Novateur Publication's
International Journal of Innovation in Engineering, Research and Technology [IJIERT]
ICITDCEME'15 Conference Proceedings
ISSN No - 2394-3696

ROBUST DIGITAL IMAGE WATERMARKING BY USING DCT TECHNIQUE

Sanjeevani Subhash Kagade
Department of E&TC Engineering, TPCT COE, Osmanabad, India.

Sudhir S. Kanade
Department of E&TC Engineering, TPCT COE, Osmanabad, India.

ABSTRACT

Nowadays the internet and the personal computers becomes more popular because these are very easy to handle and use and being used in many fields for the transmission of most of the information in digital format. Due to the digital format transmission the copy write protection for this data is necessary in the World Wide Web and multimedia applications. The copyright protection and authentication generally loses their security of the data. Therefore it is necessary to protect the intellectual property in technical study and the research. Recently, most of the watermarking techniques are used to protect the intellectual property of the data. In this paper, an effective algorithm is present to embed the watermark into the host image by using DCT transform. There were many papers presented by using the same concept to embed watermark into the middle band coefficients of DCT blocks. But these papers have disadvantage that these are not computable for the Joint Photograph Expert Group (JPEG) image compression. The JPEG compression generally discards the high band frequencies in the DCT block it also includes some middle band data. In this paper the lower band coefficients of DCT blocks was employed, because it is robust against the attacks by the JPEG. In order to improve the imperceptions, only one bit was embedded in each coefficient of a DCT block. Finally, the experimental results show the proposed algorithm suitable for different image compression techniques like as JPEG, BMP, TIFF, GIF and PNG, etc.

INTRODUCTION

Nowadays, internet is an important part of our life. There are numerous types of digital data over the Internet, such as text, images, audio tracks, videos and 3D graphical objects etc. These are used more and more in industrial, medical and entertainment applications. Digital data is so widely used because it is easy to store, transfer and duplicate with high quality. However, the convenience also facilitates the access of malicious users to produce unauthenticated and pirate copies of the original work.

There are two typical digital data protection techniques: cryptography and watermarking. Cryptography completely changes the appearance of the data and as a result nobody would be able to decode the message without the secret key. Cryptography is often used in the transmission stage. Users have to decode the message before they can read or use the data. In contrast, watermarking preserve the observable quality of the data, for example the image fidelity, the audio and the video quality, in such that the people can use the data without being aware of the existence of the embedded message. Watermarking can be used both in transmission and for data usage. In addition, cryptography aims to modify every single bit of the original data. In Digital Watermarking the aim is to embed a code consisting of bits into a cover media, representing image, audio, video or graphics information [1]-[3]. Digital watermarking is generally considered as a copyright protection technique. Most of the digital data available in World Wide Web is in the form of images, audio and video form. Therefore these data is very easy to copy, distribute, modify, manipulate and destroy by the intruders, so there is a great need to protect the digital data, the watermarking technique is used to avoid the unauthorized copying or tempering of digital data.

The digital watermarking is used to protect the contents presents in the digital images. The information presents in the digital images are either visible or invisible. Depending on that there are two types of watermarking are presents viz. visible watermarking and invisible watermarking. Also the digital watermark has a visible or an invisible identification code that is permanently embedded in the host image. In the last decade, digital watermarking becomes an active research area and many watermarking techniques are presents for audio, images, and the videos. The watermarks and watermarking techniques can be divided into various types in various ways [4]-[5].

The organization of this paper is in the following way, the section II shows the introduction of proposed methods used in this paper. In section III the implementation of system is presents. The detail explanation of the system is present in this section. In the section IV an experimental and segmentation results are presents. Finally the section V concludes this paper.

