Volume 3, Issue1
February 2014

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Robust Watermarking Algorithms for Content Authentication and Secure Image Transmission through Single Carrier Frequency Division Multiple Access

Safey A. S. Abdelwahab
Engineering Department, Nuclear Research Center
safeyash@yahoo.com

ABSTRACT

Images are the most common and convenient means of transmitting information as one image is worth than thousand words. The need for the protection of digital media has gained importance as the networked multimedia systems have rapid growth. Also images can now easily be copied and distributeddue to improvements in imaging technologies and the ease with which digital content can be created and manipulated.This paper presents image watermark algorithms which are developed to ensure security and protection of images and pictures. The purpose of proposed digital watermarking is not only to restrict use of multimedia resources, but also to facilitate data authentication and copyright protection for secure image transmission through Single Carrier Frequency Division Multiple Access (SC-FDMA).Simulation of the proposed algorithms is done using Matlab software and a comparison between them is done. The proposed algorithms are tested against image attacks using Checkmark software and the experimental results approved that the proposed algorithms have good robustness and they are resistant against cropping, scaling and compression distortion.

Keywords*:SC-FDMA, Image Watermarking, Wireless Communication, Communication*

1. INTRODUCTION

Single Carrier Frequency Division Multiple Access (SC-FDMA) is a promising technique for high data rate uplink communication. It is a recent variant of Orthogonal Frequency Division Multiple Access (OFDMA) with similar throughput performance and complexity. The advantage of SC-FDMA is the lower Peak-to-Average Power Ratio (PAPR) because of its inherent single carrier nature where low peak-to-average power ratio greatly benefits the mobile terminal in terms of transmitting power efficiency and manufacturing cost. Therefore SC-FDMA is seen as an attractive alternative to OFDMA [1:3].

The recent progress in the digital multimedia technologies has offered many facilities in the transmission, reproduction and manipulation of images. However, this advancement has also brought the challenge such as copyright protection for content providers. Digital watermarking is one of the solutions for copyright protection of multimedia data. Image watermarking is the process that embeds a watermark into a cover image. The watermark is a secret code that containingidentification information such as copyright, license, authorship etc. The earliest use has been to record the manufacture's trademark on the product so that authenticity could be easily established. The Government uses it for currencies, postage stamps, revenue stamps, etc. Now due to the information and computer age, digital watermarking is being expanded [4:8].

A watermarking system which plays an increasingly important role for proving authenticity and copyright protection can be modeled as communication where the cover image is treated as noise and the watermark is viewed as a signal that is transmitted through it, it was only natural to try to apply techniques that worked in communications to watermarking.

In order a watermark to be effective it should not degrade or affect the image quality, it should be resistant to attacks such as cropping, scaling, rotation, and compression distortion, and also watermark should not be removed beyond reliable detection by targeted attacks.

Volume 3, Issue1
February 2014

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

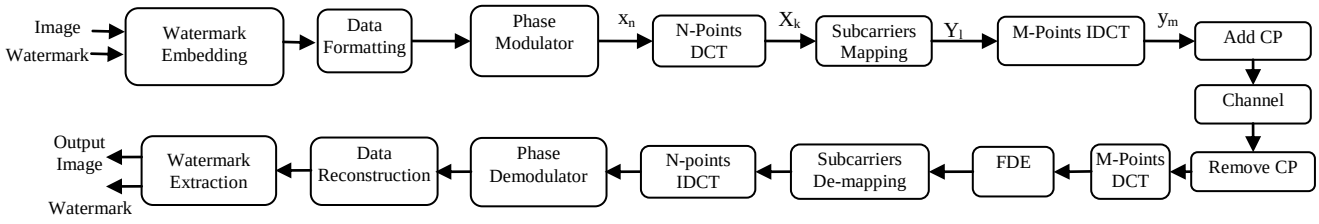


Figure 1: Image Watermarking over the SC-FDMA System

2. IMAGE WATERMARKING OVER THE SC-FDMA SYSTEM

Figure 1 shows the architecture of Image Watermarking over the SC-FDMA system. The watermark embedding block embeds the watermark into the cover image with the used algorithm either in spatial or frequency domain. The image formatting is used to transmit the image over the SC-FDMA system by converting it to a binary form suitable to be inserted and processed by the SC-FDMA system. The SC-FDMA transmitter starts with an encoder then a modulation of the input signal using binary Quadrature Phase Shift Keying (QPSK), Let x_n represent the modulated source symbols. The signal after the DCT can be expressed as follows:

$$X_k = \sqrt{\frac{2}{N}}\beta_k \sum_{n=0}^{N-1} x_n \cos\left(\frac{\pi k(2n+1)}{2N}\right) \qquad (1)$$

where x_n is the modulated data symbol, and β_k is given by:

$$\beta_k = \begin{cases} \frac{1}{\sqrt{2}} & k = 0 \\ 1 & k = 1,2,\ldots\ldots,N-1 \end{cases}$$

Where N is the input block size, { x_n : n = 0, ...,N -1} represents the modulated data symbols. The outputs are then mapped to M ($M > N$) orthogonal subcarriers followed by the M-points IDCT. The subcarriers mapping assigns frequency-domain modulation symbols to subcarriers Y_l , which represent the frequency-domain sample after subcarriers mapping. After the Inverse Discrete Cosine Transform (IDCT), the signal can be expressed as follows:

$$y_m = \sqrt{\frac{2}{M}} \sum_{l=0}^{M-1} Y_l \beta_l \cos\left(\frac{\pi l(2m+1)}{2M}\right) \qquad (2)$$

where Y_l is the signal after the subcarriers mapping. M is the IDCT length (number of subcarriers) (M=Q.N). Q is the bandwidth expansion factor of the symbol sequence. If all terminals transmit N symbols per block, the system can handle Q simultaneous transmissions without co-channel interference.

