A Novel Technique for Ownership Protection and Authentication of Satellite Imagery

Alavi Kunhu[1], Saeed Al Mansoori[2] and Hussain Al-Ahmad[1]

College of Engineering and IT, University of Dubai, UAE
[2]Applications Development and Analysis Section, Mohammed Bin Rashid Space Centre (MBRSC), UAE

Abstract *— Satellite imagery is a pivotal source of valuable information for monitoring our planet along with natural resources. This proposed research paper deals with the design and development and performance evaluation of a novel algorithm for protection and authentication of DubaiSat satellite images. In the proposed research work, the ownership protection algorithm implemented in wavelet domain by embedding ownership information using discrete wavelet transform and authentication algorithm implemented in spatial domain by embedding hash function generated SHA3 key using bit insertion technique. In the proposed algorithm, by changing the scaling factor of watermarking, the robustness can be controlled and the proposed ownership protection algorithm can be implemented either in the RGB layer or Y layer of the DubaiSat satellite images. In the proposed paper, we will used various metrics such as structure similarity index measurement and peak signal to noise ratio to evaluate quality degradation of satellite images due to ownership information and authentication SHA3 key embedding process and normalized correlation metric is used to evaluate the quality of the extracted ownership information from watermarked satellite images. Our proposed ownership protection algorithm can survive various attacks such as lossy compression JPEG, cropping, median filter, average filter, noise addition and scaling attacks. The proposed authentication algorithm is sensitive to even small modification on the watermarked DubaiSat image and can accurately detection modified region on the various layers of watermarked satellite images. Our proposed ownership and authentication algorithm gives better performance compare to state-of-art algorithms mentioned in the literature review.*

Keywords — *Satellite Image, Peak Signal to Noise Ratio, Ownership Protection, Authentication, Normalized Correlation, SHA3 hash key, Structural Similarity Index Measurement.*

I. INTRODUCTION

A. Importance of Watermarking

Nowadays we are living in the era of information technology and there is a widespread use of digital photos, multimedia documents, photos and video. But still technology lacks the ownership protection of intellectual property rights. One of the best technique to protect your digital documents from illegal usage is called digital watermarking, where some ownership information will embedded within the cover image in a way that ownership information cannot be removed [1,2,3,4]. In general any digital watermarking algorithm consists of an encoding process and decoding process and It can be implemented either in spatial domain or frequency domain. The watermark information embedded into the digital cover image using encoding process, while the embedded watermark information can be later extracted from the cover image using decoding process. The watermarking technique can be used to protect the copyright ownership of any type of digital data and to control illegal usage of it. In general for copyright ownership protection of digital data can be implemented using frequency domain watermarking techniques called robust watermarking, while fragile watermarking techniques cab be used for the content authentication of the multimedia products [5,6,7]. In general when developing or using a watermarking algorithm for copyright protection make sure that your algorithm can survive various type international and non-intentional attacks such an scaling attacks and lossy compression[8]. To make sure that your watermarking algorithm is effective, need to consider certain features such as undeletable and imperceptible[9,10]. Additionally need to check whether the watermarked data is edited or not and to protect the authenticity of the watermarked images, normally we are using fragile watermarking techniques. The fragile watermarking can accurately detection the modified region on the watermarked images using hash key generating function.

B. Evaluation of Watermarking Algorithm

While designing an ownership protection and authentication algorithm, the selection of various types metrics for the quality assessment of algorithm is very important. These quality measures play important roles in a broad range of applications such as image compression, communication, image enhancement and watermarking. Watermarked image quality can be assessed using two methods: subjective and objective. Objective methods are based on computational models that can predict perceptual image quality, while subjective methods are based on the perceptual assessment of a human viewer about the attributes of an image. Here we

will be discussing about various types of metrics to measure quality degradation cover image due to different type of watermarking methods and the quality of the extracted ownership information [11, 12, 13, 14, 15, 16]. The mean square error (MSE) represents the cumulative squared error between the two image. MSE is defined as the square of differences in the pixel values between the corresponding pixels of the two images. The MES value indicate the level of the quality degradation of image by watermarking process at a pixel level. In our proposal, the MSE compares pixel by pixel quality between original and watermarked DubaiSat images. Mathematically, MSE is expressed as [12]:

$$MSE = \frac{1}{3xy}\sum_{m,n}\left((Or_{m,n} - Wr_{m,n})^2 + (Og_{m,n} - Wg_{m,n})^2 + (Ob_{m,n} - Wb_{m,n})^2\right) \dots (1)$$

where Ob , Og and Or are the original satellite image blue layer, green layer and red layer components, while Wb, Wg and Wr are watermarked satellite image the blue layer, green layer and red layer components. The MSE value is inversely proportional to image quality degradation of watermarked satellite images.

The peak signal-to-noise ratio (PSNR) is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise. Here PSNR is used to measure the quality degration due to the watermark encoding process under various scaling factors. The PSNR is an approximation to human perception of reconstruction quality and it is most easily defined via the MSE. In our proposal, the PSNR compares pixel by pixel quality between original and watermarked DubaiSat images. The higher the PSNR, the better the quality of the degraded image. Mathematically, PSNR is expressed as [14, 16].

$$PSNR = 10.log_{10}\left(\frac{{MAX_1}^2}{MSE}\right) \dots\dots\dots (2)$$

where, MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 8 bits, then MAX_I is 255 and in general, when pixels are represented using linear PCM with B bits per pixel, MAX_I is 2^B-1.