PROPOSED METHODS

The DCT is a transformation technique in which the different functions are presents which are used in the signal processing. The DCT transforms a signal from time domain to frequency domain. Due to the good performance of this technique, it has been used in the JPEG standard for image compression. The DCT has been also applied in many fields like as data compression, pattern recognition, and image processing, and so on. The formulas for the DCT transform and its inverse can be expressed are as follows:

$$F(u,v) = \frac{4C(u)C(v)}{n^2}\sum_{j=0}^{n-1}\sum_{k=0}^{n-1} f(j,k)\cos[\frac{(2j+1)u\Pi}{2n}]\cos[\frac{(2k+1)v\Pi}{2n}] \tag{1}$$

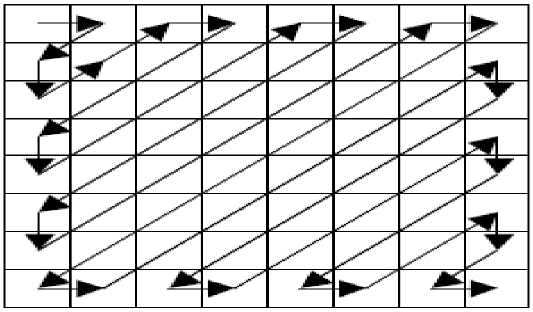
$$f(j,k) = \sum_{u=0}^{n-1}\sum_{v=0}^{n-1} C(u)C(v)F(u,v)\cos\left[\frac{(2j+1)u\pi}{2n}\right]\cos\left[\frac{(2k+1)v\pi}{2n}\right] \quad (2)$$

Where,

$C(w) = \frac{1}{\sqrt{2}}$ when w=0

C(w) = 1 when w= 1,2,3,4………..n-1

As the image transformed by DCT transform, it is usually divided into non-overlapped m x m block. In general, a block always consists of 8x8 components. The block coefficients are shown in figure 1. The left-top block coefficient is the DC component while the others blocks has AC components. For these blocks the zigzag scanning permutation is applied for the energy distribution from high frequency to low frequency and from low frequency to high frequency with the same manner. The human visual system is more sensitive to noise in lower frequency band than the higher frequency. Generally the energy of natural image is concentrated in the lower frequency range rather than the higher frequency range. Therefore the watermark hidden in the higher frequency band might be lost after a lossy compression. Due to this reason in this paper work the watermark is embedded in the lower frequency band of the host image that transformed by DCT is perfect selection. The lower-band coefficients of DCT block are described as in Figure 1. The DCT is a mathematical transformation technique that takes a signal and transforms it from time domain into the frequency domain.



	1	5	6				
2	4	7					
3	8						

Fig.1.a. The DCT block coefficient and zig-zag, b)The eight lower -band coefficients.

Most of the digital image compression and video compression schemes use a block based DCT technique, because this algorithm requires minimum amount of data to recreate the digitized image. In general, the JPEG and MPEG compression techniques are used for the DCT to concentrate image information by removing time domain data redundancies in two dimensional images [9].

In the standard JPEG compression encoding, the representation of the colours presents in the image is converted from RGB to YCbCr, then this image is decomposed in 8×8 blocks then these blocks are transformed from the spatial domain to the frequency domain by using the DCT. Then, each DCT coefficient is divided by its corresponding constant values in a standard quantization table and rounded down to the nearest integer value. After this step, the DCT quantized coefficients blocks are scanned in a predefined zigzag manner. In each block the 64 DCT coefficients are set up from the lowest frequencies (upper left corner) to the highest frequencies (lower right corner) [17].

A. EMBEDDING ALGORITHM

In this paper, an original grayscale image of size (N x N) is divided into n = (N x N) non-overlapped blocks. Here the image is divided into (8x8) blocks. This can be done by using the DCT which transformed the image into frequency domain from time domain. The each block has 64 coefficients as shown in Figure 1. The watermark bit stream is embedded into eight coefficients in lower band of each block shown in Figure 2. For the purpose of distribute the watermark into the host image and prompting the security, the pseudo random system is used to generate a random position in watermarking algorithm. The secret key is used to feed into pseudo random number system in which the size of n (N x N / 64) non-repeated random numbers is generated. Since it is time consumption in the pseudo random number system, we can calculate the random number set with off line manner. The processing of embedding watermark is described below.

