Image Contents Verification Algorithm using Transform Domain Techniques

S. S. Nassar, N.M.Ayad
Nuclear Research Center,
Atomic Energy Authority
Abo zabal, Inshas, P. O. Box
13759 Egypt, phone:

M.H. Kelash, O. S. Faragallah, F. E. Abd-Elsamie
Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt

M. A. M. El-Bendary
Faculty of Industrial Education,
Helwan University, Egypt

ABSTRACT

The rapid growth of digital multimedia and Internet technologies has made data security as an important issue in digital world. Encryption techniques are used to achieve data confidentiality, and this paper proposes a novel integrity verification method for images during transit. The confidential image is first divided into dedicated number of blocks; a discrete transform domain algorithm is used to embed a block based mark of the same image in another block according to a specific algorithm. In this work, the popular discrete transform domains, such as the discrete cosine transform (DCT), discrete Fourier transforms (DFT), and discrete wavelet transform (DWT) are examined individually. Different image analyses and comparisons are verified to examine the suitability of proposed algorithm with these domains. The discrete cosine transform (DCT) proved to be more efficient transform domain used with the proposed scheme. Higher sensitivity to simple modifications makes proposed scheme more applicable tool for image integrity verification with hyper secure data transformations such military and nuclear applications.

Keywords

Information security, Integrity, Image verification, Authentication, Digital Watermarking, DCT, DFT, DWT, MSE, PSNR, Correlation , Noise

1. INTRODUCTION

In real life scenarios like forensic, medical, broadcasting, a military, and nuclear; content verification and identity authentication are much more of a concern. Because of rapid advance in image processing techniques, people can easily modify the image content, so it should be focused on the capability of the watermarking schemes to be more sensitive to detect any intentionally (forgeries and masquerade) or unintentionally modifications. For example, the staff in a military field always has to be sure about the authenticity and content integrity of the digital images before planning any action. Also nuclear data through its transmission should be treated in the same manner. For all such cases fragile watermarking schemes have been used successfully [1]-[2].

Digital watermarking is a method to approve the owner identification and protect the copyright and integrity of multimedia data content. Digital watermarking techniques are classified according to various criteria like robustness, perceptibility, and embedding and retrieval methods. Robustness is an important criterion which means the ability of watermark to resist common image processing operations. Watermarking techniques based on robustness can be further divided into three main categories; Robust, Fragile, and Semi-fragile. A robust watermark is used to protect the copyright because it is designed to resist various kinds of manipulation to some extent, provided that the visual acceptability and commercial value of the altered images is retained [3-5]. On the contrary a fragile or semi-fragile watermark is used to verify the authenticity and content integrity in the sense that, when attacked, the embedded watermark should be entirely or locally destroyed [6].

Semi-fragile watermarking has properties of both fragile watermarking and robust watermarking, which can authenticate the reliability of digital contents [1].

In 2009, Chen et al., [7] proposed a spatial domain watermarking technique based on the idea of incorporating block-wise dependency information in watermarking procedure for thwarting VQ attack without compromising on localization capabilities of the scheme. Bhattacharya et. al. [8] proposed a new approach which makes use of both fragile and robust watermarking techniques. Wolfgang and Delp developed an authentication method that embeds bipolar m-sequence into blocks watermarks are generated from the checksum of pixel values excluding LSB. [9]. And Many semi-fragile watermarking schemes for image authentication have been proposed [10-13]. In this work a scheme for achieving image content integrity by exploiting a transform domain technique to embedding an assigned block based feature of original image into another dedicated block. A valuable comparison is introduced between commonly used frequency domain transforms (DCT, DFT, and DWT) to determine which one of those domains is more applicable, and has acceptable image analysis results. Section 2 provides a review on commonly used frequency domain transforms. The proposed scheme is described systematically in section 3. The results analysis and comparisons are presented in Section 4. Section 5 concludes the paper with future trends.

2. The TRANSFORM DOMAINS

Frequency domain techniques have proved to be more effective than spatial domain techniques in achieving higher embedding performance. The most popular and commonly used frequency domain transforms are Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Discrete Fourier transform (DFT). Most of the transform domain techniques embed the information into the transform coefficients of the cover image, and after the modification of the coefficients, the image is converted back into the spatial domain [14-16].

2.1 Discrete-Cosine Transform

The DCT separates the image into parts of different importance. It transforms image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components (Fl, FM, and FH) as shown in figure 1. In low frequency sub-band, much of the signal energy lies at low frequency which contains most important visual parts of the image, while in high frequency sub-band, high frequency components of the image are usually removed through compression [17].