The structural similarity image quality paradigm is based on the assumption that the human visual system is highly adapted for extracting structural information from the scene. The structural similarity index measure (SSIM) is proposed, by hypothesis that human nature is that it will extract structural information from a scene and the SSIM is used for measuring the similarity between two images and it is based on visible structures in the image. In our proposal the SSIM compares local pattern of normalized pixel intensities for luminance and contrast between original and watermarked DubaiSat images. Mathematically, SSIM is expressed [16].

$$SSIM(O,W) = \left(L(O,W)\right)^{\alpha}.\left(C(O,W)\right)^{\beta}.\left(S(O,W)\right)^{\gamma} \dots\dots (3)$$

$$L(o,w) = \frac{2\mu_X\mu_Y + A}{\mu_X^2 + \mu_Y^2 + A}, \quad C(o,w) = \frac{2\sigma_X\sigma_Y + B}{\sigma_X^2 + \sigma_Y^2 + B}, \quad S(o,w) = \frac{\sigma_{XY} + C}{\sigma_X\sigma_Y + C}$$

where L indiacte the luminance, C indicate the contrast and S indicate the structure components respectively. Similary parameter α is sued to adjust relative importance of the luminance component, while β is used to adjust the relative importance of the contrast and γ is used to adjust the relative importance of the structure components. Finally O and W indicate the original and watermarked DubaiSat images. The higher value of SSIM mean larger similarity between watermarked and original DubaiSat images.

The quality of the ownership information extracted from watermarked Dubaisat image is measured uisng the Normalized Correlation (NC). If the extracted ownership watermark exactlty same as the original ownership information, then the NC will be 1. Mathematically NC is expressed as [11].

$$NC = \sum_{m,n}\frac{\left(Lo_{m,n}Lr_{x,y}\right)}{Lo_{m,n}^2} \dots\dots (4)$$

where Lo indicate the original ownership, while the Le indicate the extracted ownership information.

1.3 Image Discrete Wavelet Transform

The wavelet analysis is based on the concept of details and approximations, where the high frequency details components gives flavor and low frequency approximations components gives the identity. The discrete wavelet transform technique divide an image into four components known as LL, LH, HL and HH compenents, where horizontal (HL), vertical (LH) and diagonal (HH) are the three detail components, while LL is the lower resolution approximation image [20, 21, 22]. In the case of multi level wavelet transform, the decomposition process can be repeated a number of items. The advantages of the wavelet transform technique is the accurate aspects of the HVS and normally watermark information is embeded in to the high resolution less sensitive detail bands such as LH, HL and HH H.

II. Proposed Ownership Protection and Authentication Embedding Algorithm

The block diagram of the proposed ownership protection and authentication embedding algorithm is shown in Figure 1. Here initialy the ownership information is embeded into satellitae image by using the discrete wavelet transform in the wavelet

domain. Then hash function generated SHA3 512bit authentication key is embedded into the ownership information embeded satelliate image using the Odd/Even bit insertion method in the spatial domain [23, 24]. Our proposed ownership protection and authentication technique is blind and later to extract ownership information,no need the original satellite image.

Figure 1. A block diagram of the proposed technique

A. Ownership Embedding Algorithm

Using discrete wavelet transform, the ownership embedding technique embeds ownership information into a selected RGB or Y layer of the satellite images in wavelet domain. This process will be done by using 2D-DWT 'db1' wavelet and by apply multi-level decomposition on selected RGB or Y layer of image as shown in Figure 2. Firstly, need to convert the ownership information into index mapped bits using the index mapping table shown in Table 1. Secondly the indexed ownership information embedded into the into selected multi-level decomposed block of the selected RGB or Y layer using Odd/Even hiding method which was explained using equation 5 [6, 18]. The block diagram of the ownership embedding algorithm is shown in Figure 3.

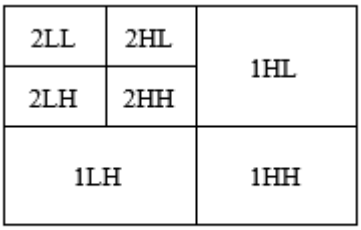

Figure 2. DWT multi-level decomposition

The ownership information embedding is done using the below given equation:

$$[2LL,2LH,2HL,2HH] = 2DDWT\{B_k\}, \quad .....(5)$$

$$if \;\; Lo(m,n) = 0 \;\; then$$

$$2LL(m,n) = \begin{cases} \Delta Q_{\square}\left(\dfrac{2LL\;(m,n)}{\Delta}\right) \\ 2LL\,(m,n) \end{cases}$$

$$if \;\; Lo(m,n) = 1 \;\; then$$

$$2LL(m,n) = \begin{cases} \Delta Q_e\left(\dfrac{2LL(m,n)}{\Delta}\right) \\ 2LL\,(m,n) \end{cases}$$

where B_k represent the k[th] block of selected RGB or Y layer of the DubaiSat image and 2LL represent the low freuqency approximation of the two level descrete cosine transform decomposed satellite image. The L*o(m,n)* indicate the the index mapped ownership information and Δ represent the scaling factor.The Q_e represent the even quantization and the Q_o represent odd quantization to an integer number.

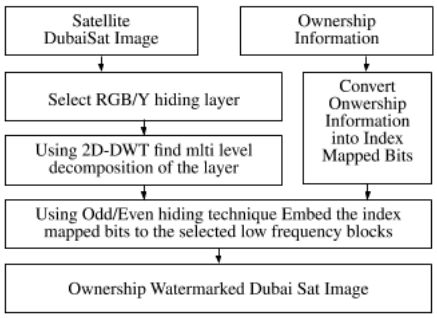

Figure 3. Ownership embedding algorithm

Table 1. Ownership information Index mapping table

Ownership Colours	Index Key	Binary Value
Colour1	0	00
Colour2	1	01
Colour3	2	10
Colour4	3	11

B. Authentication Embedding Algorithm

The authentication embedding algorithm embeds unique SHA3 512bits key generated into 64x64 authentication blocks of the ownership watermarked DubaiSat image using the insertion technique called LSB in spatial domain [21, 22]. The block diagram of the proposed authentication embedding algorithm is shown in Figure 4. To increase the security of authentication technique, we have used four 64 x 64 size random patterns keys as sown in Figure 5.