It also inserts a set of symbols referred to as Cyclic Prefix (CP) in order to provide a guard time to prevent Inter-Block Interference (IBI) due to multipath propagation. The CP is a copy of the last part of the block. It is inserted at the start of each block. The transmitted data propagates through the channel.

At the receiver, the CP is removed, and then the received signal is transformed into the frequency domain by (DCT). The samples are passed through the Frequency Domain Equalizer (FDE) then the de-mapping operation isolates the frequency-domain samples of each source signal. The inverse transform (IDCT) at the receiver transforms equalized symbols back to the time domain. The demodulation process recovers the original data, which is passed through the decoder. The image reconstruction is used to convert the binary form to an image to recover the original image. Watermark extraction is used to extract the watermark from the watermarked image.

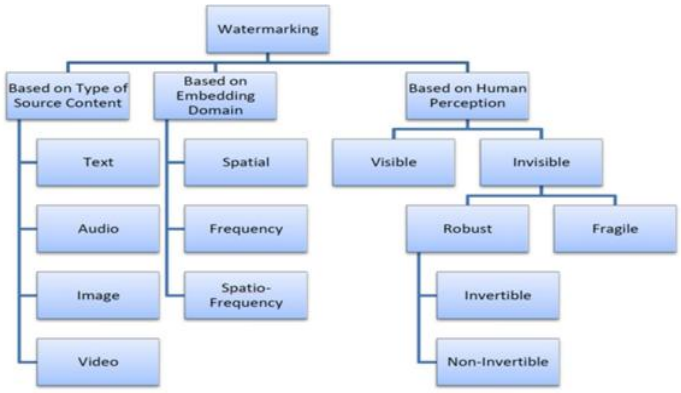


Figure 2: Watermarking Classification

3.IMAGE WATERMARKING ALGORITHMS

The watermarking techniques can be classified into many categories as shown in figure 2. In this paper we will introduce algorithms in spatial domain and frequency domain.The first one is based on spatial domain techniques, which embed the watermark by directly modifying the pixel values in the image. The second category comprises of transform domain methods, which embed the watermark by modulating the transform domain coefficients of the data. The frequency domain methods are more complex, but more robust than the spatial

Volume 3, Issue1
February 2014

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

methods. Watermarks embedded in a frequency domain representation of the host signal perform better under signal processing operations than spatial domain approaches [4].

3.1 Spatial Domain Watermarking:

Least significant bit (LSB) watermarking technique is the earliest and also the simplest spatial domain watermarking method, the watermark embedding is achieved by directly replacing the least significant bits of the host image directly with the watermark. But the disadvantage of this method is that the robustness of the watermark is very weak. Most of the watermark will be lost after some attacks take place such as JPEG compression and Gaussian noise. The watermark message may be able to survive after some basic operation such as cropping and scaling. The watermark message will not be extracted correctly, even after single filtering and add noise operation.

Suppose the first eight pixels of the original image have the grayscale values as shown in figure 3-a [9:11]:

To hide the letter A whose binary value is 01000001, we would replace the LSBs of these pixels to have the new grayscale values as shown in figure 3-b:

11010010	01001010	10010111	10001100
00010101	01010111	00100110	01000011

(a)

11010010	01001011	10010110	10001100
00010100	01010110	00100110	01000011

(b)

Figure 3: (a) First Eight Pixels of the Original Image and (b) The New Grayscale Values

In this way a watermark is being embedded in the image data by changing only the LSB of the image data

3.2 Frequency Domain Watermarking

In transform domain technique the host image is first converted into frequency domain by transformation method such as the discrete cosine transform (DCT), discrete Fourier transform (DFT) or discreet wavelet transform (DWT),etc. then, transform domain coefficients are altered by the watermark. The inverse transform is finally applied in order to obtain the watermarked image.

3.2.1 The Discrete Cosine Transform:

The Discrete Cosine Transform (DCT) is a technique that converts a spatial domain signal into its constituent frequency components as represented by a set of coefficients. Discrete Cosine Transform (DCT) decorrelates the image data.

The frequency domain methods allow an image to be broken up into different frequency bands. Embedding the watermark in the low frequency increases the robustness with respect to image distortions. The high frequency band of an image will be lost by compression or scaling due to quantization. The middle frequencies embedding of the watermark avoid the most visual important parts of the image and it is robust to compression and noise attacks. The definition of the DCT regions is shown in figure 4.

