A Novel Reversible Watermarking Scheme based on SHA3 for Copyright Protection and Integrity of Satellite Imagery

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

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

Summary
Satellite imagery is a pivotal source of valuable information for monitoring our planet along with natural resources. However, these images have an extreme acquisition cost. Nowadays, with the widespread of the advanced technology, unauthorized ordinary people can access these data, modify their content and utilize them illegally. Therefore, there is a massive demand for providing secure storage and transmission of such data. Hence, digital watermarking has been introduced for overcoming this illegitimate practice. This paper presents a novel reversible invisible watermarking scheme based on SHA3 to ensure copyright protection and the integrity of satellite imagery. Simulation results demonstrate that the proposed scheme has no perceptible impact on the quality of the watermarked image and it shows robust resistance against typical signal processing attacks. Three quality indices are utilized to assess the performance of the proposed method; Peak Signal to Noise Ratio (PSNR), Structure Similarity Index Measurement (SSIM) and Wavelet Signal to Noise Ratio (WSNR).

Keywords:
Reversible watermarking, Satellite images, SHA3, Hash function

1. Introduction

With the rapid advent of the Information Technology (IT) and the Internet, digital data can be duplicated, modified and distributed illegally over the globe in a fraction of a second with a relative ease. This issue has become more serious when it comes to special data such as satellite imagery due to its commercial value and the sensitivity of its information. In order to secure this valuable information, the concept of "Digital Watermarking" has been introduced as an effective tool for digital rights management (DRM), to protect the intellectual property and authentication of satellite imagery as well as its tamper recovery.

In this context, digital watermarking is a process of embedding unique identification information (i.e., watermark) into satellite images which can be retrieved later to prove the property ownership without degrading the quality of the protected images. Figure 1 shows a block diagram of the digital watermarking system. Several watermarking techniques have been proposed in the literature for satellite imagery [1-5], which are classified according to different criteria.

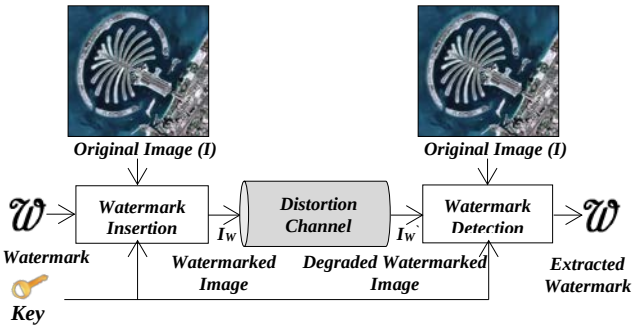

Fig. 1 The block diagram of Watermarking System.

For instance, visible and invisible watermark depends on the perceptivity of the hidden information (i.e., watermark) [6, 7]. Technically, they can be categorized into spatial and transform methods based on the domain in which the hidden information is embedded [8]. Spatial domain methods are comparatively simple because they operate directly at pixel level [9, 10]. However, watermarking methods applied in transform domain remain more resilient to attacks [11]. From the applications point of view, they can be classified into robust and fragile watermarking methods. The robust watermarking methods are commonly used for copyright protection while the fragile methods are used for authentication and tamper detection.

Recently, a novel category of watermarking schemes, Reversible Watermarking, has been gaining more evolution and desirability due to the escalating growth of its applications particularly in healthcare, military communications, etc. In some literature [12, 13], reversible watermarking is identified as invertible, lossless and erasable watermarking. Reversible watermarking of satellite images allows a full restoration of the host image without impacting its quality and permits a complete extraction of the watermark at the decoder. It can be implemented based on the following process. Initially, the watermark ($\boldsymbol{W}$) is inserted into the satellite image ($\boldsymbol{I}$) to get a watermarked one ($\boldsymbol{I_w}$). Afterwards, the $\boldsymbol{I_w}$ is processed through an authenticator to find out if it has been tampered or not. After confirming the authentication, the decoder removes the watermark and recovers the host image. The aim of this paper is to design and develop a novel reversible

Manuscript received March 5, 2019
Manuscript revised March 20, 2019

invisible watermarking scheme based on SHA3 to ensure the copyright protection and the integrity of satellite imagery. The layout of this paper is organized as follows: Section 2 presents the proposed embedding algorithm while Section 3 describes the extraction process. The analysis and comparison of the experimental results are shown in Section 4, and conclusions are discussed in Section 5.

2. Embedding Algorithm

In the proposed fragile reversible invisible watermarking algorithm, the index mapped color logo is embedded in the satellite image for the copyright protection. However, the hash key watermark generated by SHA3 is inserted for the content authentication of satellite images. Both watermarking information is embedded into the color satellite images using additive prediction algorithm and additive predictor error technique.

2.1 Hash Function

A hash function (H) is an efficient tool, which is utilized to map an arbitrary length input message to binary strings of a fixed length message called the hash-value. The primary application of hash functions in watermarking is message integrity. The hash-value provides a digital fingerprint of the watermarked image, which ensures that the watermarked image has not been altered by an intruder. In general, hash functions, are computationally infeasible to find any two messages m1 and m2 such that H(m1) = H(m2). There are several well-known hash functions available today such as Hashed Message Authentication Code (HMAC), Message Digest 2 (MD2), Message Digest 4 (MD4), Message Digest 5 (MD5), Secure Hash Algorithm 0 (SHA-0), Secure Hash Algorithm 1(SHA-1), Secure Hash Algorithm 2(SHA-2) and Secure Hash Algorithm 3(SHA-3). SHA-0 model is proposed by the National Institute of Standards and Technology (NIST) for the Secure Hash Standard (SHS), produces a 160-bit hash value. In our proposed reversible watermarking algorithm, the latest member of the Secure Hash Algorithm family of standards, SHA-3, 512bits length hash function is used for the content authentication of satellite images.