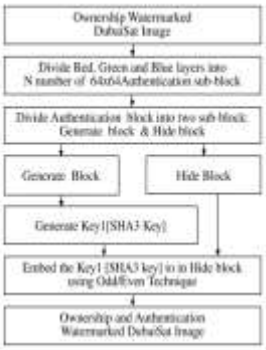

Figure 4. Authentication embedding algorithm

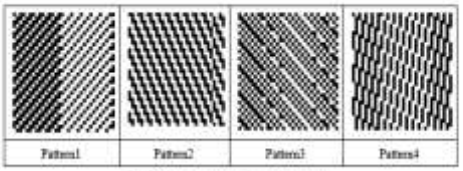

Figure 5. Random pattern selection keys

III. Proposed Ownership Protection and Authentication Extraction Algorithm

A. Authentication Extraction Algorithm

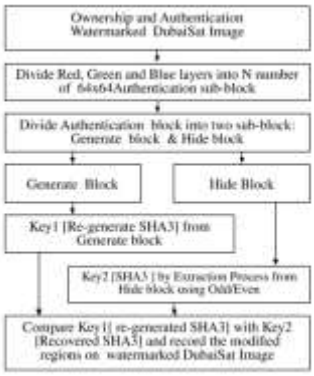

Figure 6. Authention extraction algorithm

The block diagram of the authentication extraction algorithm is as shown in Figure 6. Here first need to run the proposed authentication extraction algorithm to check the level of authenticity of the DubaiSat image in block by block. Here firstly divide red, green and blue layers of the ownership and authentication watermarked DubaiSat image into 64x64 authentication block and divide authentication block into hide block and generate block using 4 different patterns. As next step, extracts the authentication SHA3 key from the hide sub-blocks using the Odd/Even method and re-generate SHA3 key from generate sub-block. Now need to compare both SHA3 keys [re-generated and extracted] and If the extracted and re-generated SHA3 keys match, then the selected authentication block is authentic, else indicates that some modification has been done in the selected authentication sub-block.

B. Ownership Extraction Algorithm

The proposed ownership extraction algorithm is used for the ownership copyright protection of the DubaiSat images by extracting the ownership information from the ownership and authentication watermarked DubaiSat image. Initiallay need to extract the ownership index mapped bits from selected selected RGB or Y layer, lower frequency block of the multi level discrete cosine transform decomposed watermarked image using Odd/Even decoding method mentioned in equation 6, Once extract the ownership index mapped bit, next step is convert it into ownership information using the same index mapping table used for ownership embedding process. The Figure 7, show the block diagram of the propossed ownership extraction process.

$$\text{if } Q\left(\frac{F_k(u,v)}{\Delta}\right) \Rightarrow \text{Odd Number} \Rightarrow Lr(m,n) = 0$$
$$\Downarrow$$
$$\text{Even Number} \qquad \ldots\ldots\ldots (6)$$
$$\Downarrow$$
$$Lr(m,n) = 1$$

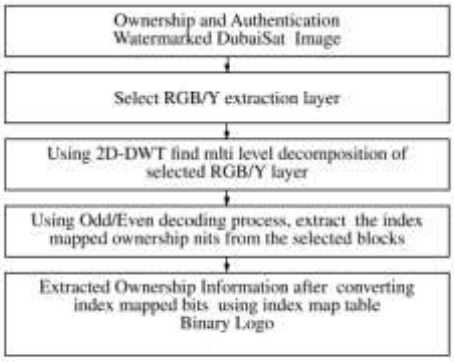

Figure 7. Ownership extraction algorithm

IV. Result and Analysis

Figure 8 shows the various satellite images [1024 x 1024 pixels] captured by DubaiSat used to test the performance of the developed ownership protection and authentication algorithm and Figure 9 shows University of Dubai logo [128x128] used as ownership information. Hash function is used to generate a unique SHA3 512bit length hash-key for authentication key and various scaling factors such as 12, 16 , 20 and 20 are used to control the watermark strength of the developed algorithm. Various metrics such as the peak singal to noise ration and structural similarity index measure are used to asses the quality degradation of DubaiSat image due to different type of watermarking and normalized correlation value is used to compare the quality of the extracted ownership information with original ownership information. The robustness performance of the developed ownership protection and authentication algorithm is evaluated under different types of attacks such as scaling, filtering, cropping and lossy compression JPEG attacks.

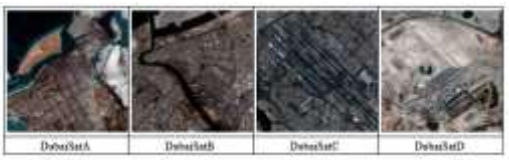

Figure 8. DubaiSat images

Figure 9. Ownership information

The peak signal to noise ration performance of the RGB and Y layer ownership watermarked images under various watermark strength scaling factor are

shown is Table 2, 3 and 4. Similarly the Tables 5, 6 and 7 shows it's structure similarity index measurement performance. Figure 10, shows a compariosn of the peak signal to noise ration under different scaling factor for RGB and Y layer ownership and authentication watermarked satellite images. Similary Figure 11, shows structure similarity index measurement performance comparison for different layer ownership and authentication watermarked images for various scaling factors. By comparison the PSNR performance of watermarked satellite images in Table 2 and 3, we have noticed that RGB green layer embedded ownership and authentication watermarked images gives better performance compare to the Y layer embedded ownership and authentication watermarked images.