Step 1*:* The watermark image is converted into grayscale image and converted into bit stream.

Step 2*:* By using the pseudo random system, obtain a random number, which points to corner block of 8 blocks or 6 blocks of original image. Image is converted into blocks by using DCT.

Step 3*:* Embed the 8-bit watermarking data from the first step into the 8 lower band coefficients in the block pointed in second step.

Step 4*:* Repeat all above steps, until the whole watermark bit stream is to be embedded in the all block coefficients.

B. THE EXTRACTION ALGORITHM

The extraction steps for the watermark from original image are similar to the process of the embedded watermark algorithm. We use the same set of random number, which is applied in the embedded strategy. The watermarked image must be transformed from time domain to frequency domain by using the DCT. The 8-bit watermark data of each DCT block will be extracted by mean of the inverse step that is embedded. Once all of the 8-bit watermark data are extracted, we rearrange the watermark bit stream to configure the original watermark image as soon. The exaction step is described below.

Step 1: Apply transform to the input colour watermarked image to convert the time domain to frequency domain using DCT.
Step 2: In the second step use the same set of random numbers, which are helps for the embedding process.
Step 3: Find the exact location of the DCT block by applying the random number to the watermarked image.
Step 4: Now extract each bit watermark data from each DCT block by using inverse embedding process.
Step 5: Lastly rearrange these bits to get the output watermark image.

IMPLEMENTATION OF SYSTEM

In this section the development of system is presents. The development of system is concerned with identifying the software components; specify the relationships between various components and maintaining a record for design decisions.

A. BLOCK DIAGRAM

This section shows the proposed watermarking scheme, in which the Discrete Cosine Transform (DCT) is applied to an original image which is used to embed the messages. While in a watermarking extraction process, the embedded watermarks are extracted by using Inverse Discrete Cosine Transform (IDCT) coefficient blocks.

1) WATERMARK EMBEDDING

The figure 2 shows a proposed watermark embedding process block diagram. This watermark embedding process can be divided into four steps.

Step 1: The original input image is converted from colour image to grayscale image plane. Simultaneously the watermark image is also converted from colour image to grayscale image plane.
Step 2(2-D DCT): A two dimensional discrete cosine transform is applied to the original host image of size is M x N.
This image is split the image into 8x8 sub blocks. Simultaneously the watermark image is converted into binary image.
Step 3 (Message encoding): The binary numbers of watermark image are embedding into 8x8 blocks of image planes of original image.
Step 4: Finally combine the 8x8 blocks of image planes of original image by using IDCT to get the watermarked image.

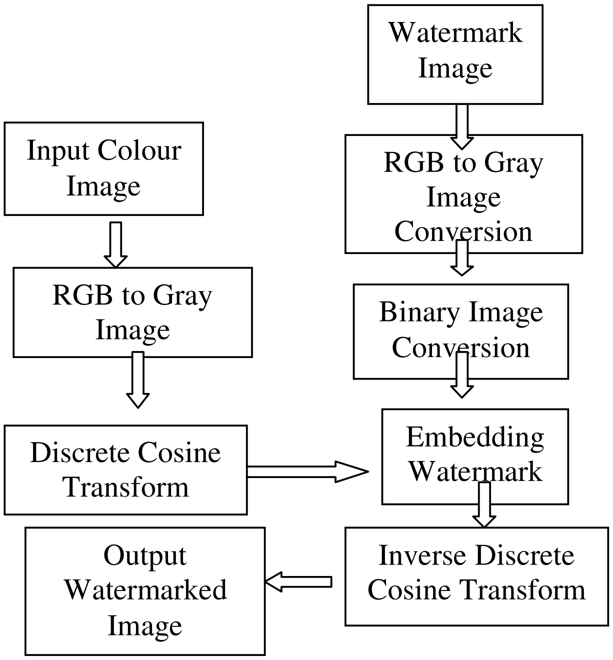


Fig.2. Embedding the watermark block diagram.