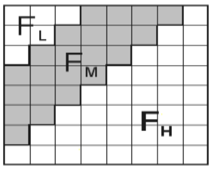

Fig1: Definition of DCT Regions

So the secret message is embedded by modifying the coefficients of the middle frequency sub-band, so that the visibility of the image will not be affected. The general equation for a 2D (N by M image) DCT is defined by the following equation:

$$C(u,v) = a(v)\sum_{i=0}^{N-1}[a(u)\sum_{i=0}^{N-1} x_i \cos\left(\frac{(2i+1)u\pi}{2N}\right)]\times \cos\left(\frac{(2i+1)v\pi}{2N}\right)$$

(1)

Where u, v = 0, 1, 2….N-1

2.2 Discrete Fourier Transform

The DFT is the primary tool of digital signal processing. For a 2-dimensional signal $f(x,y)$ of size M x N, the transform and its inverse are defined by [16]:

$$F(u,v) = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)e^{-j2\Pi(ux/M+vy/N)}$$

(2)

$$f(x,y) = \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} F(u,v)e^{j2\Pi(ux/M+vy/N)}$$

(3)

The discrete Fourier transform of an image is generally complex-valued, resulting in a magnitude and phase representation for the image. The watermark can be added to either the phase or the magnitude. Many watermarking techniques use the DFT amplitude modulation because of its shift invariant property but the phase modulation is more used because it is more important than the amplitude of the DFT for the intelligibility of an image.

2 .3 Discrete Wavelet Transform

The DWT separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. This process can then be repeated to a compute multiple "scale" wavelet decomposition, as in the scale 2 DWT shown below in Figure 2 [18].

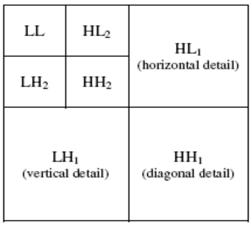

Fig 2: Scale 2 DWT

The discrete wavelet transform (DWT) we applied in this research is Haar-DWT. In Haar-DWT the low frequency wavelet coefficients are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels. A signal is passed through a series of filters to calculate DWT.

3. PROPOSED VERIFICATION ALGORITHM

The model proposed in this paper is an attempt that can be used as image content verification scheme, and it may seem like as a fragile watermarking in the main object (Integrity approval), but it different in depending on an internal block based marks instead of an external watermark. The model can be divided into two sub modules, where one module deals with marking process and the other module deals with verification process. The models are explained in a step-wise procedure below.

3.1 Marking Process

This section presents the steps of marking the transmitted data. The algorithm uses the confidential data such as image, as an input and the output will be a signed block based image, which appears to be the same as the original image. Assuming original image is a standard gray scale image of size (M*N) for example. The remarking algorithm of the transmitted data steps are described as in the following;

STEP 1- Input the original image (f), and then divide it into two equal halves (f1=f2). Then (f1) and (f2) are divided to (8×8) non-overlapping blocks of pixels.

STEP 2- Working from left to right, top to bottom through f1, DCT is applied to each block.

STEP 3- Working from left to right, top to bottom through (f2), row k; (k= 1,2,3,…8), and column k of block (s); (s=1,2,3,…..,M*N/128) are embedded instead of row k, and column k of the transformed DCT blocks in the same position(s) through (f1).

STEP 4– Working from left to right, top to bottom through (f1), the inverse DCT is applied to each block.

STEP 5– Step2, and 3 are repeated, but here DCT is applied to each block of (f2), and row k, column k of original (f1) blocks are embedded instead of row k, and column k of the transformed DCT blocks in the same orders (s) through f2.

STEP 6– The inverse DCT is applied to each block of (f2).

STEP 7– After applying inverse DCT process in steps3, and 5 the two halves of image are assembled to produce a block based marked image (x).

In this work, the proposed scheme is implemented with the popular transform domains as mentioned earlier. So in case of DFT the same pervious steps are approximately implemented. In case of DWT, the situation is quite different, which a 2-level Haar DWT is applied to each block which result in formation of four bands i.e. LL, HL1, LH1 and HH1 of size (4*4) as shown in figure 6. The approximation band LL is selected for embedding a mark of the same order block in the second half of image.

3.2 Verification Process

This model takes the marked image as an input, and implements the reverse process of embedding scenario to reconstruct the true original image in case of no modification occurs through transit. The following steps are describing the flow of extraction process;

STEP 1– Input the marked image

STEP 2- Divide the marked image (z) into two equal halves (z1=z2). Then (z1) and (z2) are divided to (8×8) non-overlapping blocks of pixels.

