Robust Watermarking Technique based on DCT to Protect the Ownership of DubaiSat-1 Images against Attacks

Saeed AL-Mansoori[1] **and Alavi Kunhu**[2]**,**
S_Mansoori@eiast.ae
[1]Image Processing Department, Emirates Institution for Advanced Science & Technology (EIAST), UAE
[2]Department of Electronic Engineering, Khalifa University of Science, Technology and Research (KUSTAR), UAE

Summary
Nowadays, with the rapid growth of technologies and the prevalence of network communication, new challenges raises to protect the multimedia data transmission on the World Wide Web (internet). Data security is one of the main important needs these days, especially in the field of remote sensing. Emirates Institution for Advanced Science and Technology (EIAST) as an example provides a satellite images captured by DubaiSat-1 satellite to customers inside the UAE including government agencies, universities, research centers, and distributed also outside the region. To deal with the issue of data security, the concept of watermarking has been introduced. The idea of watermarking is to embed a secret message, watermark inside an image and to increase the digital data security. The aim of this study is to hide an entire pattern as a watermark such as an organization's logo (or trademark) directly into the original DubaiSat-1 satellite image. This will prevent any unauthorized manipulation to the image data. This secret watermark is used for copyright protection and ownership authentication for (EIAST). This study will be based on Discrete Cosine Transform (DCT) to provide an excellent protection and highly robust under flipping, noise, resize and rotation attacks.

Key words:
Watermarking, EIAST, Discrete Cosine Transform (DCT), Peak Signal to Noise Ratio (PSNR), DubaiSat-1 Satellite, attacks.

1. Introduction

Watermarking is a combination of electrical (image and signal processing) and computer science fields which is the process of hiding information (i.e data) which can be a signature, logo, image, label, text into a multimedia object such as text or image or audio or video in such away it can be extracted later to show the ownership and authentication of an object. Generally, there are three main parts for watermarking scheme; the watermark, encoder, and decoder. Figure 1 shows a basic block diagram of watermarking process. A block diagram (figure1) shows the basic principles stages in digital image watermarking process; starting from generating and embedding the watermarked logo and information into the original image to produce a watermarked signal and this process called "encoding", then the watermarked signal transmitted to somebody.

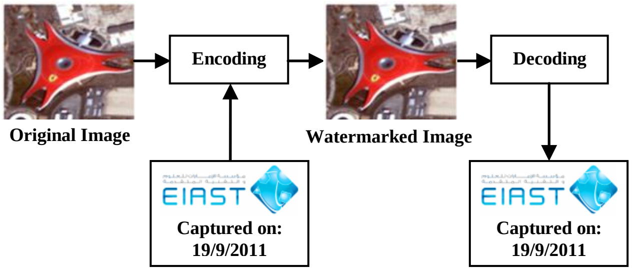


Fig. 1 Basic block diagram of watermarking process

Any modification attempt to the transmitted signal is considered an "attack". The most common types of attacks are flipping, rotation, cropping, JPEG compression, and scaling. This stage examines the robustness of the algorithm implemented. Finally, detection process is applied to watermarked signal to extract the information embedded into the original image.

Section 2 discusses the DCT domain watermarking. Section 3 describes the research methodology while section 4 explains the proposed algorithms; section 5 highlights the quality testing assessment; section 6 discusses the output of the methodology and explains the results. Section 7 concludes the work done and gives an estimation of our future work.

2. DCT DOMAIN WATERMARKING

Discrete Cosine Transform is used in many digital signal processing applications, which can be classified into Global DCT watermarking and Block based DCT watermarking [1]. DCT is a frequency linear transformation domain approach, which is characterized as more robust against attacks compared to the spatial (time) domain approach. DCT is a process of converting a signal to its frequency components. Such approach is robust against some image processing operations (i.e. attacks). Figure 2 presents a block diagram that explains the main idea of discrete cosine transform for image. It is noticed that the energy focusing in the upper left corner (i.e. DC component). The initial popular step in DCT is to segment

Manuscript received June 5, 2012
Manuscript revised June 20, 2012

an image into non-overlapping blocks where (8 x 8) blocks are commonly used and applies DCT to each block. This will divide an image into three main regions as shown in figure 2; low frequencies sub-band (F_L), middle frequencies sub-band (F_M) and high frequencies sub-band (F_H) which makes it easier to select the band in which the watermark is to be inserted. Many studies indicate that the middle frequency bands are commonly chosen, because embedding the watermark in a middle frequency band does not scatter the watermark information to most visual important parts of the image [2]. The third step is to apply block selection criteria based on the knowledge of Human Visual System (HVS). In addition, the fourth step applies coefficient selection criteria (e.g. highest, middle, lowest).The literature survey reveals that mostly DCT based schemes differ either in these two steps (third and fourth). The remaining steps involves embedding the watermark by modifying the selected coefficients and finally applying inverse DCT transform on each block.