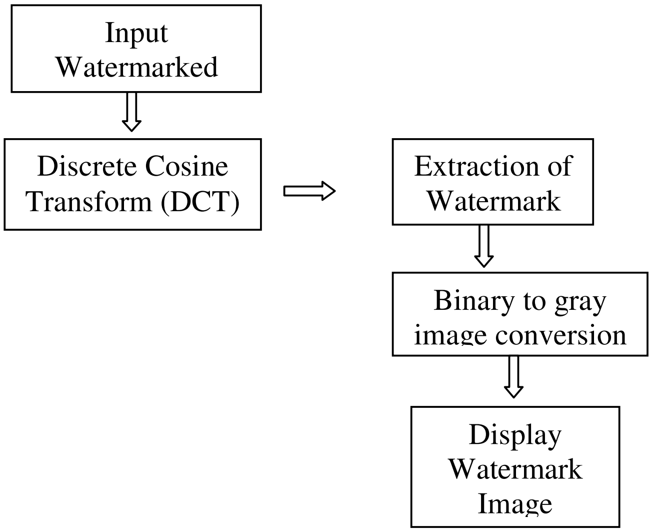


Fig.3. Extraction of watermark block diagram.

2) WATERMARK EXTRACTION

The figure 3 shows a block diagram of the watermark extraction process. The watermark extraction is the inverse process of watermark embedding which is a present in previous section.

Step 1(2-D DCT): A two dimensional discrete cosine transform is applied to the watermarked image of size is M x N. After applying the two dimensional DCT the image split into 8x8 sub blocks.
Step 2: Extract the watermark image bits from 8x8 sub blocks of image planes.
Step 3: Convert a binary image into the gray scale image to get the watermark image.
Step 4: Display watermark image.

EXPERIMENTAL RESULTS

This section reports the performance analysis of the proposed system in terms of robustness and imperceptibility to the various distortions. While implementing any new system we need to check its compatibility to the prior versions. So this paper work basically starts with embedding and extraction of watermark into the images. The software which is use for developing this proposed system is image processing and wavelet toolbox presents in MATLAB for reading the images and for performing the DCT operations.

For measuring the perceptual quality of an image, we calculate the peak of signal to noise ratio (PSNR) of an image that is used to determine the quality of the watermarked image frames in comparison with the original image frames. The unit of PSNR is decibels (db). The higher a PSNR value, the quality of the compressed or reconstructed image has better. The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, lower the error. To compute the PSNR, first we calculate the mean-squared error using the following equation:

$$\mathrm{MSE} = \frac{\Sigma_{M,N}[\mathrm{I}_1(\mathrm{m},\mathrm{n}) - \mathrm{I}_2(\mathrm{m},\mathrm{n})]^2}{\mathrm{M} * \mathrm{N}} \qquad (3)$$

In this equation, M and N are the number of rows and columns in the input images, respectively. Then the PSNR can be calculated by using the equation.

$$PSNR = 10lcg_{10}\left(\frac{\mathrm{R}^2}{MSE}\right) \qquad (4)$$

Where, R is the maximum fluctuation in the input image.

A. IMAGE WATERMARKING

The detail steps of this work are given below.

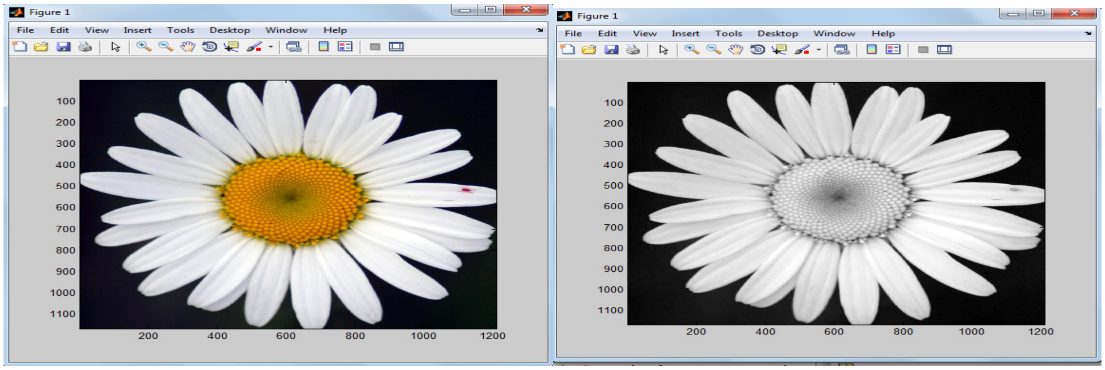


Fig.4.a) Original flower image, b) Grayscale Image of original image.