STEP 3– Working from left to right, top to bottom through (z1), DCT is applied to each block.

STEP 4– Row k and column k of (z1) blocks are embedded instead of row k, and column k of the blocks in the same position(s) through (z2).

STEP 5 – The inverse DCT is applied to each block of (z1).

STEP 6 – Step3, and 4 are repeated, but here DCT is applied to each block of (z2), and row k, column k of (z2) blocks are embedded instead of row k, and column k of the blocks in the same positions (s) through (z1).

STEP 7– The inverse DCT is applied to each block of (z2).

STEP 8– After applying inverse DCT process in Steps5, and 7 the two halves of image are assembled to produce an original image in case of no modification occurred.

4. RESULT ANALYSIS AND COMPARISONS

Simulation experiments were established in MATLAB R2013a with windows7 environment, and performance of proposed model was evaluated in case of DCT, DFT, and DWT. All experiments were implemented on standard gray scale image (cameraman.tif) with size of (256*256) as an original image, which is shown in Figure 4.

Fig 4: Original image

4.1 Marking Process

In this paper the performance analysis of proposed scheme are evaluated based on some quality metrices, which are calculated, and discussed for every transform domain Some of these image quality metrics are defined briefly as follow;

- ***The image histogram analysis:*** is one of the most important methods of the image quality evaluation which gives the relative frequency of occurrence of each pixel value in an image. Figures 5, 6, and 7 show Original image, and Watermarked image with their histograms for every transform domain.

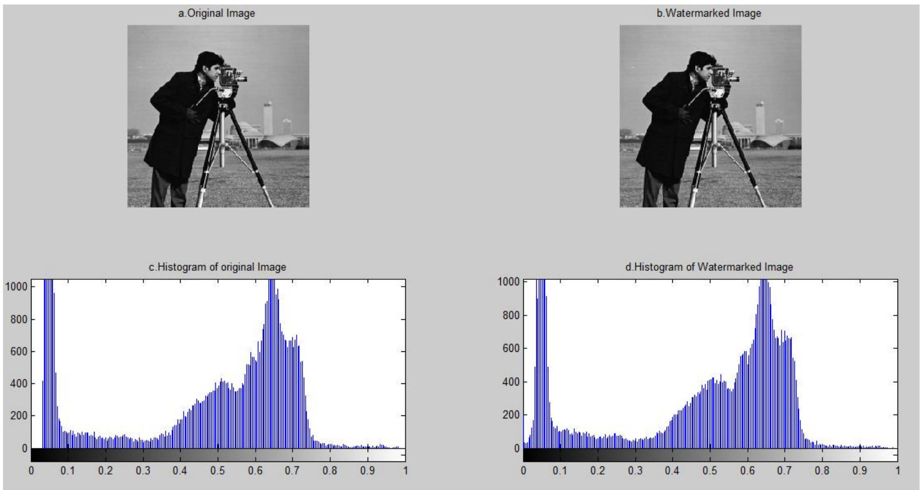

Fig 5: Original image, its histogram, and Watermarked image, its histogram in case of DCT

The results shown in figures 5, 6, and 7 indicate that; proposed scheme with DCT domain verifies the most acceptable results related to imperceptibility, and image histogram. The original and watermarked images appeared to be the same, and their histograms are approximately similar.

- ***Correlation (C)***

This tool used to evaluate the degree of closeness between the Original image and the Watermarked image, so it gives a direct measure of proposed algorithm efficiency. The most efficient algorithms produce images with correlation ratios more close to unity.

The block based correlation between all blocks (1024 blocks) of Original image, and Watermarked image in case of DCT, DFT, and DWT are shown in figures 8, 9, and 10 respectively.

