. Transform domain watermarking techniques more robust in comparison to spatial domains method. To get more robust watermark against geometrical attack and jpeg compression is main issue in most of the watermarking algorithms. Due to the property of DCT, the DCT based digital image watermarking has replaced DWT based watermarking. DCT of the whole cover image is taken then segmented in to blocks for single value decomposition. Watermark image is scrambled using Arnold transform and then it is embedded in singular values. This not only improves the robustness but also security of the watermark. This helps in preserving the quality of watermarked image. To evaluate the algorithm, the DCT based watermarking is compared with the original image on the basis of the PSNR and robustness. Experimental evaluation shows that this algorithm is able to resist a variety of attacks including JPEG compression, different signal processing attacks and geometric attacks. Different features like robustness imperceptibility, secret key, and fragility are mentioned for a watermarking algorithm and watermarking is classified on different basis. A fragile watermarking is used for tempering detection. This helps in authentication of the data. There are two transform domain algorithm based on DWT and DCT. These algorithms are evaluated on the basis of PSNR and normalized correlation (NC) of the extracted watermark.

II. OBJECTIVES

During last two decades, with the growing of the digital communication, more popularity of the internet and the multimedia technology, users have been associated with multimedia data. Consequently it has been necessary to provide protection to the intellectual property rights of digital media. A number of text images, audios and videos are being transmitted over digital media on internet or any other public channel. Due to easy accessing of these contents there may be a chance that anyone can fetch of copy data and redistribute as duplicate copy of that content without permission of the owner. Some techniques for copyright protection should be used. Watermarking techniques is used to resolve the problem of copyright protection. Apart from copyright protection digital watermarking is also being used in many other applications like in meta-data insertion medical X-rays could store patient record. Many successful works have been completed on digital watermarking. Like watermarking is also used in tamper detection. In this application by embedding fragile watermarks digital data can be detected for tampering. If the fragile watermark is degraded destroyed then indicates the occurrence of tampering and consequently the digital content should not be trusted. Watermarking is classified into two categories spatial and transform domain. Spatial domain watermarking methods are earlier methods and easy for implementation but these techniques are not robust to attacks. In this method the set of pixels of the cover image are changed according to the watermark.

The objectives of this work include:

- (i) DCT based watermarking method is performed and compared on the basis of various performances parameters. Comparison has been made on the basis of the quality of extracted watermark from the noisy/attacked watermarked image in recovering algorithms.
- (ii) DCT based compression of the watermarked images is done and the compressed images are compared with the watermarked images.
- (iii) Extraction of the watermark and the host image is done after the process of compression and the obtained images are compared with the original images on the basis of various performance parameters.

III. PRINCIPLE

A watermarking system can be divided in to three stages embedding, distribution and extraction stages. A watermarking algorithm embeds the watermark in to the host image and generates the watermarked image. This watermarked image is then transmitted through medium or channel. Attacks make some modification in watermarked image but in case of robust watermark it is possible to extract watermark even after malicious attacks. A secret key provides security to watermarking system. The watermarking process may be dividing in three stages described below:

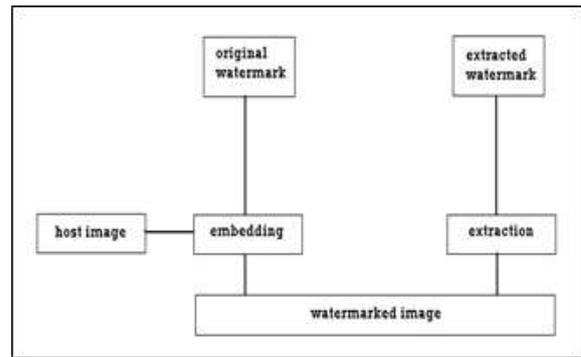


Figure1. Block diagram of a watermarking system

A. Embedding Stage

Embedding of watermarking can be done in two ways either directly or after transforming the host image using any of transform algorithms. Transform based watermarking involves changing the image to the desired transform. This includes the discrete cosine transform (DCT), the discrete Fourier transforms (DFT) and the wavelet transforms domains. The watermark to be embedded may be a bit stream, a binary image or a pseudo-random number that is to be placed in to host or cover image. The watermark image is then attached to the desire coefficients of the transform as recommended by human visual system (HVS) research. The watermarked image is the output of this process and is obtained by performing an inverse transform on the modified transform coefficients.

B. Distribution stage

The watermarked image obtained above is then distributed through digital channels. In this process, watermarked image in the channel may have undergone one of the several mappings, such as the image manipulations, compressions, and enhancement, etc. in addition, malicious attacks are also possible in this stage to degrade or destroy the watermark.