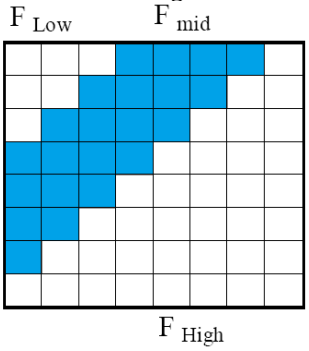


Figure 4: Definition of DCT Regions

The 2-D DCT is can be expressed as [12]:

$$Y[u,v] = 2C_u C_v / N \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} X[m,n] \cos[(2m+1)u\pi / 2N] \cos[(2n+1)v\pi / 2N] \quad (3)$$

Where:

u, v = discrete frequency variables (0, 1, 2, …, N - 1)
X[m, n] = N by N image pixels (0, 1, 2, …, N - 1)
Y[u, v] = the DCT coefficients
C_u ,C_v = 1 / Sqrt(2) when u,v = 0
= 1 Otherwise

And DCT can be expressed in the matrix form as:

$$Y = C.X . C^T \quad (4)$$

Where

X is an NxN image block
Y contains the NxN DCT coefficients
C is an NxN matrix defined as:

$$C_{mn} = K * \text{Cos}[(2m+1)* n * \pi /2*N]$$

Where

K = 1 / Sqrt(2) when n = 0
K = 1 Otherwise

Volume 3, Issue1
February 2014

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Watermark insertion and extraction algorithm in DCT domain which shown in figure 5 starts by reading the input image to be watermarked and the watermark then computing the forward DCT coefficients of both image and watermark after dividing them into non overlapping blocks and applying forward DCT to each block.Obtaining the DCT components of the watermarked image by adding the DCT coefficients of both image and watermark in the mid band frequency only then generate the watermarked image by applying the inverse DCT and merging all blocks. After transmitting the watermarked image through the SC FDMA system, image and watermark extraction starts by computing the forward DCT coefficients of the watermarked image after dividing it into non-overlapping blocks and computing forward DCT for each block.Extract the DCT components of the imagefrom the DCT coefficients of watermarked image by subtracting the DCT coefficients of the watermark. Generate the cover image by applying the inverse DCT.

3.2.2The Discrete Wavelet Transform:

Wavelet is a suitable tool for transient, non-stationary or time-varying phenomena so it provides a way where an image can be de-correlated without introducing any artifacts or distortions. The Wavelet transform is a compression algorithm that decomposes the image into sub-image of different spatial domain and independent frequency district using low-pass and high-pass filters. The image is then divided into four sub-bands. These 4 frequency districts which are one low-frequency district (LL) and three high-frequency districts (LH, HL, HH) as shown in figure 6 and figure 7. The frequency bands where it has the lowest resolution of the (LL) which close to the original image can be also decomposed into a 2nd level (pass). The frequency districts of LH, HL and HH respectively represent the level detail [13, 14].

The embedding media is the LL-subband of the wavelet decomposition. Since all LL-subband coefficients are used for watermark embedding, the size of the watermark pattern is equal to the size of the LL-subband of the host image.

Watermark insertion and extraction algorithm in DWT domain which shown in figure 8 starts by reading the input image to be watermarked and the watermark then decomposing both image and watermark into four frequency bands using one level DWT decomposition. Sub-band suitable for embedding watermark is chosen. Wavelet coefficients of the selected sub-band are modified according to the watermark image. Then generate the watermarked image by applying the inverse DWT. After transmitting the watermarked image through the SC FDMA system, image and watermark extraction starts by decomposing the watermarked image using one level DWT decomposition. Extract the DWT components of the image from the DWT coefficients of watermarked and generate the cover image by applying the inverse DWT.