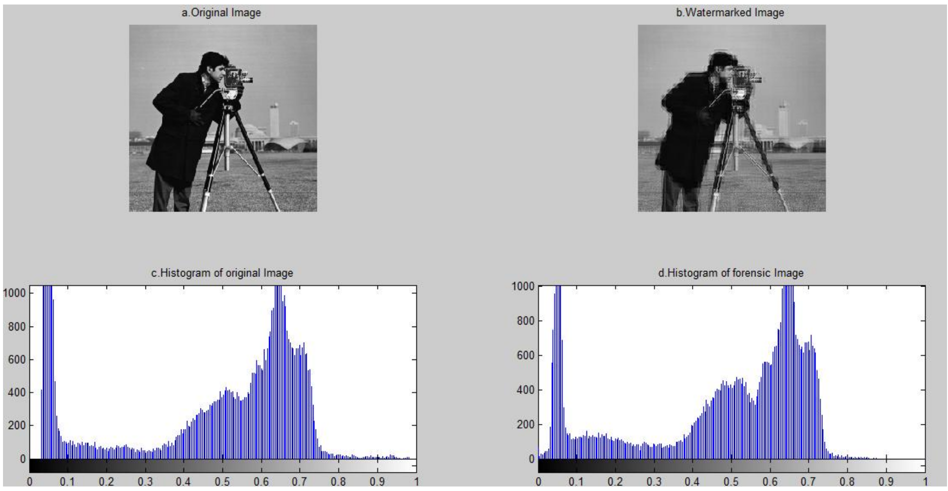

Fig 6: Original image, its histogram, and Watermarked image, its histogram in case of DFT

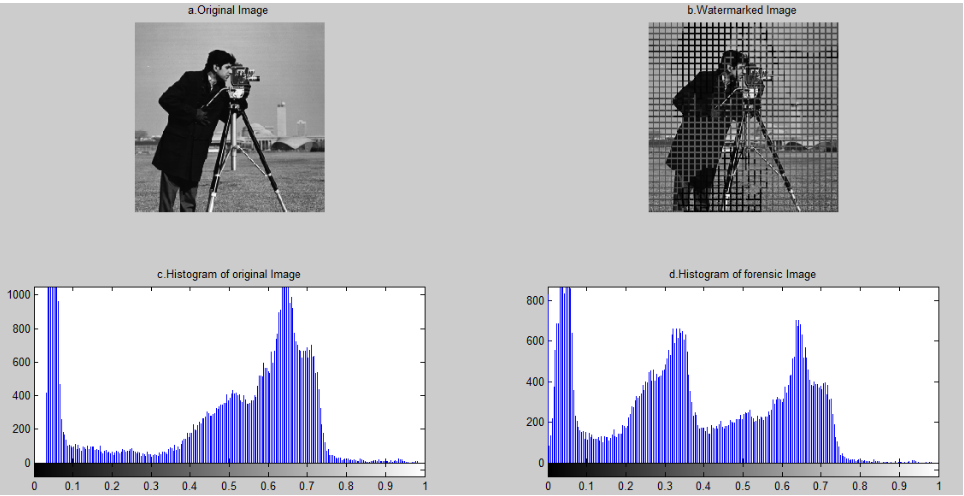

Fig 7: Original image, its histogram, and Watermarked image, its histogram in case of DWT