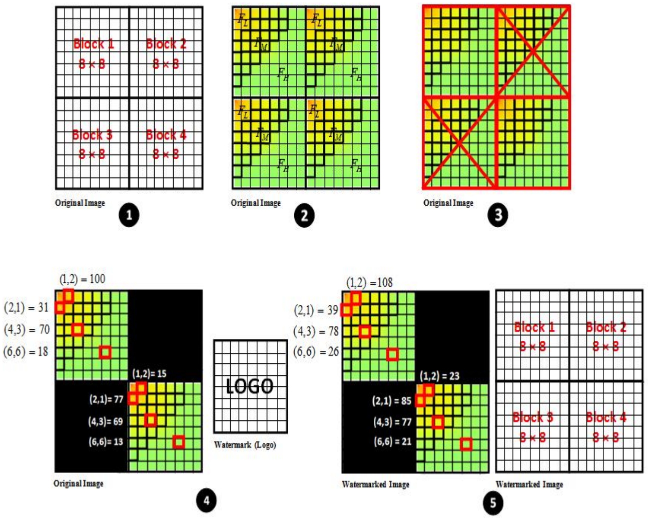


Fig. 2 General DCT Steps (when step size = 8)

It can be noticed that much of the signal energy lies at low-frequencies sub-band which contains the most important visual parts of the image [3]. Moreover, the high frequency components of the image are usually removed through compression and noise attacks. Therefore, watermark is embedded into an image by modifying the coefficients of the middle frequency sub-band, this is done so that the visibility of the image will not be affected, and the watermark will not be removed by compression. Researchers who deal with DCT can design their scheme by selecting the best frequency band depending on the expected attacks.

In 2010 [2], Tribhuwan and Vikas proposed a watermarking technique based on embedding a watermark (logo and name) into the middle frequency band of the Discrete Cosine Transform (DCT) blocks of the grey scale image. Their algorithm is slightly different from the traditional DCT. Adobe Photoshop was used to simulate the different attacking operations. JPEG compression, cropping and noise addition (Gaussian and Salt &Pepper) were the attacks used to evaluate the scheme's robustness. The proposed scheme gave best results for the JPEG compression attack. Through this paper, Tribhuwan proves that his scheme is better than Vikas scheme [4] when using a very high JPEG compression. The PSNR values were approximately 42dB for the Lena image under different attacks.

3. Research Methodology

In this paper, we are proposing the robust image watermarking algorithms for embedding EIAST logo information in all DubaiSat-1 Satellite images. All the proposed watermarking algorithms are totally blind and do not need any host satellite images for logo information extraction process. To compromise between visual degradation and robustness the logo watermarking information was embedded in the low frequency of (8×8) DCT blocks. For each DubaiSat-1 image, we will first find out the best 8 locations for embedding the logo information inside each (8×8) DCT blocks, and will be based on the highest magnitude of first 16 lower frequency coefficients and will register its location as secret key.

The Discrete Cosine Transform (DCT) technique converts the image from spatial domain to frequency domain. This technique converts exactly each pixel value of the image to a frequency value. Thus, changing the value of the pixel when embedding information will not affect the quality of the image. Since, it does not affect the quality. This technique gives the system designer the advantage of having a wider range of pixel values to examine. Let us assume that ***f(i,j)*** be the grey-level of DubaiSat-1 image with size N_H pixels. Moreover, let ***w(i,j)*** be the binary converted and reshaped watermark gray logo of size N_W bits, which is usually much smaller compared to the host image size. To simplify the matter, let us assume that the host image size could accommodate integer copies of the watermark image.

4. Proposed Algorithms

The proposed watermarking algorithms embed watermark logo information inside each (8×8) Discrete Cosine Transform (DCT) block in the G channel of DubaiSat-1 color image. This operation is done based on a secret key. Here we have used DCT based Odd/Even technique to embed the watermarking information inside cover image.

In addition, we used (90 x 230) gray EIAST logo as the watermark information and (2304 x 2304) color satellite image as the Cover. In this algorithm, we first reshape and convert the (90 x 230) gray logo into (288 x 576) binary logo and then hide it in the G channel of host satellite image using DCT odd/even method.

- Algorithm 1 (Method 1A):

The proposed watermarking algorithm is based on embedding two bit of binary watermark logo information inside each (8 x 8) Discrete Cosine Transform (DCT) block in the G channel of DubaiSat-1 color image based on a secret key.

- Algorithm 2 (Method 1B):

This proposed watermarking algorithm embeds two copies of two bit of binary watermark logo information inside each (8 x 8) Discrete Cosine Transform (DCT) block in the G channel of DubaiSat-1 color image based on a secret key

- Algorithm 3 (Method 1C):

The proposed watermarking algorithm is based on embedding three copies of two bit of binary watermark logo information inside each (8 x 8) Discrete Cosine Transform (DCT) block in the G channel of DubaiSat-1 color image based on a secret key.

4.1 Embedding Algorithm

The proposed embedding algorithm as shown in figure 4 can be described as follows: Step 1, divide the host satellite image into N_{HB} (8 x 8) sub-blocks and find DCT transform, using equation 1 [5, 6].

$$O_k(u,v) = DCT\{o_k(i,j)\},$$
$$1 \le u \ , \ v \le 8 \ , \ 1 \le k \le N_{HB} \qquad (1)$$

$$O_k(u,v) = DCT\{o_k(i,j)\}, \textit{if } w(i,j) = 0 \textit{ then}$$
$$O_k(x,y) = \begin{cases} \Delta Q_{\circ}\left(\dfrac{O_k(x,y)}{\Delta}\right) & x,y \in H_k \quad 1 \le k \le N_{HB} \\ O_k(x,y) & x,y \notin H_k \quad 1 \le k \le N_{HB} \end{cases}$$
$$\textit{if } w(i,j) = 1 \textit{ then} \qquad (2)$$
$$O_k(x,y) = \begin{cases} \Delta Q_e\left(\dfrac{O_k(x,y)}{\Delta}\right) & x,y \in H_k \quad 1 \le k \le N_{HB} \\ O_k(x,y) & x,y \notin H_k \quad 1 \le k \le N_{HB} \end{cases}$$

Step2, Convert the grey watermark logo into binary watermark mask by doing decimal to binary conversion and reshaping. Step3, Hide binary watermark mask bits into host satellite image sub-blocks (8 x 8) using the embedding equations as follows [5, 6]:

Where 1 ≤ x, y ≤ 1, and Q_e indicate the even quantization and Q_o indicate the odd quantization to nearest number. Δ indicate the various scaling factor used for both quantization process.[5] Step4: Hide multiple copies of binary watermark mask depend on the size of both satellite host image and watermark logo by repeating step3 N times. Step5: Reconstruct the watermarked host satellite image using the inverse DCT transform of all sub-blocks of O(u,v).