A) WATERMARK EMBEDDING

Step1. Select a 24 bit true color image of dimensions any size and called this image as Original image plane. Here flower image is selected which is shown in figure 4 a).

Step2. Decompose the original image into gray scale image. Figure 4 b) shows the gray scale image of original image (flower image).

Step3. Apply the Discrete Cosine transform (DCT) to a gray scale image of original image. The DCT algorithm splits this image into 8x8 blocks.

Step4. Select another 24 bit true color image of 10% in size of original image i.e. the original image is 90% greater in size than watermark image and called this image as watermark image. Here logo image is selected which is shown in figure 5 a).

Step5. Decompose the watermark image Gray Scale Image. Figure 5 b) shows the gray scale image of watermark image.

Step6. Embed the values of gray scale image of watermark image into the 8x8 block of original image. Apply Inverse Discrete Cosine Transform (IDCT) to these images to combine the 8x8 blocks. It creates the watermarked image which is gray scale image which is shown in figure 6 a).

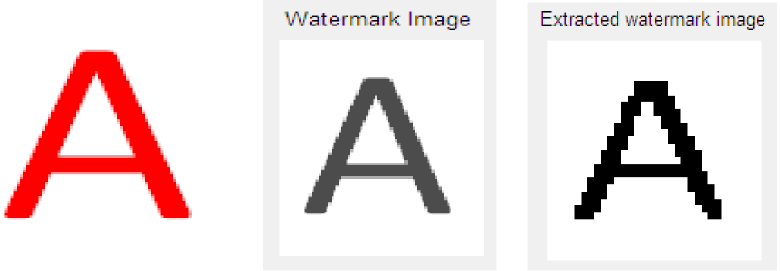


Fig.5.a) Watermark image, b) Grayscale image of watermark image, c) Extracted watermark image.

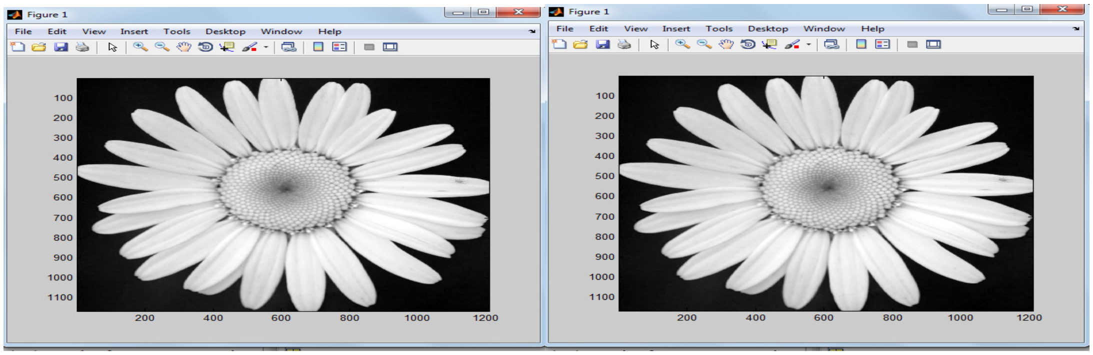


Fig.6. a) Watermarked Gray Scale Image., b) Gray Scale Image Of Watermarked Image.