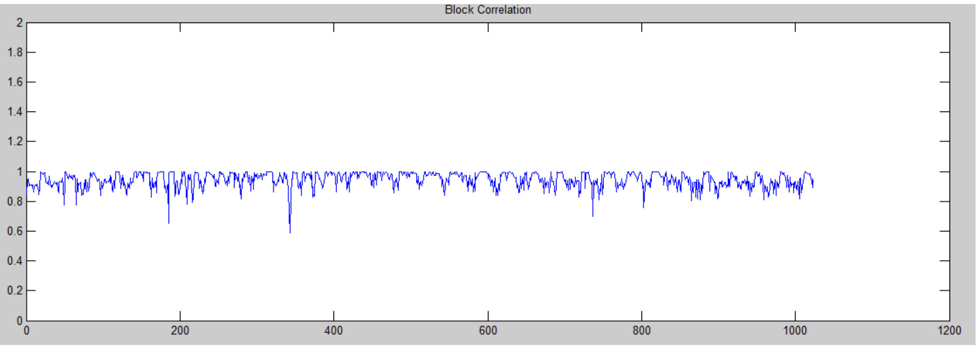

Fig 8: Block Correlation in case of DCT

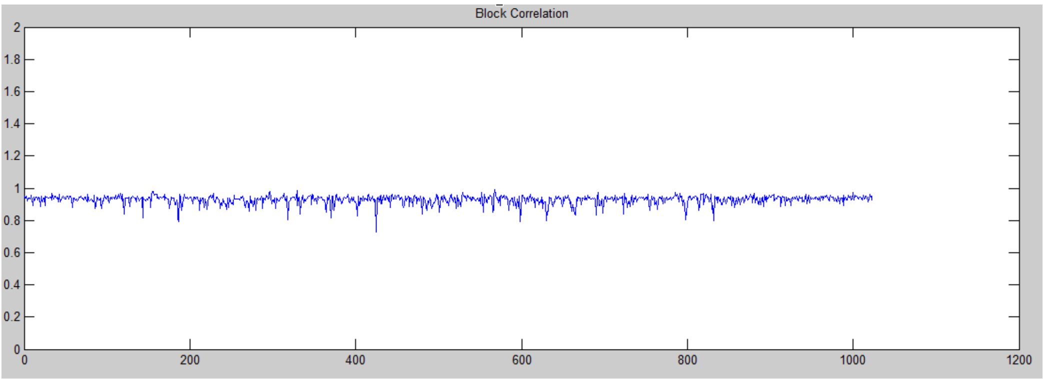

Fig 9: Block Correlation in case of DFT

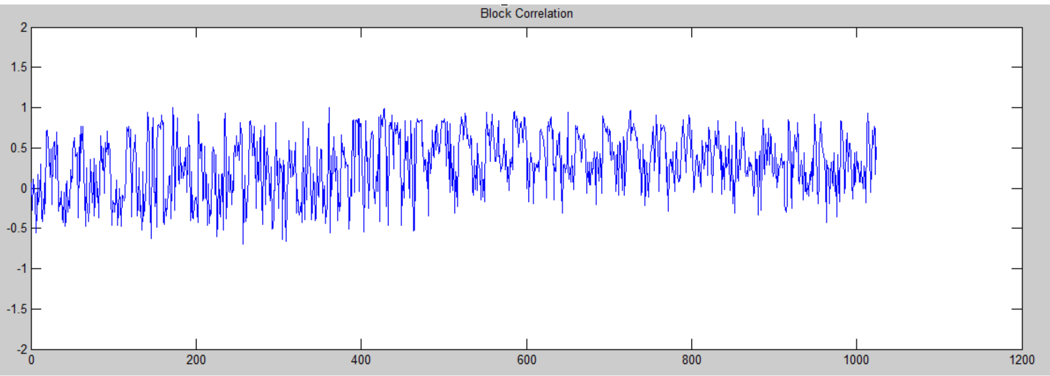

Fig 10: Block Correlation in case of DWT

As shown, and by comparing results of figures 8, 9, and 10, the proposed scheme using DCT algorithm verify best results related to block by block correlation. In which the majority of blocks correlation ratios are nearest to unity. The results related to DFT seem to be less than those of DCT, and worst results are obtained in case of using DWT algorithm. The average image correlation ratio between the whole Original and Watermarked image are calculated with another quality metrics and listed in table 1.

- ***Mean square error (MSE)***

MSE is one of the most frequently used for image quality measurement, and it can be defined as; the measure of average of the squares of the difference between the intensities of the Secret image and the Extracted Secret Image. It is mathematically represented in (4).

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(f(i,j)-f'(i,j))^2$$

(4)

Where f (i, j) is the original Secret Image and f' (i, j) is the Extracted Secret Image. Higher value for MSE means that the image is of poor quality.

- ***Peak signal to noise ratio (PSNR)***

This metric is used for discriminating between the Secret image and the Extracted Secret Image. The easy computation is the advantage of this measure. It is formulated in (5):

$$PSNR(dB) = 10\log\left(\frac{255^2}{MSE}\right)$$

(5)

A low value of PSNR shows that the extracted image is of poor quality [19].

The correlation between Original image, and marked image, MSE, and PSNR are calculated for the three used transform domains and listed in table 1. Higher correlation ratio, higher PSNR, and lower MSE are obtained in case of implementing proposed scheme using DCT algorithm.

Table 1 Image quality metrics with different transform domains

Transform Domain	**Image Quality Metrics**		
	MSE	**PSNR**	**C**
DCT	19.0397	35.3682	0.997
DFT	35.0269	32.7208	0.9781
DWT	3603	12.5974	0.6060

4.2 Verification Process

Suppose the medium is of free error, and no attacks tampered the marked image. The extraction process related to DCT domain is chosen to be implemented only, because it gives best performance results in the embedding process. Figure 11 shows Original image, Extracted image, and their histograms. In case of no attacks or any modification reasons the original image is extracted successfully.

The image quality metrics at the same conditions are listed in table 2, which show that the original image in case of no subjection to any type of modification can be extracted successfully and image integrity is verified.

Due to each block is subjected to DCT and its inverse with their uniform quantization and variable length coding two times, and at every time some error is introduced during quantization resulting in blocking artifacts in the decoded image. So, a very small difference in correlation ratio between the Original image and Extracted image is introduced.