2.2 Watermark Information

In our proposed watermarking algorithm, colour logo is used for copyright protection and SHA-3 hash function generated key is used for the content authentication of color satellite image. Initially, we have converted the colour logo into 2-bits index logo using the index mapping table shown in Table 1 and reshaped into a row vector, which is considered as ownership watermark information. For content authentication, we have divided each layer of colour satellite images into NB non-overlapping blocks and then using SHA-3 hash function, 128 hexadecimal lengths unique key generated for each block and converted into 128×4 bits binary and reshaped into 1×512 bits information. Thus, NB blocks generate NB×512 bits of information is considered as content authentication watermark information in our proposed algorithm.

Table 1: Index mapping table for colour logo

Colour Combinations	Index Key	Binary Value	RGB Value
Colour1	0	00	(33,30,29)
Colour2	1	01	(241,245,247)
Colour3	2	10	(164,148,112)
Colour4	3	11	(34,63,136)

2.3 Additive Prediction Algorithm

The proposed prediction algorithm is used to predict the pixel values of satellite imagery. Initially, divide all the pixels of a satellite image into four groups named odd-odd pixels (OO), odd-even pixels (OE), even-odd pixels (EO) and even-even pixels (EE) respectively as shown in Figure 2. Then, find the average value of neighbor pixels in the horizontal, vertical and diagonal directions denoted by A_h, A_v, A_{d1} and A_{d2} respectively for the selected pixel group (for example: odd-odd pixel group). Afterwards, divide the neighboring pixels into 4 set named horizontal neighbors, vertical neighbors and two diagonal neighbors denoted by N_h, N_v, N_{d1} and N_{d2} respectively. Then estimate pixels intensity variation parameters at horizontal, vertical and diagonal directions, denoted by $\sigma_h^2, \sigma_v^2, \sigma_{d1}^2$ and σ_{d2}^2.

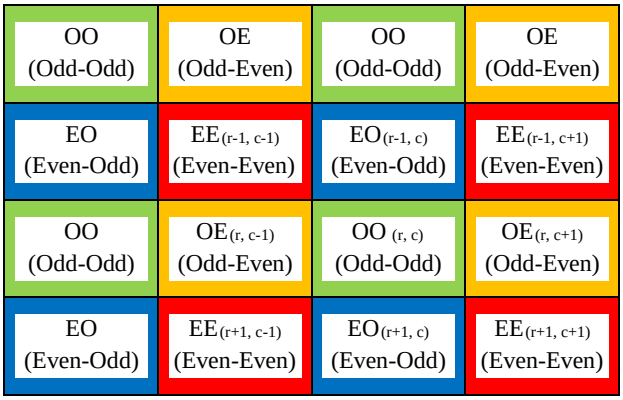

Fig. 2 Image pixels grouping

$$A_h = \left(OE_{(r,c-1)} + OE_{(r,c+1)}\right)/2$$

$$A_v = \left(EO_{(r-1,c)} + EO_{(r+1,c)}\right)/2$$

$$A_{d1} = \left(EE_{(r-1,c-1)} + EE_{(r+1,c+1)}\right)/2$$

$$A_{d2} = \left(EE_{(r+1,c-1)} + EE_{(r-1,c+1)}\right)/2$$

$$N_{h(n)} = \{OE_{(r,c-1)}, OE_{(r,c+1)}, A_h\}$$
$$N_{v(n)} = \{EO_{(r-1,c)}, EO_{(r+1,c)}, A_v\}$$
$$N_{d1(n)} = \{EE_{(r-1,c-1)}, EE_{(r+1,c+1)}, A_{d1}\}$$
$$N_{d2(n)} = \{EE_{(r+1,c-1)}, EE_{(r-1,c+1)}, A_{d2}\}$$
$$\sigma_h^2 = \left(\frac{1}{3}\right) * \sum_{n=1}^{3} \left(N_{h(n)} - A\right)^2$$
$$\sigma_v^2 = \left(\frac{1}{3}\right) * \sum_{n=1}^{3} \left(N_{v(n)} - A\right)^2$$
$$\sigma_{d1}^2 = \left(\frac{1}{3}\right) * \sum_{n=1}^{3} \left(N_{d1(n)} - A\right)^2$$
$$\sigma_{d2}^2 = \left(\frac{1}{3}\right) * \sum_{n=1}^{3} \left(N_{d2(n)} - A\right)^2$$
$$A = (A_h + A_v + A_{d1} + A_{d2})/4$$

Finally, calculate the predicted value of odd-odd pixel as weighted sum of A_h, A_v, A_{d1} and $A_{d2.}$ where C_h, $C_{v,}$ C_{d1} and C_{d2} are the horizontal, vertical and diagonal prediction coefficients respectively and N_f is the normalization factor.

$$P_{(r,c)} = A_h C_h + A_v C_v + A_{d1} C_{d1} + A_{d2} C_{d2}$$
$$C_h = (\sigma_h^2)^{-1}/N_f$$
$$C_v = (\sigma_v^2)^{-1}/N_f$$
$$C_{d1} = (\sigma_{d1}^2)^{-1}/N_f$$
$$C_{d2} = (\sigma_{d2}^2)^{-1}/N_f$$
$$N_f = (\sigma_h^2)^{-1} + (\sigma_v^2)^{-1} + (\sigma_{d1}^2)^{-1} + (\sigma_{d2}^2)^{-1}$$