Table 2. PSNR analysis of green layer ownership and authentication watermarked images

Images	Ownership Watermarked Image				Ownership and Authentication Watermarked Image			
	Δ = 12	Δ = 16	Δ = 20	Δ = 24	Δ = 12	Δ = 16	Δ = 20	Δ = 24
DubaiSatA	47.80	45.32	43.43	41.51	46.50	44.31	42.80	41.04
DubaiSatB	47.82	45.34	43.25	41.56	46.48	44.32	42.64	41.09
DubaiSatC	47.78	45.29	43.30	41.74	46.42	44.38	42.68	41.25
DubaiSatD	47.83	45.39	43.34	41.69	46.47	44.36	42.72	41.21
DubaiSatE	47.85	45.18	43.20	41.63	46.40	44.28	42.59	41.16
DubaiSatF	47.87	45.33	43.32	41.72	46.44	44.31	42.70	41.23
DubaiSatG	47.69	45.33	43.31	41.72	46.46	44.32	42.69	41.24
DubaiSatH	47.68	45.27	43.33	41.85	46.46	44.26	42.71	41.36

Table 3. PSNR analysis of Y layer ownership and authentication watermarked images

Images	Ownership Watermarked Image				Ownership and Authentication Watermarked Image			
	Δ = 12	Δ = 16	Δ = 20	Δ = 24	Δ = 12	Δ = 16	Δ = 20	Δ = 24
DubaiSatA	41.39	39.01	37.13	35.68	40.75	38.54	36.77	34.57
DubaiSatB	41.26	39.00	37.25	35.68	40.62	38.43	36.88	34.57
DubaiSatC	41.39	39.04	37.07	35.52	40.75	38.48	36.71	34.42
DubaiSatD	41.36	39.01	37.13	35.53	40.72	38.45	36.76	34.43
DubaiSatE	41.38	38.70	37.38	35.48	40.75	38.25	37.01	34.38
DubaiSatF	41.34	38.89	37.16	35.56	40.70	38.43	36.79	34.46
DubaiSatG	41.31	38.89	37.09	35.52	40.67	38.43	36.72	34.42
DubaiSatH	41.32	39.02	37.28	35.46	40.69	38.46	37.02	34.36

Table 4. PSNR analysis of RGB and Y layers ownership and authentication watermarked images

Images (Δ = 20)	Ownership Watermarked Image				Ownership and Authentication Watermarked Image			
	Red	Green	Blue	Y	Red	Green	Blue	Y
DubaiSatA	43.44	43.43	43.42	37.13	42.82	42.80	42.81	36.77
DubaiSatB	43.55	43.25	43.30	37.25	42.90	42.64	42.79	36.88
DubaiSatC	43.51	43.30	43.45	37.07	42.89	42.68	42.85	36.71
DubaiSatD	43.47	43.34	43.41	37.13	42.87	42.72	42.78	36.76
DubaiSatE	43.15	43.20	43.30	37.38	42.55	42.59	42.67	37.01
DubaiSatF	43.45	43.32	43.42	37.16	42.83	42.70	42.78	36.79
DubaiSatG	43.51	43.31	43.45	37.09	42.86	42.69	42.81	36.72
DubaiSatH	43.23	43.33	43.43	37.28	42.66	42.71	42.83	37.02

Table 5. SSIM analysis of green layer ownership and authentication watermarked images

Images	Ownership Watermarked Image				Ownership and Authentication Watermarked Image			
	Δ = 12	Δ = 16	Δ = 20	Δ = 24	Δ = 12	Δ = 16	Δ = 20	Δ = 24
DubaiSatA	0.9993	0.9983	0.9963	0.9945	0.9982	0.9974	0.9960	0.9941
DubaiSatB	0.9994	0.9972	0.9965	0.9954	0.9983	0.9968	0.9961	0.9959
DubaiSatC	0.9993	0.9993	0.9986	0.9985	0.9990	0.9990	0.9982	0.9978
DubaiSatD	0.9995	0.9994	0.9987	0.9983	0.9991	0.9991	0.9980	0.9980
DubaiSatE	0.9968	0.9959	0.9947	0.9937	0.9957	0.9948	0.9932	0.9925
DubaiSatF	0.9991	0.9992	0.9991	0.9988	0.9988	0.9989	0.9983	0.9982
DubaiSatG	0.9989	0.9987	0.9959	0.9935	0.9980	0.9978	0.9954	0.9930
DubaiSatH	0.9978	0.9967	0.9927	0.9909	0.9972	0.9958	0.9921	0.9909

Table 6. SSIM analysis of Y layer ownership and authentication watermarked images

Images	Ownership Watermarked Image				Ownership and Authentication Watermarked Image			
	Δ = 12	Δ = 16	Δ = 20	Δ = 24	Δ = 12	Δ = 16	Δ = 20	Δ = 24
DubaiSatA	0.9937	0.9895	0.9826	0.9805	0.9926	0.9883	0.9821	0.9792
DubaiSatB	0.9956	0.9917	0.9937	0.9856	0.9947	0.9904	0.9926	0.9843
DubaiSatC	0.9988	0.9968	0.9935	0.9887	0.9977	0.9961	0.9926	0.9874
DubaiSatD	0.9985	0.9965	0.9948	0.9914	0.9980	0.9963	0.9936	0.9905
DubaiSatE	0.9957	0.9797	0.9827	0.9657	0.9928	0.9783	0.9813	0.9642
DubaiSatF	0.9985	0.9969	0.9949	0.9918	0.9981	0.9962	0.9945	0.9914
DubaiSatG	0.9929	0.9856	0.9796	0.9709	0.9912	0.9854	0.9783	0.9706
DubaiSatH	0.9886	0.9798	0.9714	0.9595	0.9877	0.9786	0.9706	0.9588

Table 7. SSIM analysis of RGB and Y layers ownership and authentication watermarked images

Images (Δ = 20)	Ownership Watermarked Image				Ownership and Authentication Watermarked Image			
	Red	Green	Blue	Y	Red	Green	Blue	Y
DubaiSatA	0.9945	0.9963	0.9977	0.9826	0.9940	0.9960	0.9968	0.982
DubaiSatB	0.9986	0.9965	0.9967	0.9937	0.9982	0.9961	0.9957	0.992
DubaiSatC	0.9995	0.9986	0.9965	0.9935	0.9988	0.9982	0.9981	0.992
DubaiSatD	0.9998	0.9987	0.9987	0.9948	0.9992	0.9980	0.9982	0.993
DubaiSatE	0.9937	0.9947	0.9948	0.9827	0.9927	0.9932	0.9937	0.981
DubaiSatF	0.9995	0.9991	0.9984	0.9949	0.9991	0.9983	0.9980	0.994
DubaiSatG	0.9948	0.9959	0.9968	0.9796	0.9943	0.9954	0.9962	0.978
DubaiSatH	0.9927	0.9927	0.9926	0.9714	0.9917	0.9921	0.9923	0.970