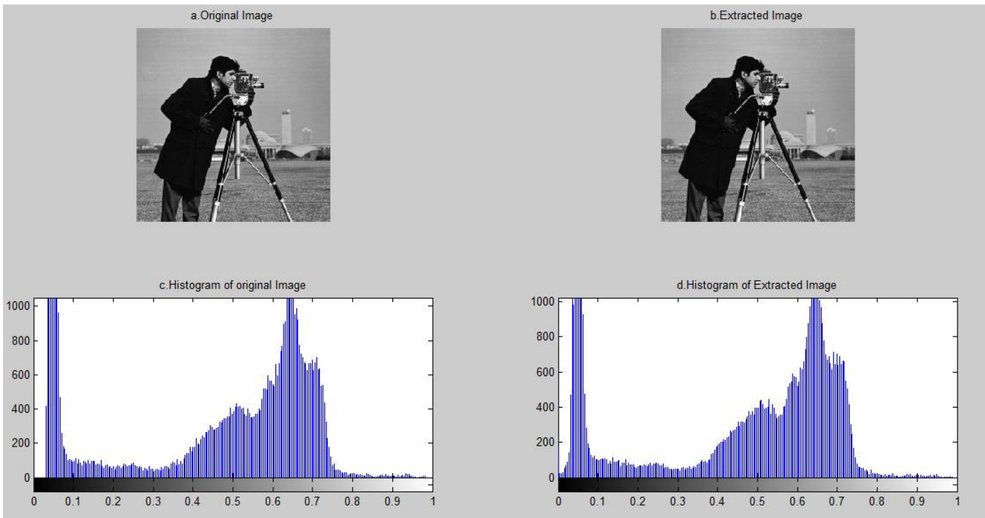

Fig 11: Original image, its histogram, and Extracted image, its histogram in case of DCT

Table 2 Image quality metrics with DCT domain

Transform Domain	Image Quality Metrics		
	MSE	PSNR	C
DCT	16.6306	36	0.998

4.3 Authentication Verification

The proposed model applicability can be tested by implementing the marked image and a copy of original image (not marked) directly to extraction algorithm, and checking the final output. Figure 12 show the output in case of implementing a copy of an original and not marked image, which seems to be a distorted image hidden behind a grid.

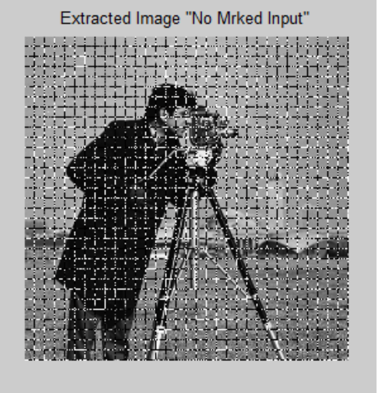

Fig 12: Extracted image in case of No Marked Input

But in case of implementing the marked image to the extraction algorithm of proposed model the output image looks like the true original image as shown in Figure 13.

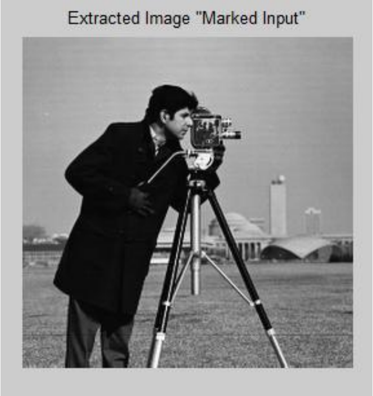

Figure 13 Extracted image in case of Marked Input

So the proposed model succeeded in verifying image authentication, in which the only intended receiver who has the extraction algorithm can, differentiate between the received marked or authenticated image and the other copies of received original image.

4.4 Adding Noise

This scenario investigates the applicability of the proposed model in sensing any image modification (integrity verification) in case of adding two different noise types with different values such as; Gaussian white noise and salt-and-pepper noise. The received marked image and the extracted image are compared in case of Gaussian white noise of mean 0 and Variance values (0.0001, 0.001, and 0.01) and shown in figures 14, 15, and 16 respectively.

The same two images are also compared in case of salt-and-pepper noise with rate (0.005, and 0.05) and shown in figure 17, and 18 respectively.