2.4 Watermark Embedding Algorithm

The proposed embedding algorithm, initially, calculate the pixel's prediction error values E_o of the selected pixel group (example: odd-odd pixels' group) of the original satellite image $S_{o,}$ by calculating the pixel's predicted values P_o using the additive prediction algorithm. Then, the index mapped ownership logo and the content authentication hash key, watermark information W_{key} embedded into the prediction error values E_o of selected pixel's by using the additive predictor error technique. Finally, it generates the reversible watermarked satellite image using the given below equations.

$$E_{o(r,c)} = I_{o(r,c)} - P_{o(r,c)}$$
$$E_{om(r,c)} = \begin{cases} E_{o(r,c)} + W_{key} * sign\left(E_{o(r,c)}\right) * \Delta & ; -\Delta \leq E_{o(r,c)} < \Delta \\ E_{o(r,c)} + W_{key} * \Delta & ; E_{o(r,c)} = 0 \\ E_{o(r,c)} + sign\left(E_{o(r,c)}\right) * \Delta & ; otherwise \end{cases}$$
$$I_{w(r,c)} = E_{om(r,c)} + P_{o(r,c)}$$

where *sign*$(E_{o(r,c)})$ implies +1 if $E_{o(r,c)}$ is positive and -1 if negative. r and c are present the pixel's coordinates of the image, Δ is the watermark strength scaling factor and I_w is the watermarked satellite image.

3. Extracting Algorithm

3.1 Watermark Extraction Algorithm

The proposed additive predictor error technique is used to extract ownership and content authentication watermark information from reversible watermarked satellite imagery. Initially, it will calculate the prediction error values E_w of selected pixel locations of reversible watermarked satellite image $I_{w,}$ by estimating the predicted pixel's values P_w using the additive prediction algorithm. Then, the index mapped ownership logo and content authentication hash key, watermarked information W_{rkey} can be extracted using the equation given below.

$$E_{w(r,c)} = I_{w(r,c)} - P_{w(r,c)}$$
$$W_{rkey} = \begin{cases} 0 \ ; & -\Delta \leq E_{w(r,c)} < \Delta \\ 1 \ ; & -2\Delta \leq E_{w(r,c)} < -\Delta \\ & \text{or } \Delta \leq E_{w(r,c)} < 2\Delta \end{cases}$$

Finally, the ownership colour logo information can be extracted using the same index mapping table used at the encoder as shown in Table 1.

3.2 Satellite Image Restoration Algorithm

Using the proposed additive predictor error technique, we can restore color satellite image I_r from reversible watermarked colour satellite image I_w. Initially, we need to calculate the prediction error values E_w of selected pixel locations of reversible watermarked satellite image $I_{w,}$ by estimating the predicted pixel's values P_w using the additive prediction algorithm. Then, calculate the residual image P_{Er} and restore the colour satellite image using the equations given below.

$$E_{w(r,c)} = I_{w(r,c)} - P_{w(r,c)}$$
$$E_{wo(r,c)} = \begin{cases} E_{w(r,c)} + W_{rkey} * sign\left(E_{w(r,c)}\right) * \Delta & ; -\Delta \leq E_{w(r,c)} < \Delta \\ E_{w(r,c)} + W_{rkey} * \Delta & ; E_{w(r,c)} = 0 \\ E_{w(r,c)} + sign\left(E_{w(r,c)}\right) * \Delta & ; otherwise \end{cases}$$
$$I_{r(r,c)} = E_{wm(r,c)} + P_{w(r,c)}$$

4. Results and Analysis

The performance of the proposed reversible watermarking algorithm is tested on colour satellite images captured by DubaiSat-1 and its grey scale version. Examples are shown in Figure 3, where each satellite image is 1024×1024 pixels. As shown in Figure 4, 128×128 pixels Color logo of University of Dubai is used as the ownership watermark information.