4.2 Reconstruction Algorithm

The proposed reconstruction algorithm as shown in Figure 5 can be described as follows: Step1, Divide the watermarked satellite image into N_{HB} (8 x 8) sub-blocks and find DCT transform. Step2, Extract the binary watermark mask bits from DCT sub-blocks of watermarked satellite image using the extraction formulas are shown below [5,6]:

$$\begin{array}{l} \textit{if } Q\left(\dfrac{O_k(u,v)}{\Delta}\right) \Rightarrow \textit{Odd} \Rightarrow w(i,j) = 0 \\ \qquad\quad \Downarrow \\ \qquad\quad \textit{Even} \\ \qquad\quad \Downarrow \\ \qquad w(i,j) = 1 \end{array} \qquad (3)$$

Step3, Extract the multiple copies of the binary watermark mask by repeating step2. Step4, Convert extracted watermarked binary mask into grey watermark logo by converting each 8 bit of watermark binary mask bits into decimal number and reshaping. Step5, Extract the final watermark logo by averaging all the copy of reconstructed watermark logo, after discard the totally degraded watermark logo.

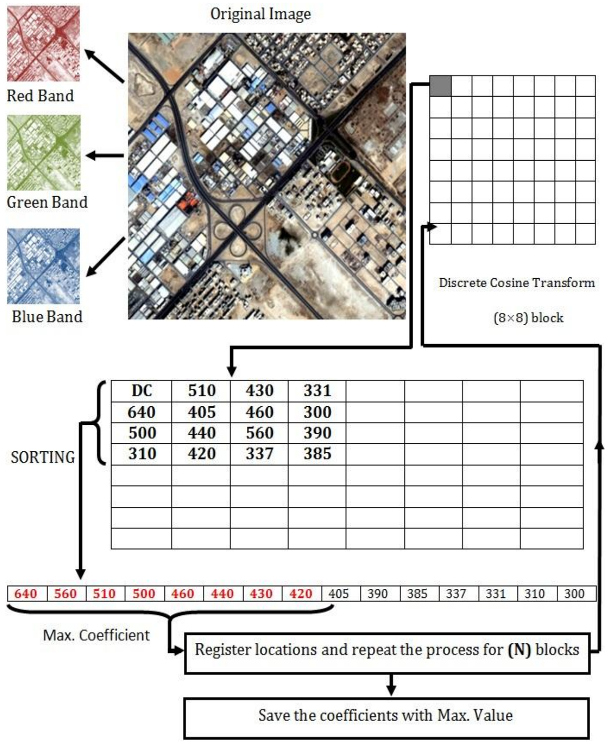


Fig. 3 Proposed DCT Algorithm

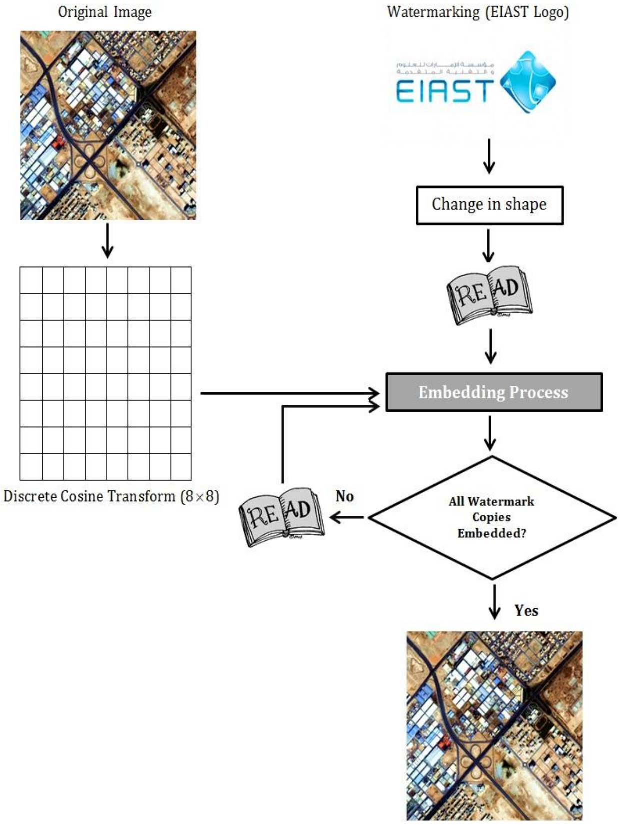

Original Image
Watermarking (EIAST Logo)
Change in shape
Embedding Process
Discrete Cosine Transform (8×8)
No
All Watermark Copies Embedded?
Yes