C. Extraction stage

In this sage, watermarking is having many properties. On the basis of that we can compare one method of watermarking to another. There are many properties of watermarking like transparency, capacity, robustness, security, imperceptibility etc.

IV. TECHNIQUE

A. Discrete Cosine Transform

A discrete cosine transform (DCT) expresses a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from lossy compression of audio (e.g. MP3) and images (e.g. JPEG) (where small high-frequency components can be discarded), to spectral methods for the numerical solution of partial differential equations. The use of cosine rather than sine functions is critical in these applications: for compression, it turns out that cosine functions are much more efficient (as described below, fewer functions are needed to approximate a

typical signal), whereas for differential equations the cosines express a particular choice of boundary conditions.

In particular, a DCT is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using only real numbers. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since the Fourier transform of a real and even function is real and even), where in some variants the input and/or output data are shifted by half a sample. There are eight standard DCT variants, of which four are common. The most common variant of discrete cosine transform is the type-II DCT, which is often called simply "the DCT" its inverse, the type-III DCT, is correspondingly often called simply "the inverse DCT" or "the IDCT". Two related transforms are the discrete sine transforms (DST), which is equivalent to a DFT of real and odd functions, and the modified discrete cosine transforms (MDCT), which is based on a DCT of overlapping data. Like any Fourier-related transform, discrete cosine transforms (DCTs) express a function or a signal in terms of a sum of sinusoids with different frequencies and amplitudes. Like the discrete Fourier transforms (DFT), a DCT operates on a function at a finite number of discrete data points. The obvious distinction between a DCT and a DFT is that the former uses only cosine functions, while the latter uses both cosines and sines (in the form of complex exponentials). However, this visible difference is merely a consequence of a deeper distinction: a DCT implies different boundary than the DFT or other related transforms.

The Fourier-related transforms that operate on a function over a finite domain, such as the DFT or DCT or a Fourier series, can be thought of as implicitly defining an extension of that function outside the domain. That is, once you write a function as a sum of sinusoids, you can evaluate that sum at any, even for where the original was not specified. The DFT, like the Fourier series, implies a periodic extension of the original function. A DCT, like a cosine transform, implies an even extension of the original function. However, because DCTs operate on finite, discrete sequences, two issues arise that do not apply for the continuous cosine transform. First, one has to specify whether the function is even or odd at both the left and right boundaries of the domain (i.e. the min-n and max-n boundaries in the definitions below, respectively). Second, one has to specify around what point the function is even or odd. In particular, consider a sequence abcd of four equally spaced data points, and say that we specify an even left boundary. There are two sensible possibilities: either the data are even about the sample a, in which case the even extension is dcbabcd, or the data are even about the point halfway between a and the previous point, in which case the even extension is dcbaabcd (a is repeated).

V. PROPERTIES

Digital watermarking is having many properties. On the basis of that we can compare one method of watermarking to another. There are many properties of watermarking like transparency, robustness, capacity, security, imperceptibility, etc

A. Transparency

This is the most fundamental necessity for any watermarking system. Watermarking system should be such that it is transparent to the user. The digital watermarking should not change original image after it is watermarked. "Transparency can be defined as the perceptual similarity between the watermarked image and host image". There should be no visible distortions.

B. Capacity

Capacity means the amount of information that is embedded into a host signal as a watermark to successfully recover during extraction. Watermark should be able to carry enough information. Different applications has different capacity requirement. Often, requirement of capacity always struggle against two important requirements, that is robustness and imperceptibility. So, there is a trade-off between capacity and either imperceptibility or robustness or both.

C. Robustness

Watermark robustness accounts for the capability of the message or watermark to detect watermark after common signal manipulations and different noise and attacks. Apart from malicious attacks, common signal processing operations can create a threat to the detection of watermark, thus there is a need to make such watermarking so that watermarking can survive those operations. For example, a good strategy for robustly embedding a watermark into an image is to insert into perceptually significant parts of the cover image. Not all watermarking applications require a watermark to be robust enough to survive all attacks and signal manipulations operations. Indeed, in an extreme case, 23 robustness may be irrelevant in some cases where fragility of the watermarking system is desirable.

D. Imperceptibility

The imperceptibility means the perceptual transparency or visual quality of the watermarked image. Ideally, there should not be any perceptible difference between the watermarked and original signal. The watermark should be embedded in the host signal in such a way that it cannot be seen. However, watermark invisibility may conflict with other requirements such as capacity or robustness or both.