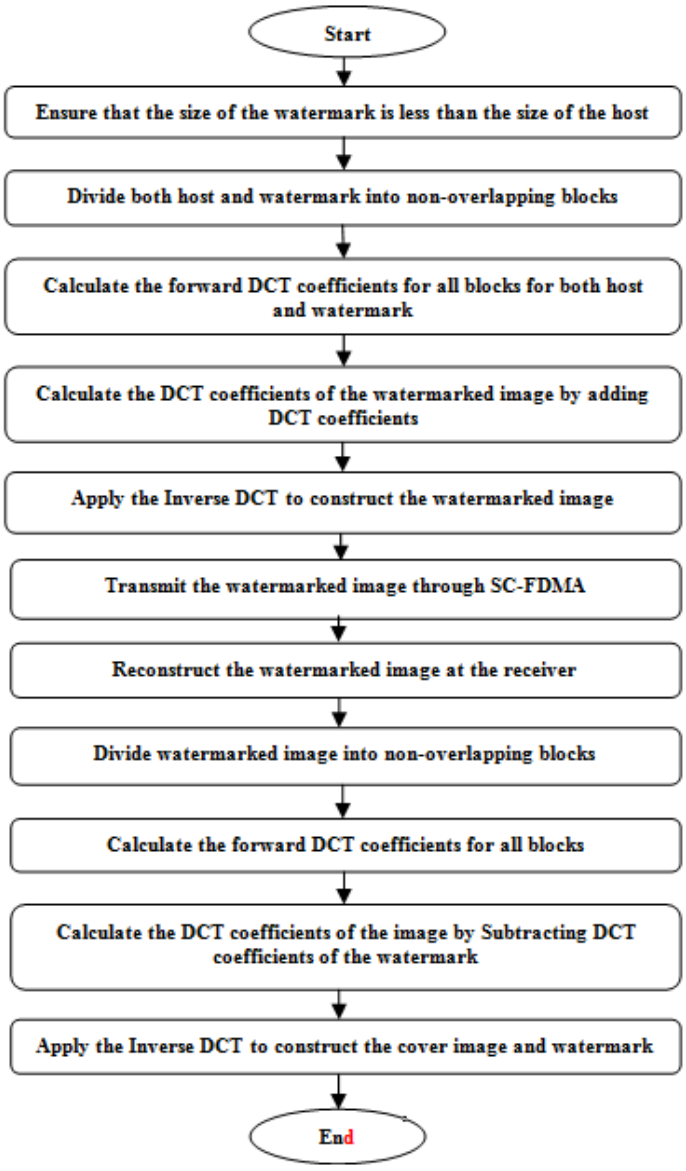


Figure 5: Watermark Embedding, Transmitting and Extraction Algorithm using DCT

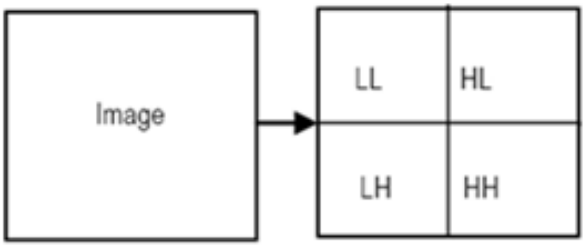


Figure 6: One Level DWT Decomposition

Volume 3, Issue1
February 2014

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

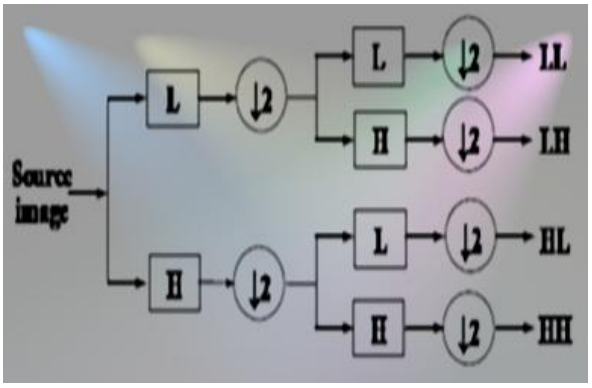


Figure 7: Structure of DWT

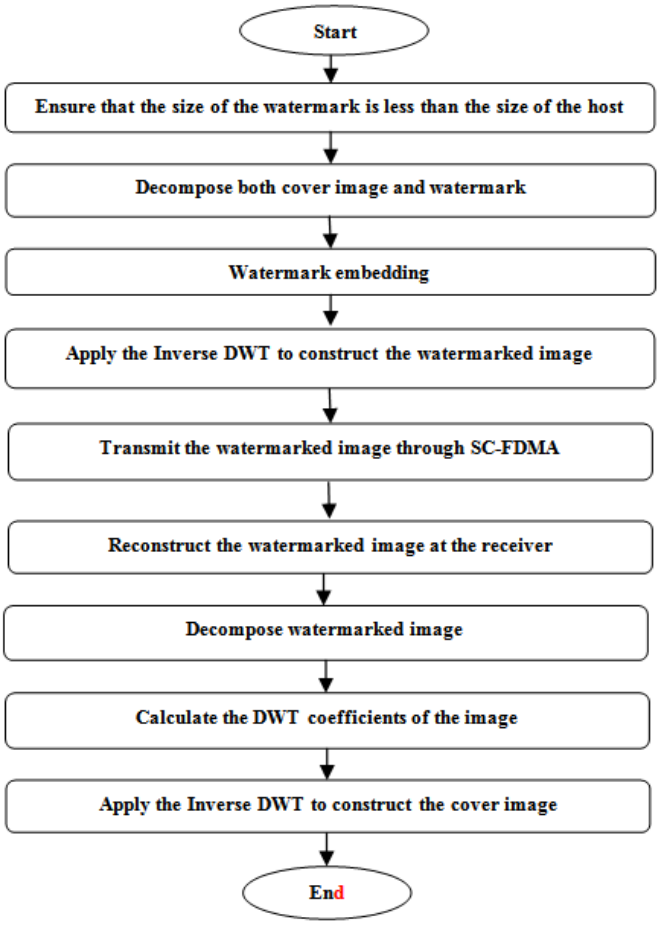


Figure 8: Watermark Embedding, Transmitting and Extraction Algorithm using DWT

4. SIMULATION RESULTS

Watermark embedding incurs distortion on the host contents. Most watermarking applications require that the distortion be small enough to be imperceptible for humans. The performance evaluation of our scheme is based on imperceptibility by comparing the amount of distortion introduced into a host image by the watermarking algorithm. We used peak signal to noise ratio (PSNR) to measure the quality of the reconstructed images at the receiver. It is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of this signal. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. The PSNR is defined as follows [3]:

$$PSNR = 10\log_{10}\left(\frac{\max_f^2}{MSE}\right) \quad (5)$$

Where $\max_f$ is the maximum possible pixel value of an image f, for 8 bit pixels, $\max_f$ =255. *MSE* is the Mean Square Error. For an N × N monochrome image, it is defined as:

$$MSE = \frac{\sum\left[f(i,j) - \hat{f}(i,j)\right]^2}{N^2} \quad (6)$$

Where $f(i,j)$ is thesource image and $\hat{f}(i,j)$ is the reconstructed image.

To evaluate the performance and efficiency of the above-mentioned systems, the 256×256 Cameraman image is used as host image and another binary image is used as the watermark. The simulation parameters are given in Table (1) and the simulation results are shown in Fig.9: Fig. 14. In order to test the performance, the watermarked image suffers some differentsignal attacks, which includes copy, sharpening, cropping and image compression.