Fig. 4 Embedding Algorithm

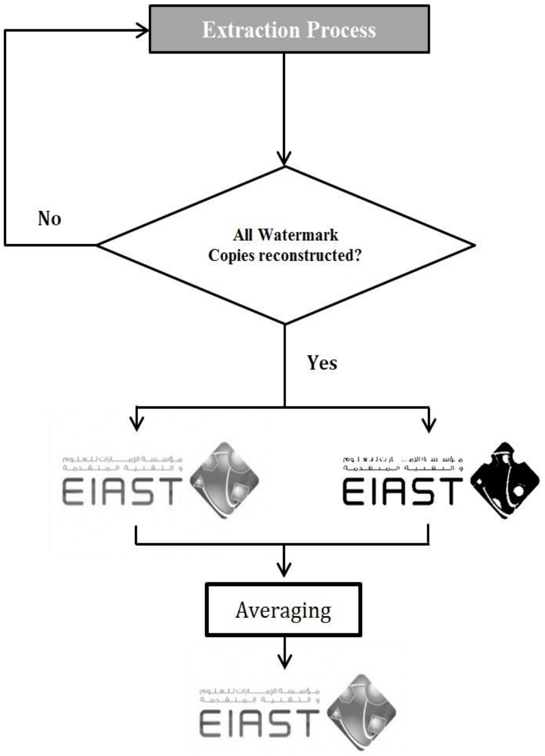


Fig. 5 Reconstruction Algorithm

5. Quality Test and Assessment

The process of determining the similarity level between original and watermarked image is called "Perceptual Similarity". A number of metrics are used to analyze the performance of watermarked image. In this study we used two different metrics to analyze the quality degradation of satellite images. The metrics measure quality degradation using pixel-based comparisons and widely applied for image quality assessment.

5.1 Peak Signal-to-Noise Ratio (PSNR):

This method that is commonly used for image quality metric, where PSNR is given by:

$$PSNR = 10 \log_{10} \frac{255^2}{Mean\ \ Sequare\ Error} \qquad (4)$$

The Mean Square Error is used to assess the quality of the image after different type of attacks. In this research, the watermarked image quality is assessed by calculating the MSE between the original and the watermarked image. The Mean Square Error (MSE) compares two images on a pixel-by-pixel basis. Mathematically, MSE for gray-scale images is expressed as;

$$MSE_{grey} = \frac{1}{xy}\sum_{x,y}(o_{x,y} - w_{x,y})^2 \qquad (5)$$

Where *o*, is the original image, *w* the watermarked images, *x* and *y* are the image pixels. In the case of colored images, the MSE is given as;

$$MSE_{colour} = \frac{1}{3xy}\sum_{x,y}(o_{r_{x,y}} - w_{r_{x,y}})^2 + (o_{g_{x,y}} - w_{g_{x,y}})^2 + (o_{b_{x,y}} - w_{b_{x,y}})^2 \; (6)$$

Where o_r, o_g , and o_b are the R, G and B components of the original colored satellite image, and w_r, w_g , and w_b are the R, G, and B components of the watermarked colored satellite image. This measure indicates how much degradation was introduced at a pixel based level. PSNR penalizes the visibility of noise in an image. Thus, two images that have the same quality will produce an infinite PSNR value.

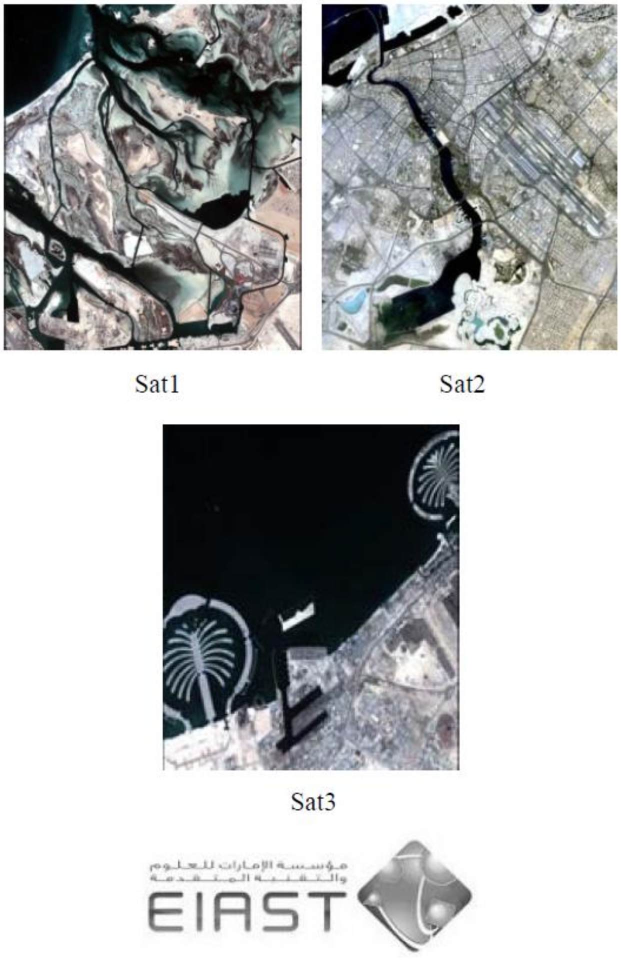
5.2. Structure Similarity Index Measurement (SSIM):

SSIM is a measure that compares local pattern of pixel intensities that have been normalized for luminance and contrast. Higher SSIM means, larger similarity between the compared images. The measured values between the original image and the watermarked should be 1, and a good watermarked image should be between 0.90 and 0.99, if the value reached 0.5 then the watermarked image quality will be considered as not acceptable.