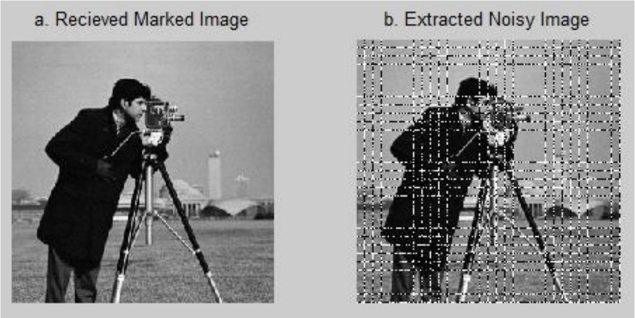

Fig 14: Received Marked Image and Noisy Extracted Image in case of Gaussian Noise (Mean 0 and Variance 0.0001)

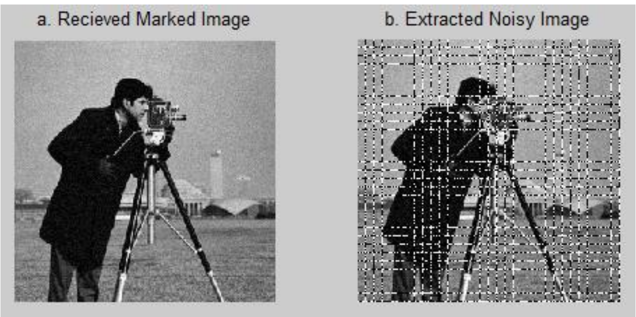

Fig 15: Received Marked Image and Noisy Extracted Image in case of Gaussian Noise (Mean 0 and Variance 0.001)

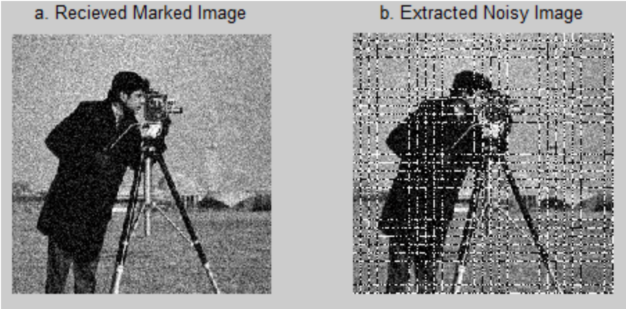

Fig 16: Received Marked Image and Noisy Extracted Image in case of Gaussian Noise (Mean 0 and Variance 0.01)

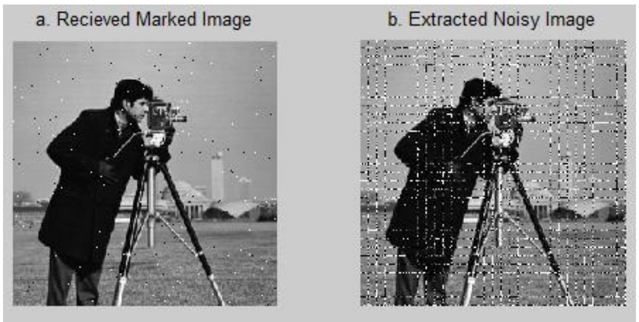

Fig 17: Received Marked Image and Noisy Extracted Image in case of Salt-and-Pepper Noise (Rate 0.005)

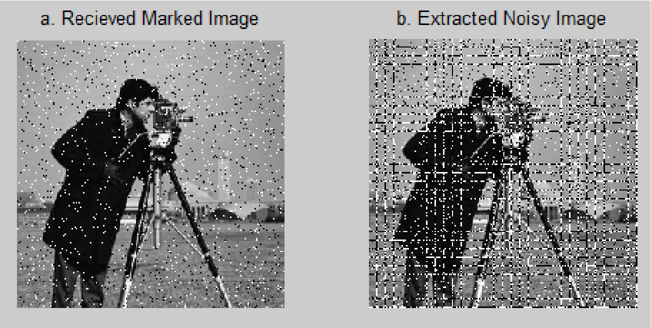

Fig 18: Received Marked Image and Noisy Extracted Image in case of Salt-and-Pepper Noise (Rate 0.05)

The results related to two noise types with different values indicate that; the proposed model gives a major indication to any small image modification (Integrity Verification).
This seems clearly in figure 14, in case of Gaussian Noise (Mean 0 and Variance 0.0001), which the received marked image appears to be not subjected to any noise (clear original image), and the recipient cannot visibly detect this noise modification but the extracted image (using proposed model) shows a major change compared to marked image. At the same time the proposed model has an acceptable level of robustness, in case of different level of image modifications (higher noise levels) as shown in pervious results.

5. CONCLUSION

In this paper, a secure image integrity verification scheme is proposed. The scheme is based on a transform domain for embedding an internal block mark into another block of an image. The popular transform domains are examined, and DCT proved to be more applicable according to imperceptibility concept and performance analysis. Because of its higher sensitivity to any tamper modification of data, it can be concluded that ,the proposed scheme is more beneficial In case of dangerous and higher secure data such as; military, and nuclear data from the data integrity point of view. Moreover the proposed scheme can be used to verify image authentication in which the only marked image can be extracted successfully and efficiently. Finally this model can subjected to more improvement in the future to get more accurate results and efficient performance.