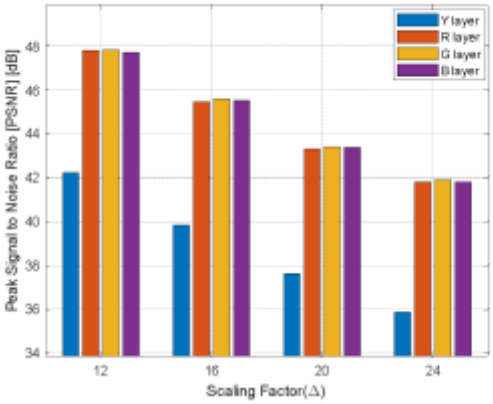

Figure 10. PSNR analysis of Y and RGB layers ownership and authentication watermarked DubaiSatA

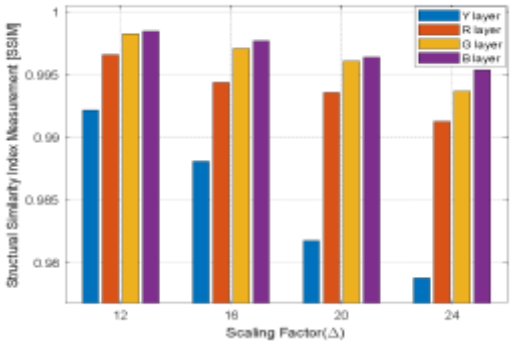

Figure 11. SSIM analysis of RGB and Y layers ownership and authentication watermarked DubaiSatA

Table 8. Extracted Ownership information NC analysis under JPEG compression attack for DubaiSat Images

JPEG(Δ=20)	Layer	95%	85%	75%	65%	55%	45%	35%	25%
DubaiSatA	Red	0.9908	0.8643	0.8141	0.8013	0.7988	0.8063	0.8114	0.80243
	Green	0.9998	0.9758	0.9244	0.8765	0.8306	0.8045	0.7993	0.8066
	Blue	0.9889	0.8157	0.8083	0.8087	0.8095	0.8084	0.8082	0.8069
	Y	0.9999	0.9995	0.9994	0.9965	0.9707	0.9167	0.8416	0.8022
DubaiSatB	Red	0.9948	0.8456	0.8012	0.78945	0.7958	0.7984	0.8022	0.8034
	Green	0.9997	0.9665	0.9034	0.8495	0.8074	0.7935	0.7953	0.7976
	Blue	0.9738	0.8028	0.8025	0.7968	0.8015	0.8022	0.8024	0.8018
	Y	0.9997	0.9995	0.9994	0.9918	0.9424	0.8696	0.8038	0.7871
DubaiSatC	Red	0.9978	0.8478	0.7913	0.7788	0.7897	0.7946	0.8001	0.8013
	Green	0.9999	0.9734	0.8985	0.8378	0.7913	0.7812	0.7892	0.7945
	Blue	0.9878	0.8078	0.7825	0.7835	0.7916	0.7975	0.8002	0.8007
	Y	0.9999	0.9998	0.9996	0.9778	0.9017	0.8228	0.7908	0.7919

Tables 8 show the extracted ownership information quality comparison under different lossy compression [JPEG] attacks from the all the RGB layers and Y layer of ownership and authentication watermarked satellite images [DubaiSatA, DubaiSatB and DubaiSatc] and Figure 12 shows the extracted ownership information quality comparison using the metric NC. Similarly Tables 9 show the extracted ownership information quality comparison under scaling attacks from the all the RGB layers and Y layer ownership and authentication watermarked satellite images and Figure 13 shows the extracted ownership information quality comparison using the metric NC. Table 10 show extracted ownership information quality comparison using normalized correlation under different type of attacks such as filter attack , noise attack and image cropping attack.

Table 9. Extracted ownership information NC analysis under scaling attack for DubaiSat Images

Images (Δ=20)	layer	Scaling 120%	Scaling 110%	Scaling 90%	Scaling 80%	Scaling 70%	Scaling 60%	Scaling 50%	Scaling 40%
DubaiSatA	Red	0.9992	0.9982	0.9902	0.9774	0.9515	0.9205	0.9131	0.8523
	Green	0.9994	0.9981	0.9884	0.9722	0.9466	0.9126	0.9053	0.8525
	Blue	0.9966	0.9963	0.9836	0.9636	0.9334	0.9007	0.8937	0.8467
	Y	0.9998	0.9995	0.9948	0.9838	0.9633	0.9348	0.9278	0.8599
DubaiSatB	Red	0.9993	0.9993	0.9981	0.9981	0.9822	0.9351	0.9032	0.8282
	Green	0.9995	0.9995	0.9983	0.9963	0.9823	0.9372	0.9004	0.8324
	Blue	0.9987	0.9987	0.9963	0.9962	0.9854	0.9444	0.9176	0.8326
	Y	0.9999	0.9998	0.9987	0.9975	0.9896	0.9556	0.9268	0.8388
DubaiSatC	Red	0.9971	0.9971	0.9881	0.9745	0.9521	0.9228	0.9101	0.8342
	Green	0.9963	0.9962	0.9872	0.9724	0.9502	0.9192	0.9095	0.8363
	Blue	0.9932	0.9933	0.9783	0.9586	0.9353	0.9054	0.8987	0.8355
	Y	0.9986	0.9984	0.9925	0.9818	0.9647	0.9368	0.9269	0.8478

Table 10. Extracted ownership information NC analysis under cropping, filter and noise attacks for watermarked DubaiSatA