Table 1: Simulation Parameters

Simulation Parameter	Value
FFT size	512 symbols
Input block size	128 symbols
Cyclic prefix size	20 samples
Image size	256 × 256 for cameraman
Channel Coding	Convolutional code with rate 1/2
Modulation type	QPSK
Subcarriers mapping	Interleaved and localized
Channel model	SUI-3,AWGN
Noise environment	AWGN
Equalizer type	MMSE equalizer

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

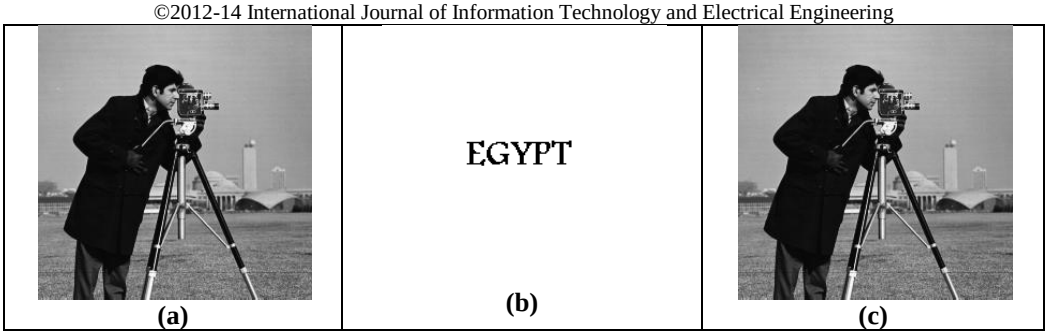
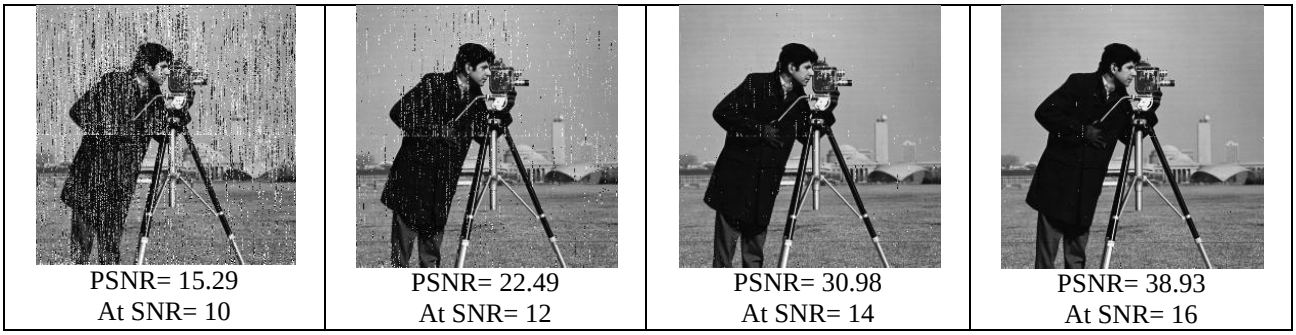
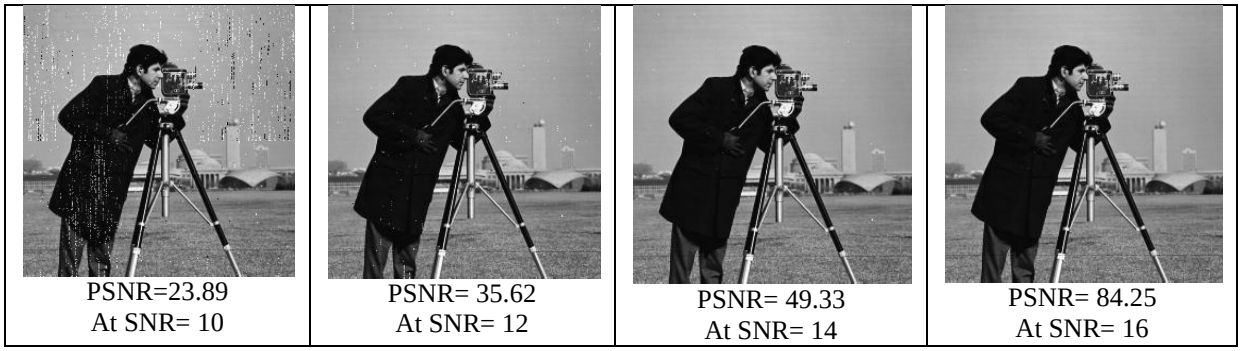


Figure 9: (a) Original Image, (b) Watermark and (c) Watermarked Image Using LSB



(a)



(b)

Figure 10: Transmitted Watermarked Image Using LSB (a)LFDMA and (b) IFDMA at Different SNR