Mathematically, SSIM is expressed as Where o is the original satellite image, w is the restored satellite image, L is the luminance, C represents contrast, and S is the structure. In addition, α, β, and γ are parameters used to adjust the relative importance of the luminance, contrast and structure components.

6. Results and Analysis

In this paper, we used three DubaiSat-1sample images for the testing purposes; Sat1, Sat2 and Sat3. EIAST logo that was used as a watermark is shown in figure 6. After the encoder process, watermarked image will be generated. In Human Visual System (HVS), it is ought to be no observable difference between watermarked and original image. Therefore, the watermarked image will be assessed via image quality parameter (PSNR) to evaluate the performance of the watermarked image. The best range commonly considered for PSNR is between 40 – 55 dB.



Sat1

Sat2

Sat3

Watermark used (Grey scale)

Fig. 6 DubaiSat-1 sample images and EIAST logo used in experiments

Table 1 shows the comparison between three proposed algorithms (1A, 1B, and 1C). It is presented in terms of Peak Signal –to- Noise Ratio by using two step sizes (Δ) = 8 and (Δ) = 16 for the three samples of DubaiSat-1 images (Sat1,Sat2, and Sat3). The highest PSNR value reached is 52.4770 dB, while the lowest PSNR value is 40.7745 dB. These values show that we are within the PSNR acceptable range. Images with step size (Δ) = 8 gives better PSNR values than images with step size (Δ) = 16. Furthermore, method (1A) gives better performance rather than other methods.

The next step is to verify the proposed watermarking methodology by simulating “attacks” and check the robustness of the algorithm. Moreover, it will illustrate the watermark strength and show how much it can resist attacks. Several types of attacks can be applied on the watermarked image, such as JPEG compression, cropping, filtering, rotation…etc. In our paper we will test our proposed algorithm against Flipping, Noise, Resize and Rotation attacks.

Table 1: PSNR between watermarked and original images

(PSNR)	Step Size (Δ) = 8			Step Size (Δ) = 16		
	Sat1	Sat2	Sat3	Sat1	Sat2	Sat3
Method (1A)	52.4770	51.8514	51.5144	46.2003	45.9560	45.6012
Method (1B)	49.3212	48.9066	49.2856	42.8748	42.8848	43.8745
Method (1C)	45.1939	47.1639	46.7964	40.7745	41.0940	40.7800

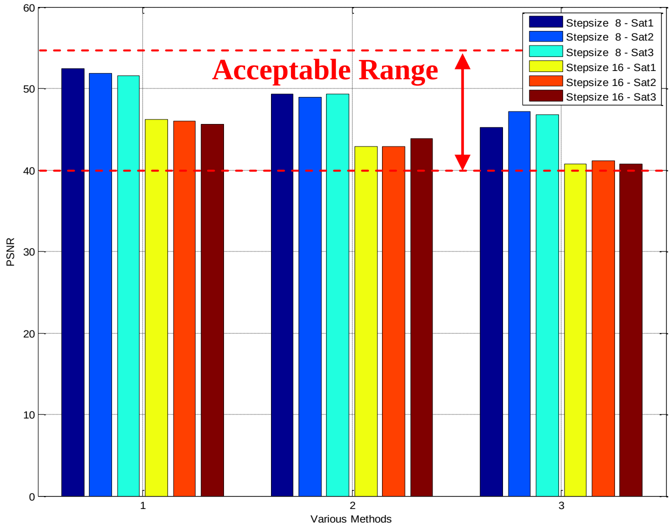


Fig. 7 PSNR performance of proposed methods

6.1 Flipping Attack

In the case of flipping attacks, we applied both horizontal and vertical flipping on the watermarked satellite images. Then the logo was retrieved from the attacked satellite images. The results of the flipping attack are shown below in Table 2 for all the three watermarking schemes.

Table 2: PSNR between retrieved and original Logos (Flipping Attack)

Logo Image	Flipping Attack (Δ = 8)		Flipping Attack (Δ = 16)	
Sat1	Horizontal	Vertical	Horizontal	Vertical
PSNR (Method 1A)	38.1228	38.1228	27.0069	27.0069
PSNR (Method 1B)	26.4014	26.4014	24.4671	24.4671
PSNR (Method 1C)	23.9151	23.9151	22.0355	22.0355

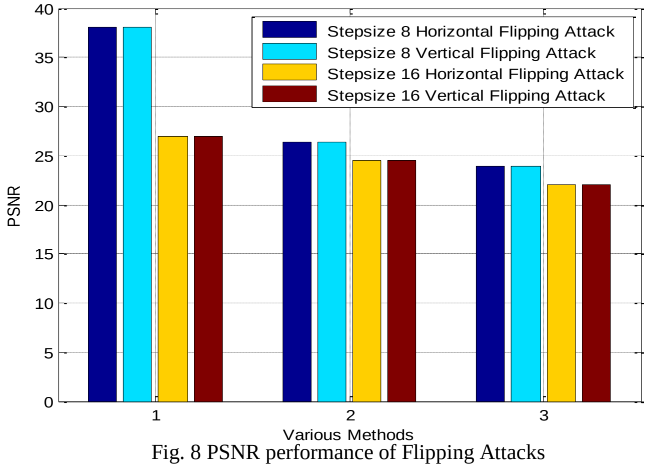


Fig. 8 PSNR performance of Flipping Attacks

This study shows that horizontal and vertical flipping's gives the same PSNR performance, while the main factor that may affects the PSNR is the step size. In our case, (Δ) = 8 gives higher PSNR than (Δ) = 16 for the three proposed methods (1A, 1B, and 1C). However, method (1A) shows higher PSNR compared to other methods. The highest PSNR obtained for this attack is 38.1228 when (Δ) = 8.