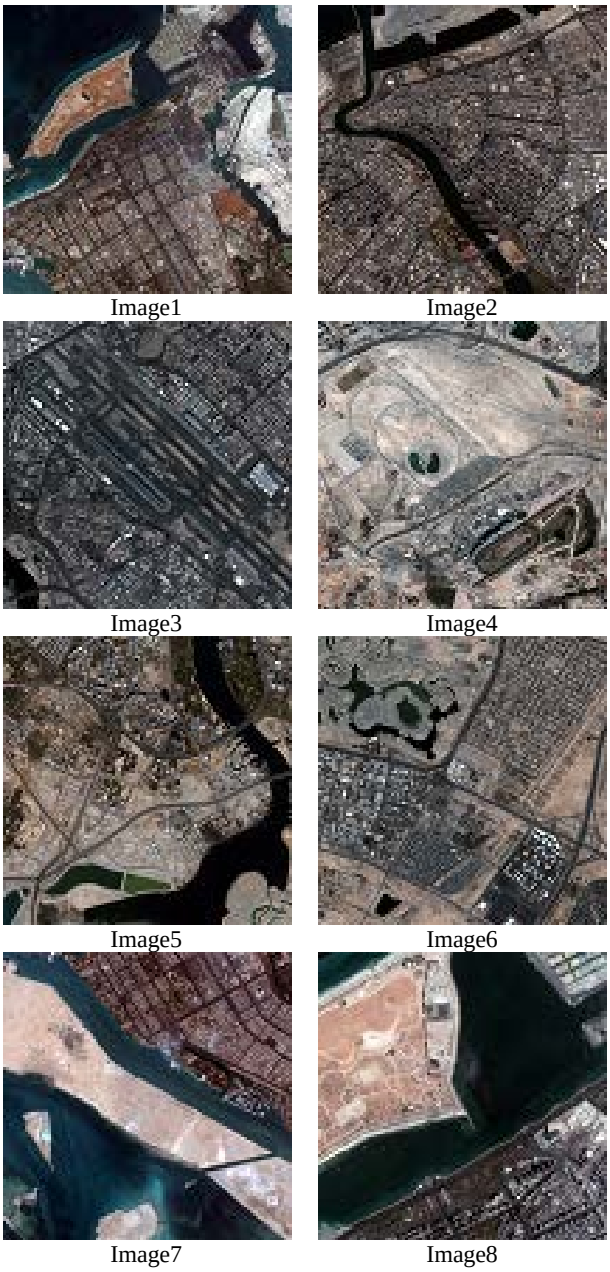

Fig. 3 DubaiSat-1 Color satellite images

Fig. 4 University of Dubai logo (watermark)

Initially, the satellite images are divided into 16 non-overlapping blocks and a unique 256bits length hash-key for each block using SHA-3 hash function is generated for content authentication purpose. The distortion caused to the colour satellite images was assessed by using the Peak Signal to Noise Ratio (PSNR), the Structural Similarity Index Measurement (SSIM) and the Wavelet Signal to Noise Ratio (WSNR).

The Peak Signal to Noise Ratio (PSNR) is the metric used to measure the quality of the watermarked satellite images using pixel-based comparison [3]. If two images are exactly the same, the PSNR will give an infinite value Mathematically, the PSNR is expressed as shown below.

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

$$MSE = \frac{1}{3rc}\sum_{r,c}\left((I_{or} - I_{wr})^2 + \left((I_{og} - I_{wg})\right)^2 + \left((I_{ob} - I_{wb})\right)^2\right)$$

where the MSE represents the cumulative squared error between the watermarked and the original image, I_{or}, I_{og} and I_{ob} represent the red layer, green layer and blue layer components of the original colour satellite image respectively whereas I_{wr}, I_{wg} and I_{wb} are the red layer, green layer and blue layer components of the watermarked colour satellite image.

The PSNR performance analyses of the reversible watermarked satellite images are shown in Tables 2, 3 and 4. Table 4 shows the PSNR performance comparison for color satellite Image1, when the ownership watermark information and hash generated authentication watermark information is embedded at eve-even, even-odd, odd-even and odd-odd pixel locations. From Figure 5, it has been noticed that as the scaling factor increases, the PSNR decreases.

Table 2: PSNR Performance Analysis of DubaiSat-1 Images

Δ=4 [*O-O Pixels Group*]	**PSNR (in dB) Watermarked Images**		**PSNR (in dB) Restored Images**	
	Grey	**Color**	**Grey**	**Color**
Image1	54.242	54.216	∞	∞
Image2	53.781	53.627	∞	∞
Image3	50.026	49.787	∞	∞
Image4	50.961	50.651	∞	∞
Image5	51.674	51.569	∞	∞
Image6	49.688	49.556	∞	∞
Image7	50.390	50.255	∞	∞
Image8	54.046	53.845	∞	∞
Image9	55.268	55.194	∞	∞
Image10	53.566	53.361	∞	∞
Image11	51.797	51.576	∞	∞
Image12	52.783	52.482	∞	∞

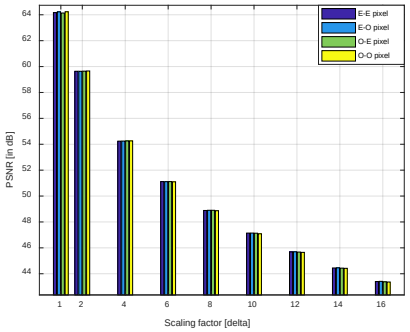

Fig. 5 PSNR Performance Analysis of Color Image1

Table 3: PSNR Performance Analysis of DubaiSat-1 Images

Δ [O-O Pixels Group]	**PSNR (in dB) Watermarked Image1**		**PSNR (in dB) Restored Image1**	
	Grey	**Color**	**Grey**	**Color**
1	64.164	63.936	∞	∞
2	59.639	59.575	∞	∞
4	54.242	54.216	∞	∞
6	51.115	51.085	∞	∞
8	48.887	48.857	∞	∞
10	47.141	47.115	∞	∞
12	45.684	45.674	∞	∞
14	44.446	44.447	∞	∞
16	43.397	43.370	∞	∞

Table 4: PSNR Performance Analysis of Color Image1

Δ	**O-O Pixels Group**	**O-E Pixels Group**	**E-O Pixels Group**	**E-E Pixels Group**
1	63.936	64.004	63.912	63.990
2	59.575	59.555	59.579	59.568
4	54.216	54.212	54.236	54.218
6	51.085	51.087	51.096	51.069
8	48.857	48.861	48.864	48.832
10	47.115	47.118	47.107	47.083
12	45.674	45.684	45.672	45.639
14	44.447	44.450	44.433	44.409
16	43.370	43.375	43.355	43.332

The Structure Similarity Index Measurement (SSIM) is a method for measuring the similarity between two images by comparing the local pattern of pixel intensities that have been normalized for luminance and contrast [7]. If two images are exactly the same, the SSIM value will be 1. Noting that, higher SSIM value means better similarity between the images. Mathematically, SSIM is expressed as shown below.

$$SSIM(I_o, I_w) = \left(L(I_o, I_w)\right)^{\alpha}.\left(C(I_o, I_w)\right)^{\beta}.\left(S(I_o, I_w)\right)^{\gamma}$$

$$L(\mathrm{Io}, Iw) = \frac{2\mu_X\mu_Y + A}{\mu_X^2 + \mu_Y^2 + A},\ C(Io, Iw) = \frac{2\sigma_X\sigma_Y + B}{\sigma_X^2 + \sigma_Y^2 + B},\ S(Io, Iw) = \frac{\sigma_{XY} + C}{\sigma_X\sigma_Y + C}$$

where I_o represents the original satellite image and I_w represents a watermarked satellite image. *L*, C, and S indicate the luminance, contrast and structure components respectively. However, α, β, γ are parameters used to adjust the relative importance of the luminance, contrast and structure components.