E. Security

A watermarking technique will be secure if the algorithms for embedding and extracting the watermark do not help an unauthorized party to detect the presence of the watermark. Security of the watermarking algorithms needs a secret key which is to be used for embedding and extracting. In this case known values of coefficients, pseudo random sequence or any description may be used as a secret key. There are two way securities. In the first one, one needs secret key for extracting the watermark. In the second one unauthorized user cannot decode watermark without knowing decryption or decoding method.

F. Effect on Bandwidth

Watermarking should be done in such a way that it does not increase the required bandwidth for transmission of watermarked image. Watermarking should not become a burden for the available bandwidth; otherwise the method will be rejected.

VI. APPLICATIONS

There are many applications scenarios of watermarking. They can be classified in a number of different ways. The following classification is based on the information type, conveyed by the watermark. In the following section we will provide a more explanation of possible application scenarios involving watermarking.

- Copyright Protection
- Digital Fingerprinting
- Content Authentication
- Broadcast Monitoring
- Miscellaneous Applications

A. Copyright Protection

Copyright protections are the most important application of watermarking. A lot of information being transmitted over insecure networks daily, so copyright protection becomes a very prominent issue. Watermarking an image will stop redistribution of copyrighted images. Copyright protection is the first application for which the digital watermarking was targeted for. It is imperceptibly embedded as a watermark in the cover image. If users of digital content have an easy access to watermark detectors, they should be able to recognize and interpret the embedded watermark and identify the copyright owner of the watermarked content. A copyright owner distributed digital contents with invisible watermark embedded in it. In the case of a copyright ownership disputes, a legal owner has to prove his ownership by showing that the original work is his/her, and that the disputed work has been obtained from the original by inserting a watermark into it. This could be done by providing the original work together with the watermark detector to detect the owner's watermark in a disputed work.

B. Digital Fingerprinting

There are few applications where the more information associated with a digital content should contain information about the end user, rather than about the owner of the digital content. For example in a film making environment, the incremental works are often disputed every day to a number of people associated in a movie making activities. These are secret. If a version is disclosed then the studio would like to identify the source of that leak. The problem of identifying the source of a leak can be solved by distributing somewhat different copy to each recipient, thus associating uniquely watermark with each copy for person make the digital fingerprinting.

C. Content Authentication

Multimedia editing software programs make easy to modify digital content. Since it is also easy to interfere with a digital data, there is a requirement to verify integrity and authenticity of the data. Problem of tamper detection can be solved by using fragile watermarking. Watermarks can

obviously be used for embedding signature directly into the content. Since watermarks used for authentication of contents have to be designed to become invalid if even small modifications of digital contents take place. These types of watermarks are fragile watermarks. Fragile watermarks can also be used in applications where it is necessary to figure out how digital content was modified or which part of it has been tampered with.

D. Broadcast Monitoring

There are many valuable products which are regularly broadcast over the television network like news, sport movies, events, advertisements etc. broadcast time is very expensive, and advertisers pay hundreds of thousands of rupee for each run of their short commercial that appears during the breaks of important serials, movies or sporting events. To provide bill accurately in this environment it is more important. So advertisers who would like to make sure that they will pay only for the commercials which will actually broadcast. Broadcast monitoring is important for the performers in commercials who would like to ask for advertisers royalty payments accurately. It is usually used to collect information about the data being broadcast, and this information is used for billing as well as other purposes. This monitoring can be done by two types. First, by human observers who watch the broadcast and keep track of the entire see. This is expensive and erroneous. So automated monitoring is used. Watermarking can also be used as automated monitoring which is having major applications in commercial advertisements.

E. Miscellaneous Applications

i. Control Labelling

In content labeling information embedded in the data, comprise annotations which give some more information about the data. Examples are digital cameras takes images with the data and time, when the photograph was taken. Another example is medical imaging machines which annotate X-Rays images with patient's name, id.

ii. Usage Control and Copy Protection

In this application digital watermark is inserted to indicate the number of copies permitted. If a copy is made every time the hardware alters the watermark and at the same time it would not create any more copies of the data. In DVD technology this application is commonly used.

iii. ID card Security

Information in a passport or ID can also be included in the person's photo that appears on the ID. This information can be embedded as a watermark. Information written on the ID can be compared by extraction and this verifies the ID card. So the adhesion of the watermark can provide an additional level of security in this application. For example, if the ID is lost or stolen and the picture may be replaced by a forged copy, the failure in the extracting the watermark will invalidate that ID card.