6.2 Noise Attacks

Various noise attacks were applied such as Gaussian, salt and pepper to the watermarked satellite images. The performance of recovered logo information was then analyzed. The results of the noise attack have been shown below in Table 3 for all the three watermarking schemes.

Table 3: PSNR between retrieved and original Logos (Noise Attack)

Logo Image	Noise Attack (Δ = 8)		Noise Attack (Δ = 16)	
Sat1	Gaussian	Salt and Pepper	Gaussian	Salt and Pepper
PSNR (Method 1A)	12.6245	9.2623	20.6746	10.4982
PSNR (Method 1B)	9.3141	9.3107	12.7114	09.4074
PSNR (Method 1C)	5.7808	5.7258	09.5906	05.7644

It can be noticed that, salt and pepper noise had a significant effects on the retrieved watermark logo, such that, the logo could not be retrieved in some cases. Method (1A) proved to be the most robust against noise attack.

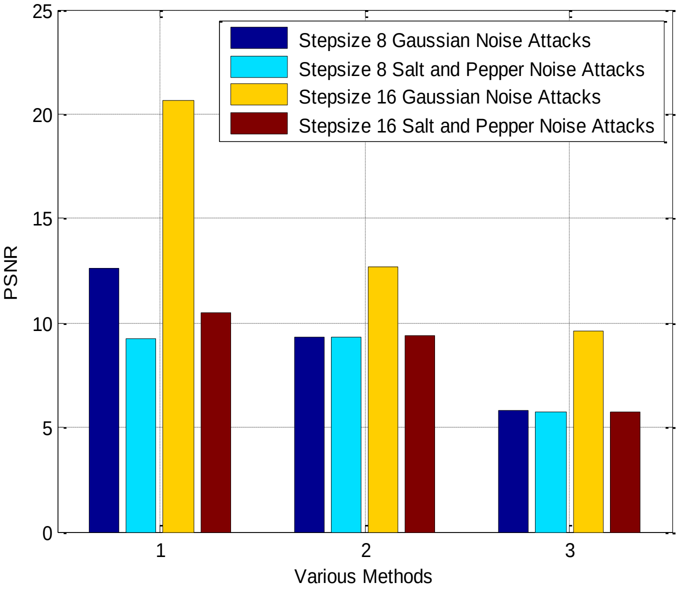


Fig. 9 PSNR performance of Noise Attacks

6.3 Resize Attacks

Most of the time when posting a picture online or sending it via email, resize the picture may be necessary. It is a non-trivial process that involves a trade-off between efficiency, smoothness and sharpness. In the case of resize attacks, we are basically changing the size of the original image. That means either increasing or decreasing the total number of pixels in the image, and then trying to recover the hidden information from the resized image.

Table 4: PSNR between retrieved and original Logos (Resize Attack)

Sat1	Resize Attack (Δ = 8)			Resize Attack (Δ = 16)		
Resize (%)	PSNR (Method 1A)	PSNR (Method 1B)	PSNR (Method 1C)	PSNR (Method 1A)	PSNR (Method 1B)	PSNR (Method 1C)
40	07.18	10.47	06.98	07.80	10.79	07.71
50	09.09	12.41	09.02	11.75	14.83	11.90
60	09.37	12.80	09.58	12.52	15.59	12.84
70	10.69	14.02	10.94	14.98	17.85	15.55
80	12.29	15.56	12.64	17.41	19.86	17.90
100	38.12	26.40	23.92	27.01	24.47	22.04
120	18.15	20.84	18.69	23.15	23.40	21.15
140	18.20	20.82	18.71	23.20	23.23	21.09
160	18.62	21.06	18.95	23.62	23.39	21.20
180	18.53	21.02	18.95	23.68	23.27	21.22
200	17.74	20.66	18.66	21.74	22.97	21.03

The PSNR analysis of various recovered logo information at various resize value are given in table 4 above. From table 4 it can be noticed that the best value of PSNR is at 100% resize. On the other hand, the PSNR value starts 40decreasing as the resize value goes above or below 100%.

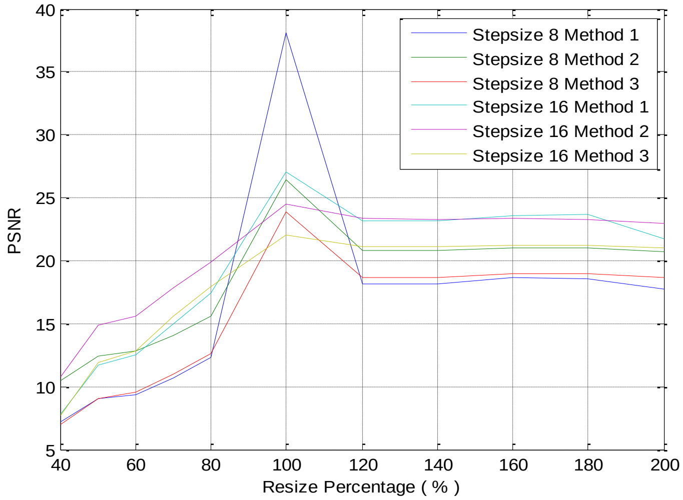


Fig. 10 PSNR performance of Resize Attacks

6.4 Rotation Attacks

Rotation attack is one of the most common geometrical attacks on digital multimedia images. First the original watermarked image is rotated by various degrees in the clock- wise direction. Then the recovered information from the attacked watermarked image performance is analyzed. The results of the rotation attack have is in Table 5 for all the three watermarking schemes.