6. REFERENCES

[1] Zhou, H., H. Li, et al. "Semi-fragile Watermarking Technique for Image Tamper Localization."International Conference on Measuring Technology and Mechatronics Automation, 2009 519-523.

[2] E. T. Lin, and E. J. Delp (1999), “A review of fragile image watermarks”, In Proceedings of the ACM multimedia and security workshop, pp. 25–29.

[3] R. Petrovic,"Digital Watermarks for Audio Integrity Verification", Serbia and Montenegro, Nis, September 2005 28-30.

[4] W.H. Chang and L.W. Chang,"Semi-Fragile Watermarking for Image Authentication, Localization, and Recovery Using Tchebichef Moments", Communications and Information Technologies (ISCIT), 2010.

[5] S. Radharani, M. L. Valarmathi (2010), “A study of watermarking scheme for image authentication”, International Journal of Computer Applications, Vol. 2, No.4, pp. 24-32.

[6] C.-T. Li, and F.-M. Yang (2003), "One-dimensional neighborhood forming strategy for fragile watermarking", Journal of Electronic Imaging, Vol.12, No. 2, pp. 284-291.

[7] W.C. Chen, and M.S. Wang (2009), "A Fuzzy c-Means Clustering based Fragile Watermarking Scheme for Image Authentication", Expert Systems with Applications, Volume 36, Issue 2, Part 1, pp. 1300-1307.

[8] Ankan Bhattacharya, Sarbani Palit, Nivedita Chatterjee, and Gourav Roy (2011), "Blind assessment of image quality employing fragile watermarking", 7th International Sym. on Image and Signal Processing and Analysis (ISPA 2011) Dubrovnik, Croatia, pp. 431-436.

[9] R. B. Wolfgang and E. J. Delp, \A Watermark for Digital Images", IEEE Proc. of ICIP, Laussane, Switzerland, Oct 1996.

[10] M.j. Tsai and C.C Chien,"A Wavelet-Based Semi-Fragile Watermarking with Recovery Mechanism", IEEE International Symposium on Circuits and Systems, May 2008pp.3033-3036.

[11] D. Zhang and Z. Pan, "A contour-based semi-fragile image watermarking algorithm in DWT domain," Proc. ETCS vol. 3, 2010, pp. 228-231.

[12] K. Maeno, S. Qibin, S.F. Chang and M. Suto "New semi-fragile image authentication watermarking techniques using random bias and nonuniform quantization". IEEE Trans Multimedia;8(1) 2006:32–45

[13] X. Wang, "A novel adaptive semi-fragile watermarking scheme based on image content," ACTA AUTOMATICA SINICA vol. 33, no. 4, 2007 pp. 361-366.

[14] C. Shoemaker, Rudko, "Hidden Bits: A Survey of Techniques for Digital Watermarking" Independent StudyEER-290 Prof Rudko, Spring 2002.

[15] A. H. Tewfik " Digital watermarking ", San Mercury News, 14 August , 2000.

[16] H. R. Myler "Image Transforms",http://ee.lamar.edu/gleb/dip/03%20-%20Image%20Transforms.pdf, April 2002.

[17]K.B.ShivaKumar,K.B.Raja, R.K.Chhotaray, SabyasachiPattnaik, "Coherent Steganography using Segmentation and DCT",IEEE-978-1-4244-5967-4/10/$26.00 ©2010.

[18] C. Shoemaker, Rudko, "Hidden Bits: A Survey of Techniques for Digital Watermarking" Independent StudyEER-290 Prof Rudko, Spring 2002.

[19] Sumathi Poobal, G. Ravindran,"The Performance of Fractal Image Compression on Different Imaging Modalities Using Objective Quality Measures," International Journal of Engineering Science and Technology (IJEST), Vol. 2, Issue 1, Jan-Feb 2011, pp 239-246.

7. AUTHOR'S PROFILE

S. S. Nassar is an Assistant Lecturer and Network Security Specialist in Department of Reactors, Nuclear Research Center (NRC), Inshas, Egypt. He received his Master of Computer Science and Engineering in 2011 from Faculty of Electronic Engineering, Menufia University, Menouf, Egypt. Currently, he is a PhD student in the same college. His research interests are in encryption techniques, steganography, watermarking, forensics, and wireless networks.