Table 5: SSIM Performance Analysis of DubaiSat-1 Images

Δ=4 [*O-O Pixels Group*]	SSIM Watermarked Images		SSIM Restored Images	
	Grey	Color	Grey	Color
Image1	0.9998	0.9998	1.0000	1.0000
Image2	0.9999	0.9999	1.0000	1.0000
Image3	1.0000	0.9999	1.0000	1.0000
Image4	1.0000	1.0000	1.0000	1.0000
Image5	0.9999	0.9999	1.0000	1.0000
Image6	0.9999	0.9999	1.0000	1.0000
Image7	0.9999	0.9999	1.0000	1.0000
Image8	0.9999	0.9999	1.0000	1.0000
Image9	0.9999	0.9999	1.0000	1.0000
Image10	1.0000	1.0000	1.0000	1.0000
Image11	1.0000	1.0000	1.0000	1.0000
Image12	1.0000	1.0000	1.0000	1.0000

Table 6: SSIM Performance Analysis of Image1

Δ [O-O Pixels Group]	SSIM Watermarked Image1		SSIM Restored Image1	
	Grey	Color	Grey	Color
1	1.0000	1.0000	1.0000	1.0000
2	1.0000	0.9999	1.0000	1.0000
4	0.9998	0.9998	1.0000	1.0000
6	0.9997	0.9997	1.0000	1.0000
8	0.9995	0.9995	1.0000	1.0000
10	0.9992	0.9993	1.0000	1.0000
12	0.9991	0.9991	1.0000	1.0000
14	0.9988	0.9988	1.0000	1.0000
16	0.9985	0.9985	1.0000	1.0000

Table 7: SSIM Performance Analysis of Color Image1

Δ	O-O Pixels Group	O-E Pixels Group	E-O Pixels Group	E-E Pixels Group
1	1.0000	1.0000	1.0000	1.0000
2	0.9999	0.9999	0.9999	0.9999
4	0.9998	0.9998	0.9998	0.9998
6	0.9997	0.9996	0.9997	0.9996
8	0.9995	0.9994	0.9995	0.9994
10	0.9993	0.9992	0.9992	0.9992
12	0.9991	0.9990	0.9990	0.9990
14	0.9988	0.9987	0.9988	0.9987
16	0.9985	0.9985	0.9985	0.9985

The SSIM performance analyses of the reversible watermarked satellite images are shown in Tables 5, 6 and 7. Table 7 illustrates the SSIM performance comparison for color satellite Image1, when the ownership watermark information and hash generated authentication watermark information is embedded at even-even, even-odd, odd-even and odd-odd pixel locations.

Table 8: WSNR Performance Analysis of DubaiSat-1 Images

Δ=4 [*O-O Group*]	WSNR (in dB) Watermarked Images		WSNR (in dB) Restored Images	
	Grey	Color	Grey	Color
Image1	67.228	67.456	∞	∞
Image2	70.548	71.303	∞	∞
Image3	68.872	69.653	∞	∞
Image4	70.078	70.888	∞	∞
Image5	70.791	71.995	∞	∞
Image6	68.636	69.440	∞	∞
Image7	69.695	70.349	∞	∞
Image8	71.817	73.092	∞	∞
Image9	71.558	72.699	∞	∞
Image10	72.136	73.371	∞	∞
Image11	69.773	70.851	∞	∞
Image12	71.146	72.319	∞	∞

Table 9: WSNR Performance Analysis of Image1

Δ [O-O Pixels Group]	WSNR (in dB) Watermarked Image1		WSNR (in dB) Restored Image1	
	Grey	Color	Grey	Color
1	67.228	67.456	∞	∞
2	70.548	71.303	∞	∞
4	68.872	69.653	∞	∞
6	70.078	70.888	∞	∞
8	70.791	71.995	∞	∞
10	68.636	69.440	∞	∞
12	69.695	70.349	∞	∞
14	71.817	73.092	∞	∞
16	71.558	72.699	∞	∞

The Wavelet-domain Signal to Noise Ratio (WSNR) is another metric employed to measure the quality of watermarked images but it is more accurate than PSNR in terms of subjective assessment [24, 25]. The WSNR predicts the image quality based on a particular viewing distance by considering both image details and edge maps in the wavelet domain. The WSNR has low complexity in comparison with other assessment tools because it doesn't require the extraction of the human visual system

coefficients. If two images are exactly the same, the WSNR will be infinite. The WSNR performance analyses of the reversible watermarked satellite images are shown in Tables 8, 9 and 10. Table 10 shows the WSNR performance comparison for color satellite Image1, when ownership watermark information and hash generated authentication watermark information is embedded at even-even, even-odd, odd-even and odd-odd pixel locations.