Cropping Attacks		Filter Attacks		Noise Attacks	
(Δ=20)	NC	(Δ=20)	NC	(Δ=20)	NC
Vertical 50%	0.922 5	Average 3x3	0.833 1	Salt and Pepper [density=0.015]	0.908 1
Vertical 75%	0.878 7	Average 5x5	0.833 3	Salt and Pepper [density =0.025]	0.854 2
Horizontal 50%	0.915 7	Average 7x7	0.832 3	Salt and Pepper [density =0.035]	0.816 4
Horizontal 75%	0.881 4	Average 9x9	0.786 7	Salt and Pepper [density =0.045]	0.801 6
Both sides 25%	0.933 6	Median 3x3	0.867 3	Gaussian [variance=0.0015]	0.809 3
Both sides 50%	0.884 8	Median 5x5	0.842 3	Gaussian [variance=0.0025]	0.776 3
Both sides 75%	0.836 9	Median 7x7	0.839 7	Poisson	0.830 7

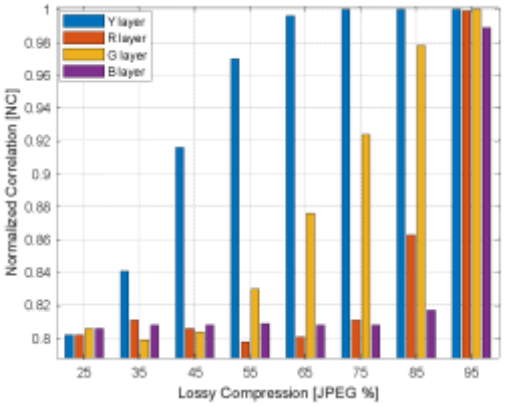

Figure 12. Extracted ownership information NC analysis under JPEG attack from DubaiSatA

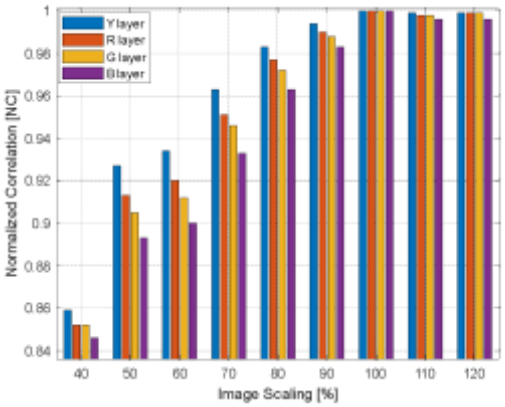

Figure 13. Extracted ownership information NC analysis under scaling attack from DubaiSatA

The developed authentication extraction algorithm compares the hash-hide sub-block, extracted 512bits SHA3 key with hash-generate sub-block, re-generated 512bits SHA3 key using hash function. If any modification has done at random pixel value in the watermarked images, as per our developed authentication extraction algorithm, there will be a difference between the SHA3 regenerated key and the extracted SHA3 key of the modified 64 x 64 authentication sub-block of the watermarked DubaiSat image. Table 11 shows a comparison between the regenerated SHA3 key and extracted SHA3 key, if any modification has done either in hide block or generate block of the selected layers of the watermarked RGB DubaiSat image or both block. Figure 14 shows modified region that are detected, when random selected pixels value minimum change by 1 in any layers of the watermarked RGB DubaiSatA image. Similarly, Figure 15 shows the modified region detected on ownership and authentication watermarked DubaiSatA image.

Table 11. SHA3 keys extracted and re-generated from Authentication sub-block when DubaiSat image modification

64x64 Authentication Block	Key1: Extracted SHA3	Key2: Re-generated SHA3
Red layer tampered/modified	c2033941311f47c97f23d02a8e8b676 a73cf24f93813c8fca10c6c6529318181 6c2033941311f47c97f23d02a8e8b67 6a73cf24f93813c8fca10c6c6529318	85348c27ac164f5373d45b72b431acb 923f19d0a6dd9d8f2f85348c27ac164f 372d45b72b431acb8f923f19d0a6dd9da 8f2fbda90560631aaa bda90560631aaa
Green layer tampered/modified	7f049518aba4eb166f865cdc503745d a4857d89b850bb6273bc38d8d7068e4 5d485db2ed52c1a2946f07ed5cfa51e0 75f7255db2727ff8c527907efaBach2fc	7dc2f839a73a843e85348c27ac164f532 d45b72b431acb8923f19d0a6dd9d8f2fb 90560631aaadc52b6623288e0fff7efabc 337e5233fb788b0c95e59474c8151213 a
Blue layer tampered/modified	485db2ed52c1a2946f07485db2ed52c 1a2946f07ed5cfa51e075f7255db2727 ff8c527907efaBach2fcbed5cfa51e075 f7255db2727ff8c527907efaBach2fcbb	3d6a3d3f891f0f8363ff85348c27ac164f5 372d45b72b431acb8923f19d0a6dd9d8f 2fbda90560631aaa3e587e0462db088c7 9a24d59cacb606abe5f831de85b48123b

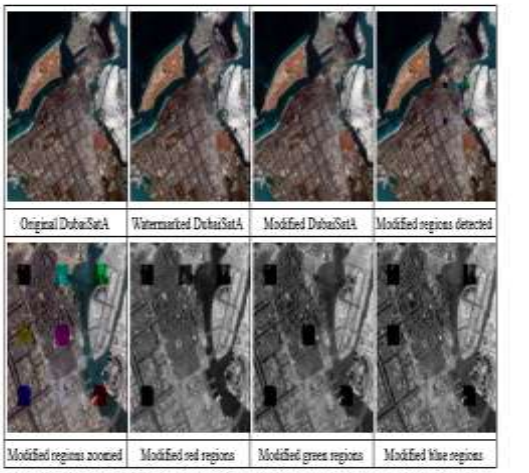

Figure 14. Localized modified regions detection from ownership and authentication watermarked DubaiSatA

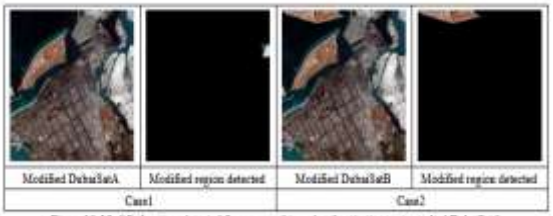

Figure 15. Modified regions detected from ownership and authentication watermarked DubaiSatA

Table 12, shows the performance comparison [PSNR] of the developed ownership protection and authentication algorithm with different state of the art algorithms discussed in the literature review. The developed ownership protection and authentication algorithm, gives better performance under many attacks such as lossy compression JPEG, image scaling, average filter, median filter and different level of cropping attacks. The developed authentication algorithm can accurately detect the modified region on tampered watermarked DubaiSat images.