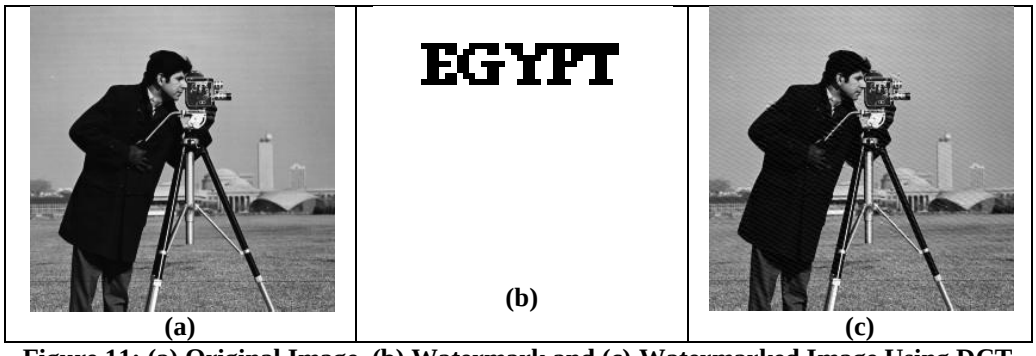


Figure 11: (a) Original Image, (b) Watermark and (c) Watermarked Image Using DCT

Volume 3, Issue1
February 2014

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

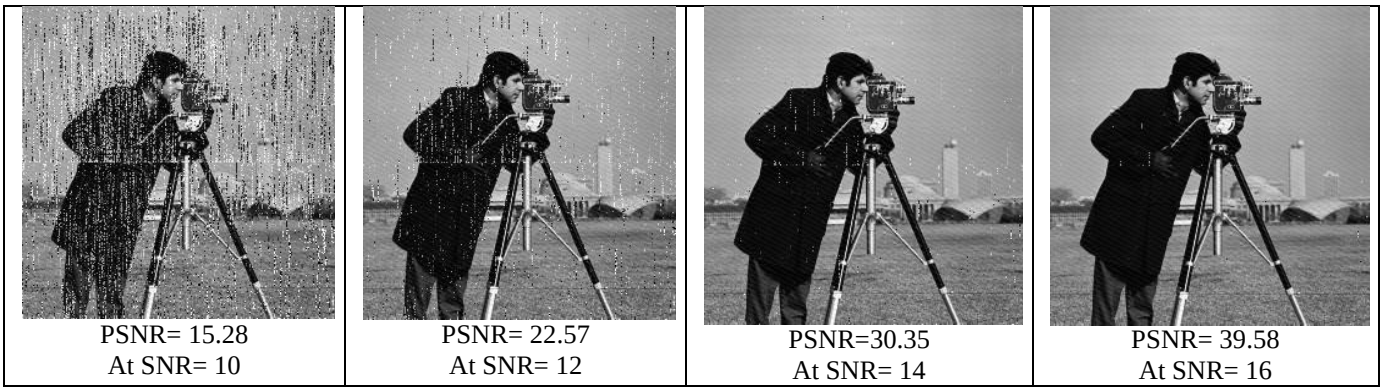


Figure 12: Transmitted Watermarked Image Using DCT (a) LFDMA and (b) IFDMA at Different SNR

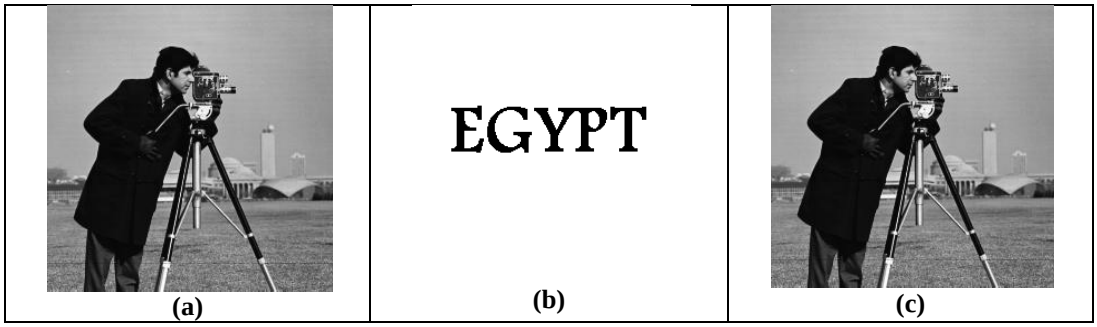
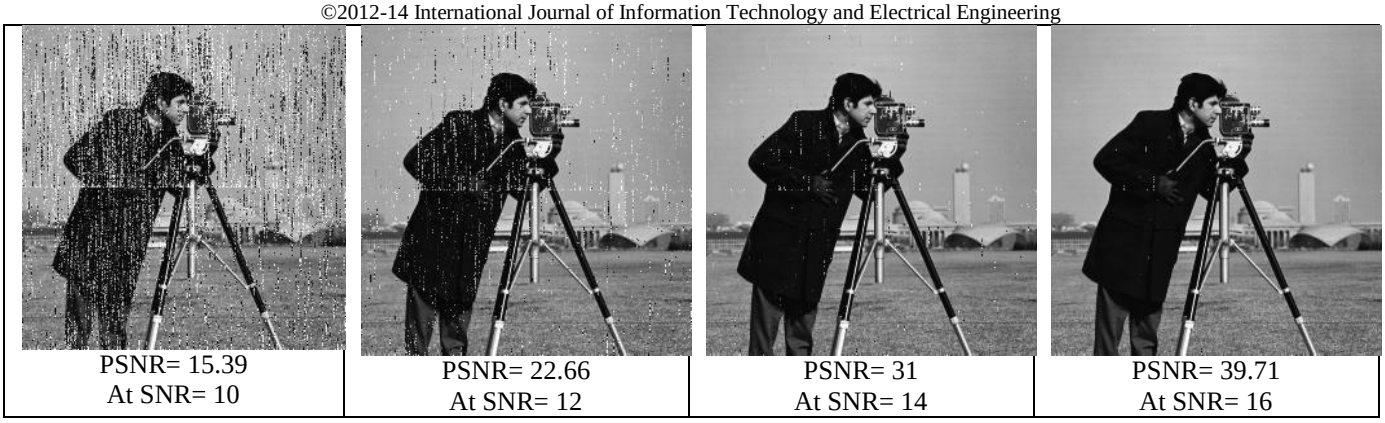
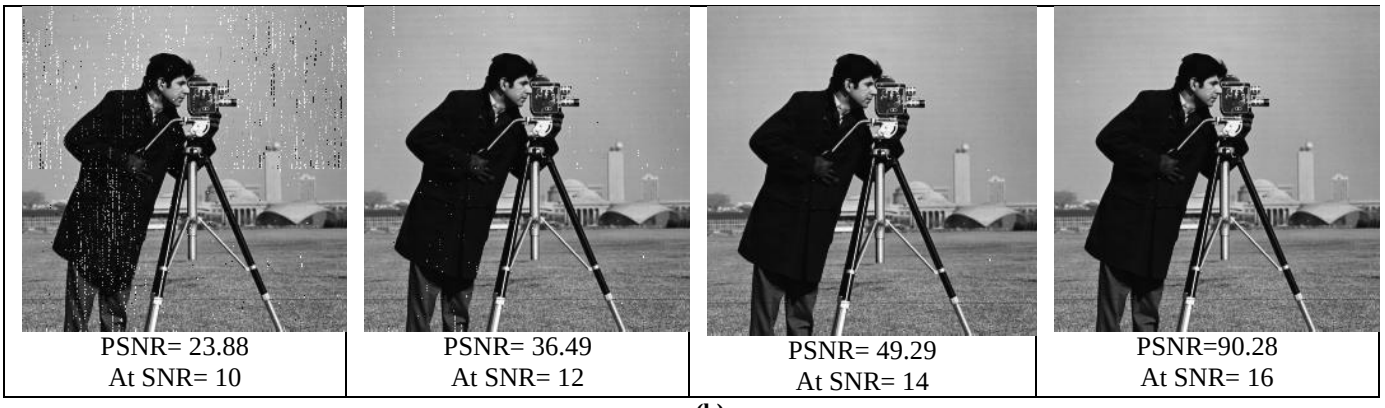