Table 1. PSNR And MSE or Different Tested Images

Sr. No.	Name & Size	Location	PSNR by Using DCT		MSE by Using DCT		
	Original Image		Watermark Image	Embedded Image	Extracted Watermark	Embedded Image	Extracted Watermark
1	Albert.bmp	A.bmp	8x8 or 6x6	40.7344	32.1019	7.2328 e-005	0.00061632
2	Arnav.bmp	t.gif	8x8 or 6x6	41.3728	18.0957	7.2328 e-005	0.015504
3	TPCT.bmp	o.jpg	8x8 or 6x6	41.4069	18.6816	7.2328 e-005	0.013547
4	Earth.gif	Tick.gif	8x8 or 6x6	43.3594	20.2494	4.3137 e-005	0.009442
5	Kartik1.gif	B.png	8x8 or 6x6	41.4079	15.7815	7.2328 e-005	0.026378
6	Kartik2.gif	t.tiff	8x8 or 6x6	41.5222	15.1744	7.04339e-005	0.030378
7	Sonu1.jpg	a.bmp	8x8 or 6x6	40.6269	32.1019	7.22668e-005	0.00061632
8	Leene.jpg	t.gif	8x8 or 6x6	41.4159	18.0957	7.2178 e-005	0.0815504
9	Vegetables.gif	B.jpg	8x8 or 6x6	40.52392	15.7875	7.18548 e-005	0.026378
10	Arnav.png	A.bmp	8x8 or 6x6	41.3728	32.1019	7.2328 e-005	0.00061632

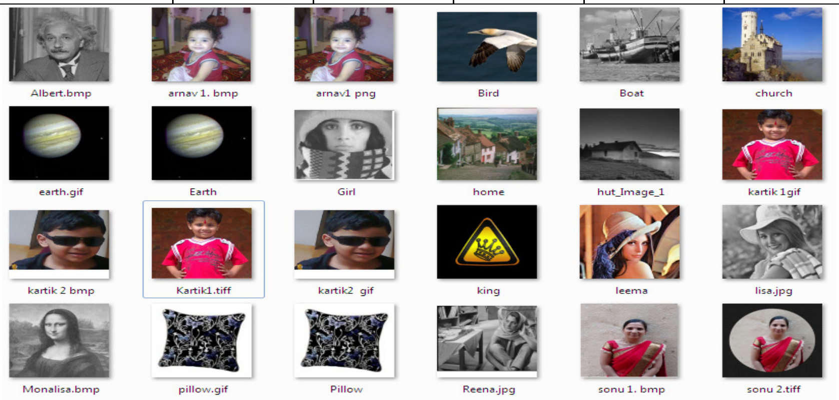


Fig.7. Different tested original images.

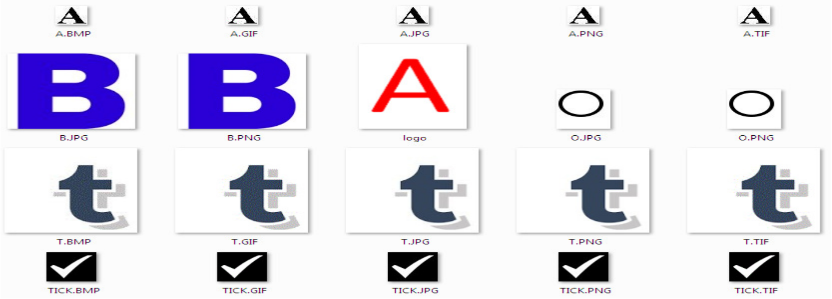


Fig.8. Different tested watermark images.

Figure 7 shows the different tested original images; figure 8 shows the different tested watermark images. There are total six parameters are calculated in this paper these are PSNR, MSE, BER, SSIM, embedding time and retrieval time. Out of these parameters PSNR and MSE are shown in table 1.

B) WATERMARK EXTRACTION

Step1: For extraction of watermark first take the watermarked image. Figure 7 b) shows the gray scale image of watermarked image.

Step2: Extract values of the watermark image from the watermarked image. The extracted watermark image has the value of PSNR is 43.3594 with respect to the original watermark image which is shown in figure 5 c). The experimental results shows that the proposed DCT method has the higher value of PSNR (Peak Signal to Noise Ratio) 43.3594 and the lower MSE (Mean Square Error) 0.009442 for watermarking, which gives higher quality of the extracted watermark.