Table 10: WSNR Performance Analysis of Color Image1

Δ	O-O Group	O-E Group	E-O Group	E-E Group
1	77.954	77.987	77.677	77.918
2	73.523	73.613	73.449	73.535
4	67.456	67.573	67.461	67.698
6	63.679	63.891	63.780	63.897
8	61.266	61.255	61.253	61.480
10	59.168	59.254	59.252	59.409
12	57.489	57.501	57.501	57.566
14	56.247	56.385	56.324	56.281
16	54.912	54.856	54.871	54.917

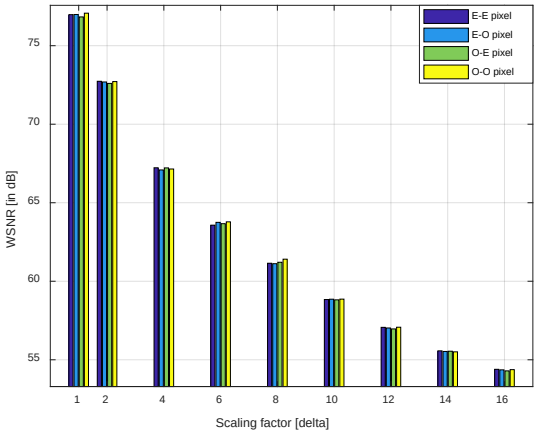

Fig. 6 WSNR Performance Analysis of Color Image1

From Figure 6, it has been observed that as watermark scaling factor increases, WSNR decreases for watermarked satellite Image1. The PSNR, WSNR and SSIM performance analyses of reversible watermarked satellite images are shown in Tables 11. From Table 12, an inversely proportional relationship exists between watermark scaling factor and PSNR, SSIM, and WSNR.

Table 11: Performance Analysis of DubaiSat-1 Images

Δ= 4 [*O-O Pixels Group*]	**Watermarked Color Images**			**Restored Color images**		
	PSNR (in dB)	**WSNR (in dB)**	**SSIM**	**PSNR (in dB)**	**WSNR (in dB)**	**SSIM**
Image1	54.216	67.456	0.9998	∞	∞	1.0000
Image2	53.627	71.303	0.9999	∞	∞	1.0000
Image3	49.787	69.653	0.9999	∞	∞	1.0000
Image4	50.651	70.888	1.0000	∞	∞	1.0000
Image5	51.569	71.995	0.9999	∞	∞	1.0000
Image6	49.556	69.440	0.9999	∞	∞	1.0000
Image7	50.255	70.349	0.9999	∞	∞	1.0000
Image8	53.845	73.092	0.9999	∞	∞	1.0000
Image9	55.194	72.699	0.9999	∞	∞	1.0000
Image10	53.361	73.371	1.0000	∞	∞	1.0000
Image11	51.576	70.851	1.0000	∞	∞	1.0000
Image12	52.482	72.319	1.0000	∞	∞	1.0000

Table 12: Performance Analysis of Image1

Δ [*O-O Pixels Group*]	**Watermarked Color Images**			**Restored Color Images**		
	PSNR (in dB)	**WSNR (in dB)**	**SSIM**	**PSNR (in dB)**	**WSNR (in dB)**	**SSIM**
1	63.936	77.954	1.0000	∞	∞	1.0000
2	59.575	73.523	1.0000	∞	∞	1.0000
4	54.216	67.456	0.9998	∞	∞	1.0000
6	51.085	63.679	0.9997	∞	∞	1.0000
8	48.857	61.266	0.9995	∞	∞	1.0000
10	47.115	59.168	0.9992	∞	∞	1.0000
12	45.674	57.489	0.9991	∞	∞	1.0000
14	44.447	56.247	0.9988	∞	∞	1.0000
16	43.370	54.912	0.9985	∞	∞	1.0000

Data hiding capacity refers to the maximum amount of watermark information embedded to cover image. In the proposed algorithm, we can hide watermark information at four different sets of pixel locations such as even-even pixels, even-odd pixels, odd-even pixels and odd-odd pixels. Similarly, for color satellite images, we can hide watermark information in red layer, green layer and blue layer of images. The hiding capacity performance analyses of the reversible watermarked satellite images are shown in Tables 13-18. Tables 13 and 15 show the data hiding capacity comparison for satellite images, when ownership watermark information and hash generated authentication watermark information are embedded at eve-even, even-odd, odd-even and odd-odd pixel locations.

Table 13: Hiding Capacity of Dubaisat-1 Gray Scale Images

Δ	O-O Group	O-E Group	E-O Group	E-E Group
Image1	137143	137136	137534	137346
Image2	132383	132448	132395	132434
Image3	118672	118551	118512	118867
Image4	119709	119435	121880	121833
Image5	167383	167602	167442	167595
Image6	91225	92042	91551	91531
Image7	175136	175072	175004	175018
Image8	203194	201995	204125	199208
Image9	231325	230330	231712	228179
Image10	221707	219850	221346	218438
Image11	174996	169741	173985	168655
Image12	190086	184589	188777	185629

Table 14: Hiding Capacity of Gray Scale Image1

Δ	O-O Group	O-E Group	E-O Group	E-E Group
1	72466	72177	72504	72659
2	104992	104559	105152	104981
4	137143	137136	137534	137346
6	160261	160227	160632	160474
8	178106	178277	178643	178297
10	192454	192446	192866	192654
12	204003	204132	204351	204273
14	213509	213654	213608	213693
16	221120	221416	221164	221376

Table 15: Hiding Capacity of DubaiSat-1 Color Images

Δ= 4	O-O Group	O-E Group	E-O Group	E-E Group
Image1	406468	406548	407463	407024
Image2	391960	391907	392331	392327
Image3	340021	339159	339921	340430
Image4	340417	340633	349399	349661
Image5	490802	491593	491659	491614
Image6	265767	267628	266899	266512
Image7	515661	515091	514997	515511
Image8	589083	588925	592414	580107
Image9	683294	681894	684789	675996
Image10	651707	647670	650877	644136
Image11	507039	495850	503258	493417
Image12	550419	537797	546241	540534

Tables 14 and 16 display the data hiding capacity comparison for satellite Image1 under different scaling factors. Similarly, Tables 17 and 18 show the layers by layer data hiding capacity comparison for color satellite Image1 at even-even and odd-odd pixel locations. From Tables 14, 16, 17 and 18, it has been noticed that as watermark scaling factor increases, hiding capacity increases for satellite images.