Figure 13: (a) Original Image, (b) Watermark and (c) Watermarked Image Using DWT



(a)



(b)

Figure 14: Transmitted Watermarked Image Using DWT (a) LFDMA and (b) IFDMA at Different SNR

The robustness test of the proposed algorithms against the image attacks was done using Checkmark software which is a benchmarking suite for digital watermarking developed on Matlab written by Shelby et al. [15, 16]. These tests include common signal processing procedures such as sharpness, lossy JPEG compression, rotation and scaling. Checkmark offers some additional attacks not present in Stirmark. Also, it takes the watermark application into account which means that the scores from individual attacks are weighted according to their importance for a given watermark purpose [4].

Our system has proved to be able to survive all of these tests and the experimental results which are listed in Tables 2,3 approved that this system has a good robustness. Some of the watermarked images under attacks are shown in Figures 15, 16, 17 and 18.

Table 2: PSNR of Watermarked Image under JPEG Compression

JPEG Compression Quality	30	40	50	60	70	80	90
DCT	29.97	30.89	31.30	35.34	41.51	42.53	45.69
DWT	30.21	30.93	31.34	35.41	42.04	42.86	45.9

Table 3: PSNR of Watermarked Image under Cropping Attack.

Cropping Percent	10%	20%	30%	40%	50%	60%	75%
DCT	25.34	25.38	25.32	25.19	25.06	25.18	24.65
DWT	25.87	25.88	25.81	25.63	25.48	25.63	23.82