Table 12. Developed algorithm comparison with other state of art techniques

Various Techniques	Implementation Domain	Cover Image	Watermark	PSNR
[8]	Discrete Cosine Transform (DCT)	512 x 512	128 x 128	31.25 dB
[10]	Discrete Cosine Transform (DCT)	512 x 512	128 x 128	42.25 dB
[21]	Slant Transform (ST)	512 x 512	64 x 64	37.44 dB
[27]	Discrete Wavelet Transform (DCT)	1024 x 1024	64 x 64	40.55 dB
Developed Algorithm	DWT & Spatial	1024 x 1024	128 x 128	41.16 dB

V. CONCLUSIONS

We have designed and implemented, a novel blind method for the ownership copyright protection and digital content authentication of satellite DubaiDsat images and tested the performance of developed algorithm using 1024 x 1024 24 bits satellite images captured by DubaiSat under many attacks such as lossy compression JPEG, scaling attack, filtering attack and cropping attack and random selected location forced pixel modifications attacks. In this research work, ownership protection algorithm implemented in wavelet domain by embedding the ownership information using discrete wavelet transform, while the authentication algorithm implemented by embedding 512 bits SHA3 genetrated hash key in spatial domain using a method called least significant bit insertion. The strength of the developed ownership protection algorithm can be controlled by adjusting the value watermark scaling factor and the developed algorithm cause little distortion to satellite DubaiSat images. We have used various metrices such as structure similarity index measurement and peak signal to noise ratio to evalaute quality of watermarked DubaiSat images and normalized correlation metric is used to evaluate the quality of the extracted ownership information from watermarked images. Developed ownership and authentication algorithm used an index mapping table to reduce the ownership payload from 24 bits /pixel to 2 bits key and to increase the security of authentication algorithm 4 different, 64 x 64 pixels pattern keys also used. In the proposed ownership protection and authentication algorithm distortion is caused mainly by the ownership protection algorithm and the distortion caused by the authentication algorithm is very small compare to ownership algorithm. The quality degradation of the

ownership information extracted is analyzed by using the normalized correlation metrics and from results analysis, it is proved that in the case of lossy JPEG compression, the embedding in Y layer is more robust as compared to the RGB layer embedding technique. By various experimental analysis, it is concluded that ownership information embedding in selected layer of RGB gives better perceptual invisility compare to embedding in Y layer of satellite DubaiSat image. Finally our developed algorithm can accurately detection modified region on all the layers of watermarked satellite image upto an accuracy of 64x64 sub-blocks.

REFERENCES

[1] Preeti Prasher and Rajeev Kumar Singh, "*A Survey: Digital Image Watermarking Techniques*" International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 7, No. 6, 2014

[2] Christine Podilchuk and Edward Delp, "*Digital watermarking: Algorithms and application*", IEEE Signal processing Magazine, 2001.

[3] Richard E Woods and Rafael C Gonzalez "*Digital Image Processing*", 3rd edition, Pearson Education, 2007.

[4] Lalit Kumar Saini and Vishal Shrivastava " A Survey of Digital Watermarking Techniques and its Applications", 2014.

[5] Baisa L. Gunjal and R.R. Manthalkar, "*An overview of transform domain robust digital image watermarking algorithms*", Journal of Emerging Trends in Computing and Information Sciences, 2010.

[6] Deepshikha Chopra, Preeti Gupta, Gaur Sanjay B.C. and Anil Gupta, "*LSB Based Digital Image Watermarking For Gray Scale Image*" Journal of Computer Engineering, 2012.

[7] Saxena and Anuj, "*Digital image watermarking using least significant bit and discrete cosine transformation*" In Intelligent Computing, Instrumentation and Control Technologies (ICICICT), IEEE International Conference on, pp. 1582-1586, 2017. ng, J. (2006) An Algorithm for Improving Watermark Robustness in DCT Domain. Journal of Computer Applications and Software, 23, 100-101. Hang, J. (2006) An Algorithm for Improving Watermark Robustness in DCT Domain. Journal of Computer Applications and Software, 23, 100-101. Zhang, J. (2006) An Algorithm for Improving Watermark Robustness in DCT Domain. Journal of Computer Applications and Software, 23, 100-101. Zhang, J. (2006) An Algorithm for Improving Watermark Robustness in DCT Domain. Journal of Computer Applications and Software, 23, 100-101.

[8] Mohamed A. Suhail and Mohammad S. Obaidat, "*Digital watermarking-based DCT and JPEG model*", IEEE Transactions on instrumentation and measurement, pp. 1640-1647, 2003.

[9] Gupta, Vinita, and Atul Barve, "*A review on image watermarking and its techniques*" International Journal of Advanced Research in Computer Science and Software Engineering 4, no. 1 (2014): 92-97.

[10] Yun-Ping ZHENG and Zi-Lun XI1, "*A Watermarking Algorithm Based on DCT and JPEG Quantization Table*", ITM Web of Conferences, 2017.

[11] O. T. P. a. S. R. L., "*Human visual system based wavelet decomposition for image compression*," Journal of Visual Communication and Image Representation, vol. 6, no. no. 2, pp. 109-121, 1995.

[12] Mahdi Khosravy, Nilesh Patel, Neeraj Gupta and Ishwar Sethi, *" Image Quality Assessment: A Review to Full Reference Indexes*", Recent Trends in Communication, Computing, and Electronics, pp.279-288, 2018

[13] Wang Kong-qiao, Shen Lan-sun and Xing Xin, "*A Quality Assessment Method of Image Based on Visual Interests*". Journal of Image and Graphics. pp.300-303, 2000.