Table 16: Hiding Capacity of Color Image1

Δ	O-O Group	O-E Group	E-O Group	E-E Group
1	208361	208285	208584	209358
2	308056	307171	308326	307487
4	406468	406548	407463	407024
6	476203	475819	476985	476376
8	530112	530113	531088	530447
10	573139	572990	574228	573508
12	607948	608054	608876	608657
14	636523	636948	637074	637271
16	660077	660560	660431	660782

Table 17: Odd-Odd Group Hiding Capacity of Color Image1

Δ	R Layer	G Layer	B Layer	RGB Layers
1	75417	69604	63340	208361
2	106638	103506	97912	308056
4	140306	136387	129775	406468
6	164160	159580	152463	476203
8	182218	177586	170308	530112
10	196385	191978	184776	573139
12	207802	203609	196537	607948
14	217017	213256	206250	636523
16	224512	220859	214706	660077

Table 18: Even-Even Group Hiding Capacity of Color Image1

Δ	R Layer	G Layer	B Layer	RGB Layers
1	75634	70121	63603	209358
2	106334	103680	97473	307487
4	140429	136629	129966	407024
6	164142	159758	152476	476376
8	182326	177784	170337	530447
10	196533	192323	184652	573508
12	207984	204166	196507	608657
14	217131	213588	206552	637271
16	224705	221228	214849	660782

The PSNR, WSNR and Hiding Capacity performance analyses of the reversible watermarked color satellite Image1 and its gray scale version are shown in Tables 19 and 20.

Table 19: Performance Analysis of Gray Scale Image1

Δ	PSNR		WSNR		CAPACITY	
	O-O Group	E-E Group	O-O Group	E-E Group	O-O Group	E-E Group
1	64.164	64.234	76.978	77.070	72466	72659
2	59.639	59.661	72.734	72.715	104992	104981
4	54.242	54.260	67.228	67.148	137143	137346
6	51.115	51.100	63.572	63.784	160261	160474
8	48.887	48.868	61.147	61.406	178106	178297
10	47.141	47.088	58.835	58.862	192454	192654
12	45.684	45.652	57.065	57.073	204003	204273
14	44.446	44.420	55.570	55.505	213509	213693
16	43.397	43.363	54.393	54.372	221120	221376

Table 20: Performance Analysis of Color Image1

Δ	PSNR		WSNR		CAPACITY	
	O-O Group	E-E Group	O-O Group	E-E Group	O-O Group	E-E Group
1	63.936	63.990	77.954	77.918	208361	209358
2	59.575	59.568	73.523	73.535	308056	307487
4	54.216	54.218	67.456	67.698	406468	407024
6	51.085	51.069	63.679	63.897	476203	476376
8	48.857	48.832	61.266	61.480	530112	530447
10	47.115	47.083	59.168	59.409	573139	573508
12	45.674	45.639	57.489	57.566	607948	608657
14	44.447	44.409	56.247	56.281	636523	637271
16	43.370	43.332	54.912	54.917	660077	660782

In the proposed reversible watermarking algorithm, SHA-3 hash function is used for content authentication purpose. Any tampering on watermarked satellite image, even if a single pixel value is changed by1 at any location, block and layer of the satellite image, it will make a difference between the recovered and the re-generated SHA-3 hash-keys as shown in Table 21. Table 22 shows the PSNR, WSNR and authentication performance of the watermarked color satellite Image1 under tampering attacks. The developed reversible watermarking algorithm is very sensitive to any modifications or tampering to the watermarked satellite images.

Table 21: Hash Authentication Performance Analysis

Image Block1 regenerated hash key	Image Block1 extracted hash key	Conclusion
89B0876351BD0F61 09380DE78E242F00 064B8E40134EE16E CECFF6D9D1FEFF0D	89B0876351BD0F61 09380DE78E242F00 064B8E40134EE16E CECFF6D9D1FEFF0D	No Tampering In R Layer-Block1
89B0876351BD0F61 09380DE78E242F00 064B8E40134EE16E CECFF6D9D1FEFF0D	5AB33DCA15207C12 7E38A9F019E6BBAE 99922984126CF3EE FD80814494BDF8CF	Tampering In R Layer-Block1

Table 22: Performance Analysis Under Tampering Attack

Δ= 4 [*E-E*]	Restored Color Satellite Image1			
	PSNR (in dB)	WSNR (in dB)	Tampering details	
			Count	Location
Case1	99.127	120.378	1	R Layer-Block1
Case2	99.129	116.856	1	G Layer-Block1
Case3	92.139	110.717	2	R Layer-Block 1 G Layer-Block 4
Case4	94.357	114.937	3	R Layer-Block 1 and 3 G Layer-Block 4
Case5	93.108	112.419	4	G Layer-Block 2 and 4 B Layer-Block 1 and 3

5. Conclusion

This paper presents a novel reversible watermarking technique using hash function and adaptive prediction algorithm for copyright protection and data integrity of DubaiSat-1 images. The ownership copyright protection algorithm is implemented by embedding watermark information and SHA-3 Hash key into satellite images. The distortion caused by watermarking process is assessed by using peak signal to noise ratio, similarity structure index measurement and wavelet signal to noise ratio. The performance of the proposed reversible watermarking algorithm is successfully tested using a number of 1024×1024 pixels 24-bit color satellite images captured by DubaiSat-1 and its grayscale versions. The experimental results demonstrate that the proposed algorithm has a better embedding capacity, signal to noise ratio and can precisely detect the tampered areas using the hash key.