Table 5: PSNR between retrieved and original Logos (Rotation Attack)

Logo Image	Rotation Attack (Δ = 8)			Rotation Attack (Δ = 16)		
Degree	PSNR (Method 1A)	PSNR (Method 1B)	PSNR (Method 1C)	PSNR (Method 1A)	PSNR (Method 1B)	PSNR (Method 1C)
1	18.90	19.35	17.88	19.47	19.47	17.87
2	15.54	16.44	14.98	16.34	16.79	15.62
3	13.47	14.49	13.22	14.58	15.20	14.12
5	11.06	12.20	10.91	12.47	13.06	12.18
10	08.66	09.94	08.69	09.89	10.61	09.83
45	05.67	06.75	05.81	06.46	07.14	06.54

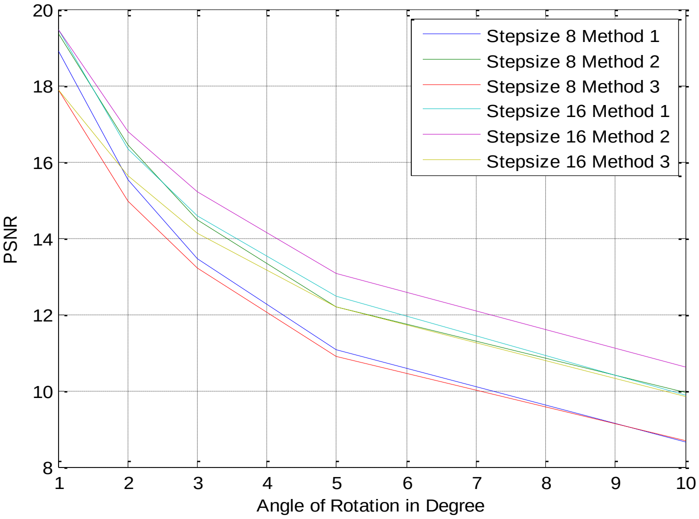


Fig 11 PSNR performance of Rotation Attacks

Table 5 shows that as the angle of rotation increase, the PSNR value start decreasing. Moreover, better PSNR values were noticed at higher values of step size for a particular rotation angle.

7. Conclusion

This paper presented three robust watermarking algorithms for embedding EIAST logo information inside DubaiSat-1 satellite images. All three watermarking algorithms were totally blind and the logo information was embedded in the best locations of the low frequency (8×8) DCT blocks.

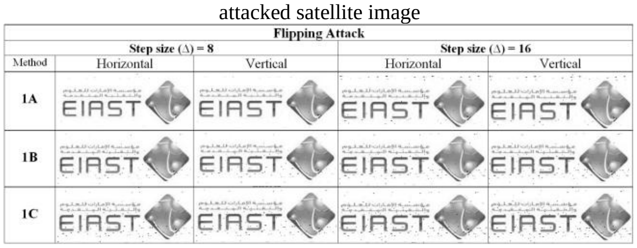
This was a tradeoff between visual degradation and robustness based on highest magnitude of first 16 lower frequency coefficients. The performance of all three watermarking algorithms have been analyzed under various attacks, such as flipping attacks, noise attacks, resize attacks and rotations attacks for scaling factors 8 and 16. The results show that all three watermarking algorithms endured powerful attacks, while maintaining excellent invisibility and qualities. In this paper we achieved the acceptable range of PSNR for watermarked images. No huge difference was noticed, which was the main goal of this study.

Moreover, different schemes provide to have different robustness against different attacks. Method (1A) was robust against flipping and noise attacks, whereas method (1B) against resize and rotation attacks. Method (1C) gave less PSNR performance compared to other proposed schemes.

Appendix

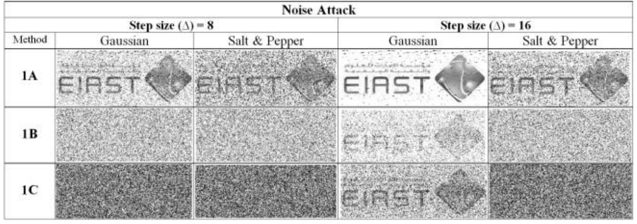
In this Appendix, we show the retrieved logo after applying different attacks using three proposed algorithms.