[14] Wang, Z., Bovik, A. C., & Lu, L. (2002). "*Why is image quality assessment so difficult?"* In IEEE International Conference on Acoustics, Speech, and Signal Processing (pp. 3313–3316). Wang, Z., Bovik, A. C., & Lu, L, "Why is image quality assessment so difficult?", IEEE International Conference on Acoustics, Speech, and Signal Processing, pp. 3313–3316, 2002.

[15] Anna Geomi George and Kethsy Prabavathy, "*A Survey On Different Approaches used in Image Quality Assessment*," International Journal of Emerging Technology and Advanced Engineering Volume 3, Issue 2, 2013.

[16] Shruti P and Sankalp A, "*Performance evaluation of image enhancement techniques*", IJSIPPR, Vol 8, 2015.

[17] Mishra, Anurag, Charu Agarwal, Arpita Sharma and Punam Bedi, "*Optimized gray-scale image watermarking using DWT–SVD and Firefly Algorithm*." Expert Systems with Applications41, no. 17 (2014): 7858-7867.

[18] "A wavelet based Digital Image Watermarking scheme using LSB Technique"- Ritu Chikara, International Journal of Computer Engineering and Applications, Volume IX, 2015.

[19] Kim, Y., Kwon, O., Park, R.: "*Wavelet Based Watermarking Method for Digital Images Using the Human Visual System*". In: IEEE International Symposium on Circuits and Systems, vol. 4, pp. 80–83, 1999.

[20] Walid Alakk, Hussain Al-Ahmad and Alavi Kunhu, "*A New Watermarking Algorithm for Scanned Grey PDF Files Using DWT and Hash Function*", 9th IEEE/IET International Symposium on Communication Systems, Networks and Digital Signal Processing, CSNDSP14, Manchester, United Kingdom, 2014.

[21] Wang, Doherty J.F and Dyck, R.E.V, "*A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images*", IEEE Transactions on Image Processing 11(2), pp.77–88, 2002.

[22] Mohsen Shahrezaee and Navid Razmjooy, "*Image Watermarking Based on DWT-SVD*", Proceedings of the 2nd International Conference on Combinatorics, Cryptography and Computation, Tehran, Iran, 2017

[23] Federal Information Processing Standards Publication 180-4, Secure Hash Standard (SHS), Information Technology Laboratory, National Institute of Standards and Technology, March 2012.

[24] Al-Nayar M. M., "*A proposed Secure Protocol for E-Mail System Based on Authentication and Hash Function*", Eng. & Tech. Journal, pp.3291-3301, 2011.

[25] Rajeswari H., Yegireddi R., and RaoV. G., "*Performance Analysis of Hash Algorithms and File Integrity*", (IJCSIT) International Journal of Computer Science and Information Technologies, pp.7376-7379, 2014.

[26] Chan X. and Liu G., "*Discussion of One Improved Hash Algorithm Based on MD5 and SHA1*", Proceedings of the World Congress on Engineering and Computer Science, 2007.

[27] R. H. Laskar, Madhuchanda Choudhury, Krishna Chakraborty and Shoubhik Chakraborty, "*A Joint DWT-DCT Based Robust Digital Watermarking Algorithm for Ownership Verification of Digital Images*", International Conference on Information Processing, pp 482-491, 2011.

Dr. Alavikunhu Panthakkan is a dynamic research scientist in electronics engineering and he is working as Assistance Professor at College of Engineering and IT, University of Dubai. His research interests are in the areas of engineering education, copyright protection, authentication, medical image processing, video signal processing and artificial neural network. He received Ph.D. in electronics engineering. He has published more than 30 papers in international conferences and journals. He is a member of Institute of Electrical and Electronic Engineers (IEEE), member of Institution of Engineers (India) (MIE), member of International Association of Engineers (IAENG), member of International Association of Computer and Information Technology (IACSIT) and member of Institute of Research Engineers and Doctors (IRED).

Prof. Hussain Al-Ahmad got his Ph.D. from the University of Leeds, UK in 1984 and he is the founding Dean of Engineering and IT at the University of Dubai, UAE. He has 33 years of higher education experience working at academic institutions in different countries including University of Portsmouth, UK, Leeds Beckett University, UK, Faculty of Technological Studies, Kuwait, University of Bradford, UK, Etisalat University College, UAE and Khalifa University, UAE. He was the founder and Chair of the Electronic Engineering department at both Khalifa University and Etisalat University College. His research interests are in the areas of engineering education, signal and image processing, multimedia, remote sensing and propagation. He has supervised successfully 30 PhD and Master students in the UK and UAE. He has delivered short courses and seminars in Europe, Middle East and Korea. He has published over 120 papers in international conferences and journals and has a UK patent. He served as chairman and member of the technical program committees of many international. He is a Senior Member of the IEEE and a Fellow of the Institution of Engineering and Technology (FIET), Chartered Engineer (C.Eng), Member of BCS The Chartered Institute for IT (MBCS), Chartered IT Professional (CITP), Fellow of the British Royal Photographic Society (FRPS), Accredited Senior Imaging Scientist (ASIS). He is the Chairman of the IEEE UAE Education Chapter and Vice Chairman of the Middle East Section of BCS. He was a founder member and Ex. Chairman of the IEEE UAE Computer Chapter and Ex Vice Chairman of the IEEE UAE Signal Processing and Communication Chapter. He was a founder member and Ex Secretary of the IEEE Kuwait section.

Saeed Al-Mansoori is the head of the Applications Development and Analysis Section (ADAS) at Mohammed Bin Rashid Space Center. He has received B.Sc. degree in communication engineering from Khalifa University of Science, Technology and Research (KUSTAR), Sharjah, UAE in 2010 and the M.Sc. degree in Electrical Engineering from American University of Sharjah (AUS) in 2016. Saeed's research interests are in the area of image processing (super-resolution, watermarking, object detection and image classification). He is the member of the international society of optics and photonics and one of the program committee in High-Performance Computing in Remote Sensing since 2012.