VII. RESULT

In the Present scenario digital watermarking are used in several application for security purpose and the compression scheme DCT are used. Here we used different images with

watermark then compress using discrete cosine transform and Determine image parameters Compression ratio (CR), Mean square error (MSE), Peak signal noise ratio (PSNR) at different BPP.



Figure 2: Images of original, watermark, compressed watermarked image

Table 1: Compressed Images Parameters on Gray Scale

ORIGINAL IMAGE			COMPRESSED IMAGE(GRAY SCALE)				
Image No.	Size (KB)	BPP	SIZE(KB)	BPP	CR	MSE	PSNR
1	169	0.3526	93.8	0.5865	1.803	11.73	37.437
2	170	0.3791	97.4	0.6498	1.750	18.62	35.429
3	238	0.3390	120	0.5155	1.927	15.29	36.286
4	179	0.4484	54.8	0.4109	3.274	4.81	41.304
5	352	0.5045	88.4	0.3775	4.009	5.23	40.943
6	9.20	1.4950	7.28	1.183	1.263	2.568	44.034
7	181	0.3780	92.1	0.5760	1.968	13.45	36.842
8	213	1.4230	108	0.7201	1.976	18.82	35.381
9	70.4	0.7342	53.9	0.5623	1.305	9.571	38.320
10	435	2.7240	182	1.142	2.384	63.399	30.110

Table 2: Compressed Images Parameters on Color Scale

ORIGINAL IMAGE			COMPRESSED IMAGE(GRAY SCALE)				
Image No.	Size (KB)	BPP	SIZE	BPP	CR	MSE	PSNR
1	169	0.3526	106	0.2209	1.596	12.72	37.008
2	170	0.3791	113	0.2501	1.515	16.91	35.918
3	238	0.3390	144	0.2053	1.650	14.13	36.627
4	179	0.4484	59.8	0.1495	2.999	10.67	37.845
5	352	0.5045	101	0.1440	3.503	7.12	39.604
6	9.20	1.495	7.97	0.4320	1.514	30.24	33.320
7	181	0.3780	103	0.2147	1.760	12.55	37.140
8	213	1.423	127	0.2841	1.669	18.14	35.540
9	70.4	0.7342	57.7	0.1622	1.508	12.01	37.334
10	435	2.724	284	0.9080	1.532	47.50	31.363

VII. CONCLUSION

Digital watermarking is a rapidly growing area of research and development. In this paper an overview of Image compression and digital watermarking is presented. First of all we took a watermark image which was to be embedded into an image, then it is compressed using DCT algorithm and the noise introduced into the image is calculated.

After the first step, the watermark image is embedded into the original image and then this watermarked image is compressed using the same algorithm. Finally the watermark is extracted from the host image and the noise which is introduced into it in the process of watermarking and compression is compared to the reading in the first step. The results show that the image parameters of color as well as gray scale images approximate same. The readings are compared to ensure that the watermark is detectable even after the DCT compression. From our readings we can conclude that the DCT watermarking scheme has good durability to DCT compression. And it was robust against expected lossy compression.