CONCLUSION AND FUTURE SCOPE

The proposed watermarking algorithm is used to protect the copyright contents present in the different images. The watermark has been embedded in DCT domain. Many of watermarking techniques have presented in time domain and transform domain. The performance of this watermarking is upgraded day by day. In this paper the watermarks were embedded the lower band of the DCT block in the host image. The pseudo random systems are used to generate a scatter random number in order to enhance the security. This paper describes an approach based on DCT digital image water marking, which is used for embedding a watermark logo image.

The DCT compression helps for reducing the size of the original image, and therefore it helps for reducing the effect of embedding the watermark into the original image. Experimental results show low MSE and PSNR upto 40 db for different images.

The current system can supports to the JPEG, BMP, TIFF, GIF and PNG compression formats of different images. The proposed method provides much better robustness and visual quality in the resulting watermark images.

The software which is use for developing this proposed system is image processing and wavelet toolbox presents in MATLAB for reading the images and for performing the DCT operations. The future scope of the paper work is copyright contents protection in a 3D images work very well under constrained conditions. Also in future a watermarking scheme for videos should be used. In this watermark is embedded into the motion scene frames of the videos.

REFERENCES

1. B. Mohan and S. Kumar, “A robust image watermarking scheme using singular value decomposition” J. Multimedia, vol. 3, no. 1, pp. 7-15, May 2008.
2. G. Lo-varco, W. Puech, and M. Dumas, "DCT-Based watermarking method using color components", Second European Conference on Color in Graphics, Imaging and Vision, Germany 2004.
3. Sverdlov, S. Dexter, and A. Eskicioglu, "Robust DCT-SVD domain image watermarking for copyright protection: Embedding data in all frequencies", International Multimedia Conference, Germany, pp. 166-174, 2004.
E. Fu, "Literature survey on digital image watermarking", Technical Report, EE381K-Multidimensional Signal Processing, 1998.
4. G. Lo-varco, W. Puech, and M. Dumas, "Content Based watermarking for securing color images", J. Imaging Science & Technology, vol. 49, no. 6, 2005.
5. S. Mohanty, P. Guturu, E. Kougianos, and N. Pati, "A novel invisible color image watermarking scheme using image adaptive watermark creation and robust insertion-extraction", 8th IEEE International Symposium on Multimedia, San Diego,
6. USA, pp. 153-160, December 2006.
7. L. Liu, A survey on digital watermarking technologies, Technical Report, Stony Brook Univ., New York, USA, 2005.
Coconu, V. Stoica, F. Ionescu, and D. Profeta, "Distributed implementation of discrete cosine transform algorithm on a network of workstations", Proceedings of the International Workshop Trends & Recent Achievements in Information Technology, Romania, pp. 116-121, May 2002.
9. X.Y. Wang and J. Wu, “A Feature-based Robust Digital Image Watermarking against De-synchronization Attack”, International Journal of Automation and Computing, 2007, Vol. 4, No. 4, pages 428-432.
10. S. Bounkong, B. Toch, D. Saad, and D. Lowe, "ICA for watermarking digital images", J. Machine Learning Research, Vol. 4, issue 7-8, pp. 1471-1498, November 2004.S. Pereira and T. Pun, "A framework for optimal adaptive DCT watermarks", European Signal Processing Conference, Finland, pp. 1669-1671, September 2006. Parthasarathy, Improved Content Based Watermarking for images, M.Sc. Thesis, Louisiana State University, August 2006.
11. W. Puech and J. Rodrigues, "Crypto-compression of medical images by selective encryption of DCT", 13th European Signal Processing Conference, Turkey, September 2005.
12. Y. Z. Lu, A Novel Face Recognition Algorithm for Distinguishing Faces with Various Angles, International Journal of Automation and Computing, 2008, Vol. 5, No. 2, pages 193- 197.
13. S. M. Metev and V. P. Veiko, Laser Assisted Micro technology, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.