References

[1] I. Kullayamma and P. Sathyanarayana, "Satellite enhanced image watermarking using gradient direction quantization," in 2015 International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO), 1–9 (2015).

[2] M. Abolfathi and R. Amirfattahi, "A reliable watermarking algorithm based on wavelet transform for satellite images," in 2009 International Conference on Multimedia Information Networking and Security, 1, 588–592 (2009).

[3] S. Al-Mansoori and A. Kunhu, "Robust watermarking technique based on DCT to protect the ownership of DubaiSat-1 images against attacks," International Journal of Computer Science and Network Security (IJCSNS), Vol.12, No.6, 1-9 (2012).
[4] Q. A. Kester, L. Nana, A. C. Pascu, et al., "A hybrid image cryptographic and spatial digital watermarking encryption technique for security and authentication of digital images," in 2015 17th UKSim-AMSS International Conference on Modelling and Simulation (UKSim), 322–326 (2015).
[5] J. S. Y. Jeedella and H. A. Ahmad, "An Algorithm for watermarking mobile phone colour images using BCH code" in 2011 IEEE GCC Conference and Exhibition, 19-22 (2012).
[6] K. A. Ahmed, H. A. Ahmad and P. Gaydecki, "Robust image watermarking using two dimensional Walsh code" in IET Conference on Image Processing (IPR2012), 1-5 (2012).
[7] Alavi Kunhu and Hussain Al-Ahmad, "A New Multi Watermarking Algorithm Based on DWT and Hash Functions for Color Satellite Images", IEEE International Conference on Electronics, Circuits, and Systems (ICECS2013), Abu Dhabi, UAE, 429-432 (2013).
[8] A. Ben Sewaif, M. Al-Mualla and H. Al-Ahmad, 2 D Walsh coding for robust digital image watermarking, Proceedings of the 4th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), Italy, 302-305 (2004).
[9] A. Al-Gindy, H. Al-Ahmad, A. Tawfik and R. Qahwaji, A new blind image watermarking of handwritten signatures using low-frequency DCT coefficients, Proceedings of the IEEE ICSPC Conference, UAE, 1367-1370 (2007).
[10] M. Chen, Z. Chen, X. Zeng, and Z. Xiong "Reversible image watermarking based on full context prediction," 16th IEEE International conference on Image Processing (ICIP), Cairo, Egypt, 4197-4200 (2009).
[11] J. Tian, "Reversible data embedding using a difference expansion," IEEE Transactions on Circuits and Systems for Video Technol, Vol. 13, No. 8, 890-896 (2003).
[12] S. Al-Mansoori and A. Kunhu, "Hybrid DWT-DCT-Hash function based digital image watermarking for copyright protection and content authentication of DubaiSat-1 images," High Performance Computing in Remote Sensing IV Conference, Published by International Society for Optics and Photonics. (2014)
[13] A. Kunhu and H. Al-Ahmad, "A new watermarking algorithm for color satellite images using color logos and hash functions," in 2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks, 251–255 (2013).
[14] S. Al-Mansoori and A. Kunhu, "Multi-watermarking scheme for copyright protection and content authentication of DubaiSat-1 satellite imagery," Satellite Data Compression, Communications, and Processing IX Conference, (2013). Published by International Society for Optics and Photonics.
[15] Z. Zhang, H. Peng and X. Long, "A Fragile Watermarking Scheme Based On Hash Function for Web Pages", International Conference on Network Computing and Information Security, 417-420 (2011).
[16] J. Cannons, and P. Moulin, "Design and Analysis of a Hash-Aided Image Watermarking System", IEEE transaction on image processing, Vol.13, No.10, 1393-1408 (2004)
[17] S. Al-Mansoori and A. Kunhu, "Discrete cosine transform and hash functions toward implementing a (robust-fragile) watermarking scheme," High Performance Computing in Remote Sensing III Conference, Published by International Society for Optics and Photonics (2013).
[18] S. P. Jaiswal, O. C. Au, V. Jakhetiya, Y. Guo, A. K. Tiwari, K. Yue, "Efficient Adaptive Prediction Based Reversible Image Watermarking," 20th IEEE International Conference on Image Processing (ICIP), Melbourne, Australia, 4540-4544 (2014).
[19] Z. Wang, A. Bovic, H. Sheikh, and E. Simoncelli, "Image Quality Assessment: From Visibility to Structural Similarity," IEEE Transactions on Image Processing, 600-612 (2004)
[20] S. Rezazadeh, S. Coulombe, "A novel discrete wavelet domain error-based image quality metric with enhanced perceptual performance," International Journal of Computer and Electrical Engineering (IJCEE), , Vol. 4, No. 3, (2012).

Dr. Alavikunhu Panthakkan is a dynamic research scientist in electronics engineering. 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 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) and member of Institute of Research Engineers and Doctors (IRED).

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.

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. His research interests are in the areas of engineering education, signal and image processing, multimedia, remote sensing and propagation. He has published

over 120 papers in international conferences and journals and has a UK patent. 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.