Table 6: Watermarked EIAST logos retrieved from various flipping attacked satellite image



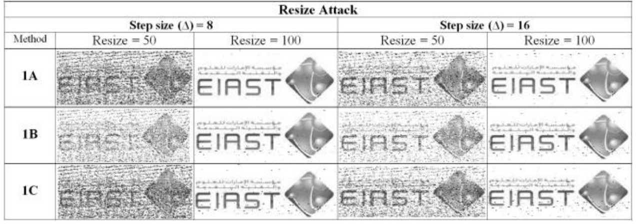
Flipping Attack				
	Step size (∆) = 8		Step size (∆) = 16	
Method	Horizontal	Vertical	Horizontal	Vertical
1A				
1B				
1C				

Table 7: Watermarked EIAST logos retrieved from various noise attacked satellite image



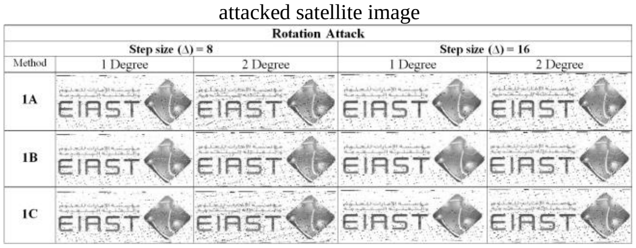
Noise Attack				
	Step size (∆) = 8		Step size (∆) = 16	
Method	Gaussian	Salt & Pepper	Gaussian	Salt & Pepper
1A				
1B				
1C				

Table 8: Watermarked EIAST logos retrieved from various resize attacked satellite image



Resize Attack				
	Step size (∆) = 8		Step size (∆) = 16	
Method	Resize = 50	Resize = 100	Resize = 50	Resize = 100
1A				
1B				
1C				

Table 9: Watermarked EIAST logos retrieved from various rotation attacked satellite image



Rotation Attack				
	Step size (∆) = 8		Step size (∆) = 16	
Method	1 Degree	2 Degree	1 Degree	2 Degree
1A				
1B				
1C				

References

[1] Keshav S Rawa, Dheerendra S Tomar, “Digital Watermarking Scheme for Authorization Against Copying or Piracy of Color Images”, IJCSE, Vol.1 No. 4 295-300.

[2] Tribhuwan Kumar Tewari,Vikas Saxena, “An Improved and Robust DCT based Digital Image Watermarking Scheme”, IJCA, Vol.3-No.1, June2010.

[3] Satyanarayana Murty.P, Dr.P.Rajesh Kumar, “A Robust Digital Image Watermarking Scheme Using Hybrid DWT-DCT- SVD Technique”, IJCSNS, Vol.10, No.10, October 2010.

[4] Vikas Saxena, J.P Gupta, “Towards increasing the Robustness of Image Watermarking Scheme Against JPEG Compression”, IMECS, VolII ,pp 1903-1906,March 2007.

[5] A.Al-Gindy, H.Al-Ahmad, R.Qahwaji and A.Tawfik, “A New Watermarking Scheme For Colour Images Captured By Mobile Phone Cameras”, IJCSNS International Journal of Computer Science and Network Security, VOL.9No.7, July 2009.

[6] A.Al-Gindy, H.Al-Ahmad, R.Qahwaji and A.Tawfik, “A novel blind Image watermarking technique for colour RGB images in the DCT domain using green channel”, in Mosharaka International Conference on Communications, Computers and Applications (MIC-CCA 2008), Amman,Jordan,2008.

[7] M.Naor, and A.Shamir, “Visual Cryptography”, Advances in Cryptology – Eurocrypt’94 Proceeding, LNCS Vol.950, Springer-Verlag, 1995, PP.1-12.

[8] R. Anderson. “Information Hiding”. Proceedings of the First Workshop on Information Hiding, LNCS-1174, Springer Verlag, New York, 1996.

[9] S.Katzenbesser and F.A.P Petitcolas. “Information Hiding Techniques for Steganography and Digital Watermarking”. Artech House, Boston, MA, 2000.

[10] Chiou-Ting Hsu and Ja-Ling Wu. “Hidden Digital Watermarks in Images”. IEEE Transaction on Image Processing, 8,pp. 58-68, 1999 .

[11] I.J. Cox, J. Kilian, T. Leighton and T. Shammon. “Secure Spread Spectrum Watermarking for Multimedia”. IEEE Transaction on Image Processing, 6, pp. 1673-1687, 1997.

[12] S.Pereira, S.Voloshynoskiy and T.Pun. “Optimal Transform Domain Watermark Embedding via Linear Programming”. Signal processing, 81,pp. 1251-1260, 2001.

[13] Jean-Paul M. G. Linnartz and van Dijk, Marten. “Analysis of the sensitivity attack against electronic watermarks in images”. In David Aucsmith, editor, second workshop on information hiding, in vol. 1525 of Lecture notes in computer science Portland, Ore-gon, U.S.A., 258–272 April, 1998, pp. 218–238. ISBN 3-540-65386-4.

[14] S. H. Low, N.F. Maxemchuk, A.M. Lapone, “Document Identification for Copyright Protection Using Centroid Detection”, IEEE Transactions on Communications, vol. 46, no. 3, pp. 372-383, March 1998.

Saeed AL-Mansoori is an assistant researcher in the Space Image department at Emirates Institution for Advanced Science and Technology (EIAST). He has received B.Sc. degree in Communication Engineering from Khalifa University of Science, Technology and Research (KUSTAR), Sharjah, UAE in 2010 and currently pursuing the M.Sc. degree in Electrical Engineering from American University of Sharjah (AUS). Saeed's research interests are in the area of image processing (super-resolution, watermarking, object detection and image classification). He is one of the program committee in High-Performance Computing in Remote Sensing which is a part of SPIE Remote Sensing Europe Symposium.

Alavi Kunhu Panthakkan a postgraduate in Digital Electronics Engineering (M.Tech). He started his career as Electronics Engineer in British company based on Abu Dhabi. Alavi joined in Khalifa University on 17th March 2008 and he work in the Electronics Engineering Department as Lab Instructor. He has 4 years Academic and over 4 years Industrial experience in the various projects in the field of Networking and Electronics Engineering.