Volume 3, Issue1
February 2014

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

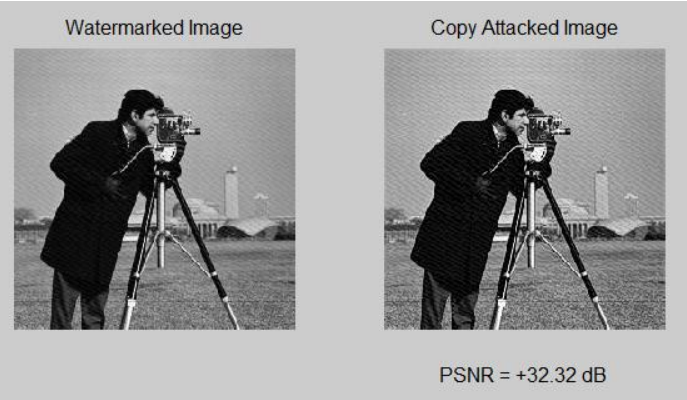


Figure 15: DCT Watermarked Image before and after Copy Attack

Figure 16: DWT Watermarked Image before and after Copy Attack

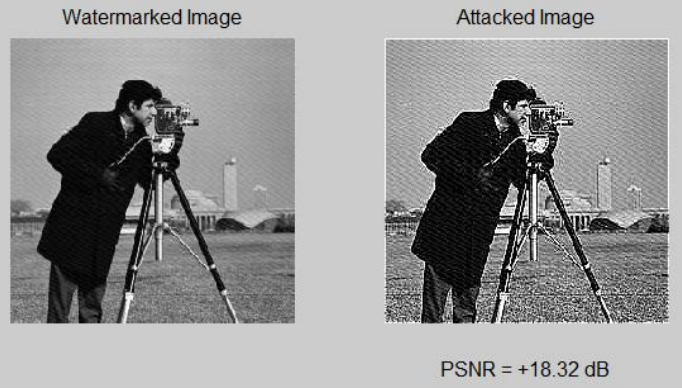


Figure 17: DCT Watermarked Image before and after Sharpening Attack

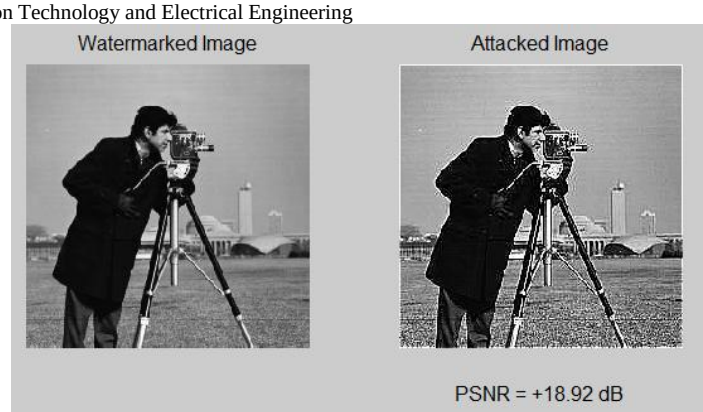


Figure 18: DWT Watermarked Image before and after Sharpening Attack

5. CONCLUSIONS

This paper presented proposed image watermark algorithms which were developed to ensure security and protection of images. The purpose of proposed digital watermarking is not only to restrict use of multimedia resources, but also to facilitate data authentication and copyright protection for secure image transmission through SC-FDMA.

Simulation of the proposed algorithms using Matlab software was done to evaluate the performance and efficiency of the system. The experimental results have shown that the system achieve higher PSNR values and watermarks embedded in a transform domain perform better under signal processing operations than time or spatial domain approach. However, the cost of transform domain is an increase in computational complexity.

The proposed algorithms are tested against image attacks using Checkmark software and the experimental results approved that the proposed algorithms havegood robustness and they are resistant against cropping, scaling, sharpening and compression distortion.

REFERENCES

[1] H. Myung, J. Lim, and D. Goodman, "Single Carrier FDMA for Uplink Wireless Transmission," IEEE Vehicular Tech. Magazine, vol. 1, Sep. 2006.

[2] H. Myung and D. Goodman, "Single Carrier FDMA a New Air Interface for Long Term Evolution", John Wiley & Sons, Ltd., 2008

[3] Safey A. S. Abdelwahab, "New and Efficient DWT SC-FDMA System for Image Transmission", ITEE, Vol. 2, Issue 2, 2013

[4] Safey A. S. Abdelwahab, "Robust Digital Image Watermarking Scheme Based On Discrete Tchebichef

Transform", 19th International Conference on Computer Theory and Applications (ICCTA 2009), Alexandria, Egypt, 17-19 October 2009.

[5] M. Kutter and F. Hartung, "Introduction to Watermarking Techniques", S. Katzenbeisser and F. Petitcolas eds., Artech House Press, Boston, 2000.

[6] V. Singh, "Digital Watermarking: A Tutorial", Journal of Selected Areas in Telecommunications (JSAT), January Edition, 2011.

[7] Smitha Rao M.S, Jyothsna A.N and Pinaka Pani.R, "Digital Watermarking: Applications, Techniques and Attacks", International Journal of Computer Applications, Volume 44– No.7, April 2012.

[8] N. Chandrakar and J. Bagga, "Performance Comparison of Digital Image Watermarking Techniques: A Survey", International Journal of Computer Applications Technology and Research, Volume 2– Issue 2, 2013.

[9] D. Chopra, P Gupta, Gaur Sanjay B.C. and A. Gupta, "Lsb Based Digital Image Watermarking For Gray Scale Image", IOSR Journal of Computer Engineering (IOSRJCE), Volume 6, Issue 1, Sep-Oct. 2012.

[10] G. Kaur and K. Kaur, "Image Watermarking Using LSB (Least Significant Bit)", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013

[11] Y. Jadav, "Comparison of LSB and Subband DCT Technique for Image Watermarking", Conference on Advances in Communication and Control Systems (CAC2S 2013)2013.

[12] Safey A. Shehata, Imbaby I. Mahmoud and Hassan M. Frahat, "Image Compression Using A Fast 2-D DCT Algorithm", International Conference on Industrial Electronics, Technology & Automation (IETA 2001), Cairo, Egypt, December 19-21, 2001.

[13] H. Shaikh,M. I. Khan and Y. Kelkar, "A Robust DWT Digital Image Watermarking Technique Basis On Scaling Factor", International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, No.4, August 2012.

[14] N. Bisla and P. Chaudhary, "Comparative Study of DWT and DWT-SVD Image Watermarking Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013.

[15] S. Pereira, S. Voloshynovskiy, M. Madueno, S. Marchand-Maillet and T. Pun, "Second Generation Benchmarking and Application Oriented Evaluation", Information Hiding Workshop III, Pittsburgh, PA, USA, April 2001.

[16] P. Meerwald and S. Pereira, "Attacks, Applications and Evaluation of Known Watermarking Algorithms with Checkmark", SPIE Symposium, San Jose, CA, USA, 2002.

AUTHOR PROFILES

Assoc. Prof. Safey Ahmed ShehataAbdelwahab: Received his B.Sc. in Electronics and Communicationsform Engineering Faculty – Cairo University in 1992. He received his M.Sc. andPh.Din Systems & Computers Engineeringform Engineering Faculty – Al-Azhar University in 1998, 2003. His interests are: Digital Image and Digital Signal Processing, Fuzzy Logic, Design of Microcontroller based instruments, Design of radiation measurement instruments, Software programming for interfacing and data acquisition, Embedded Systems, Developing ICT- Based Materials, Design of FPGA based instruments, Computers.