VII. REFERENCES

- [1]. A.K.Jain, "Fundamentals of Digital Image Processing" , Second Edition, PHI, New Delhi, 2000.
- [2]. A.S. Tolba, "Wavelet packet compression of medical images", Digital Signal Processing, vol.12, pp. 441–470, 2002.
- [3]. Andras Cziho et al., "Medical Image Compression Using Region-of-Interest Vector Quantization", *Proc. of the 20th Annual Int. Conf. of the IEEE Engineering in Medicine and Biology Society*, vol. 20, No.3, pp. 1277-1280, 1998.
- [4]. Antonini M, Barlaud M, Mathieu P, Daubechies I, "Image coding using wavelet transform," *IEEE Trans.on Image Processing*,vol. 1, pp.205-220, April 1992.
- [5]. Askelof J., Carlander M., and Christopoulos C., "Region of interest coding in JPEG2000", *Signal Processing Image Communication*, vol.17, pp.105–111, 2002.
- [6]. B.Chanda and M.D.Dutta, "Digital Image Processing and Analysis" , First Edition, PHI, New Delhi, 2000.
- [7]. Brennecke R, et al., "Comparison of image compression viability for lossy and lossless JPEG and wavelet data reduction in coronary angiography", *Int. Journal of Cardiovascular Imaging*, vol. 17, Issue 1, pp.1-12, February 2001.
- [8]. C. Chang, T. Chen, L. Chung, "[A steganographic method based upon JPEG and quantization table modification](#)", *Elsevier: J. of Information Sciences*, vol.141, Issues 1-2, pp.123-138, March 2002.
- [9]. C. Christopoulos, A. Skodras and T. Ebrahimi, "The JPEG 2000 still image coding system: An overview", *IEEE Trans. on Consumer Electronics*, vol. 46, No. 4, pp 1103-1127, November 2000.
- [10]. C. Christopoulos, J. Askelöf and M. Larsson, "Efficient Methods For Encoding Regions of Interest in the Upcoming JPEG2000 Still Image Coding Standard", *IEEE Signal Processing Letters*, vol. 7, No. 9, pp. 247-249, Sept. 2000.
- [11]. C. Chrysafis, A. Ortega, "Line based, reduced memory, wavelet image compression", *IEEE Trans. Image Processing*. vol. 9, Issue 3, pp. 378-389, March 2000.
- [12]. Chien-Shun Lo et al., "Fractal Based JPEG2000 ROI Coding", *IEEE Int. Conf. on Systems, Man and Cybernetics (SMC '06)*, vol. 1, pp. 553 – 555, 8-11, Oct. 2006.
- [13]. Clunie D.A. et al., "Detection of discrete white matter lesions after irreversible compression of MR images", *American Journal of Neuroradiology*, vol. 16, pp. 1435-40. August 1995
- [14]. D. A. Huffman, "A method for the construction of minimum redundancy codes," *Proc. of the Institute of Radio Engineers*, vol. 40, pp.1098-1101, Sept.1952.
- [15]. D. Kramer, et.al. , "Comparison of wavelet, fractal and DCT based methods on the compression of prediction-error images", *Proc. of the Int. Picture Coding Symposium (PCS '97). ITG-Fachberichte*, VDE-Verlag, Berlin, vol. 143, pp. 393-397, 1997.
- [16]. D. S. Crus, T. Ebrahimi, M. Larsson, J. Askelöf, and C. Christopoulos, "Region of interest coding in JPEG2000 for interactive client/sever applications", *Proc.of IEEE 3rd Workshop on Multimedia Signal Process.*, pp.389–394, 1999.
- [17]. D. S. Taubman and M. W. Marcellin, "JPEG2000: Image compression fundamentals, standards and practice", Norwell, Massachusetts: Kluwer Academic Publishers, 2002.
- [18]. D.Taubman, Marcellin, M., "JPEG2000: image compression fundamentals, standards and practice", Springer, 2002.
- [19]. David Nister, Charilaos Christopoulos, "[Lossless region of interest coding](#)", *Elsevier: J. of Signal Processing*, vol. 78, Issue 1, pp.1-17, October 1999.
- [20]. Diego Santa-Cruz, Raphaël G. and T. Ebrahimi, "JPEG 2000 Performance Evaluation and Assessment", *Elsevier: J. of Signal Processing: 5278*

- Image Communication*, vol. 17, Issue 1, pp. 113–130, 2002.
- [21]. Frank Y.S., Yi-Ta Wu, “Robust watermarking and compression for medical images based on genetic algorithms”, *International Journal of Info. Sciences*, vol. 175, pp. 200–216, 2005.
- [22]. Good W.F. et al., “JPEG compatible data compression of mammograms”, *Journal of Digital Imaging*, vol. 7, Issue 3, pp.123-32, August 1994.
- [23]. Hung-Yam C., Hamed S., Bradley I.G., Shaun S.G., “Content-Based Compression of Mammograms with Fractal-based segmentation and a Modified JPEG 2000”, *Journal of Optical Engineering*, vol. 43, No. 12, pp. 2986–2993, Dec. 2004.
- [24]. I. Avcibas, et al., “A progressive lossless/nearlossless image compression algorithm,” *IEEE Sign. Proc. Letters*, vol. 9, no. 10, pp. 312–314, 2002.
- [25]. Jiang-Lung Liu, “[Efficient selective encryption for JPEG 2000 images using private initial table](#)”, *J. of Pattern Recognition*, vol.39, Issue 8, pp. 1509-1517, Aug 2006.
- [26]. Jurate P., Vytenis P., Jonas P., “[Ultrasound and angio image compression by cosine and wavelet transforms](#)”, *Int. Journal of Medical Informatics*, vol. 64, Issues 2-3, pp. 473-481, Dec.2001.
- [27]. K. Chen and T. V. Ramabadran, Near lossless compression of medical images through entropy coded DPCM,” *IEEE Trans. Med. Imag.*, vol. 13, no. 3, pp. 538–548, 1994.
- [28]. K. R. Rao and P. Yip, “Discrete Cosine Transform: Algorithms, advantages, applications”, Boston: Academic Press, 1990.