Highly Efficient Copyright Protection Algorithm for Satellite Imagery Using Turbo Product Codes

Sara AlMaeeni[†], Alavi Kunhu[††] and Hussain Al-Ahmad[††]

[†]Mohammed bin Rashid Space Centre, Dubai, UAE
[††]University of Dubai, Dubai, UAE

Summary
Satellite imagery has been used in many applications and fields of research. This paper proposes a novel algorithm used in embedding a serial key information into satellites Imagery. The proposed algorithm is based on encoding the information using turbo product code (TPC) in discrete wavelet transform (DWT) domain. The watermarked imagery was evaluated using a wavelet domain based signal to noise ratio (WSNR), that were proved to be simple and more accurate than the spatial domain peak signal to noise ratio (PSNR) in terms of the objective assessment. Besides, it predicts the image quality based on a particular viewing distance. The evaluation considered color images; RGB, YCbCr, and grayscale images. Experimental results show that the proposed algorithm is very efficient in protecting the copyright ownership of the satellite imagery. Also, the proposed algorithm survived various attacks such as JPEG compression, geometrical rotation, resizing, cropping, and filtering.

Key words:
Watermarking; turbo code; satellite imagery; image copyright.

1. Introduction

Satellite imagery is one of the most powerful resources for many types of research such as meteorology, agriculture mapping, and environmental monitoring [1, 2]. These images contain a large number of data that are helpful in analyzing, understanding, and providing new insights into universal development. The transmission and storage procedures of these images are straightforward and quick, due to the rapid evolution of the Internet, this makes these images vulnerable to the risk of being copied and tampered with. Consequently, substantial interest and efforts by the researchers have been done to introduce different technologies to resolve the data security, copyright, and protection issues. Such technologies are digital watermarking, Steganography, and cryptography [3-9].

Digital watermarking is one of the most popular techniques used in multimedia data that comes in different formats such as audio, image, and video [10]. Digital watermarking prevents unauthorized copy of the digital media by inserting hidden information that can be image, text, or number. The hidden information must satisfy four factors: perceptual transparency, robustness, security, and data hiding capacity [11]. Moreover, digital watermarking has also been applied to various applications such as broadcast monitoring, image labeling and indexing [12, 13].

The embedding process of the watermark could be done in spatial domain [14] or transform (frequency) domain [15, 16]. In the spatial domain, the watermark is embedded directly in the least significant bits (LSB) of the cover image pixels [17]. On the other hand, transform domain watermarking is based on using the discrete cosine transforms (DCT), discrete wavelet transforms (DWT) or any other transform techniques. The watermark information is inserted into specific coefficients in the transform domain. The embedding is done in the low-frequency coefficients so that the watermark will survive attacks such as JPEG compression and low-pass filtering that affects the high-frequency coefficients.

The robustness parameter in watermarking indicates the ability to restore the hidden information after attacks. Error correcting codes are a powerful technique used to improve the robustness of watermarked images [18-23]. In [22], AlMaeeni et al. investigated turbo product code (TPC) in embedding logo in grayscale images. In [23] and [24], Jeedella et al. investigated Reed-Solomon (RS) code and Binary Coded Decimal (BCH) code for embedding phone number digits in color images. Due to its small size, multiple copies of phone watermark information can be embedded in the image compared to a logo. Hence phone information can survive more attacks like cropping attack. In [25], Kamal et al. investigated Walsh code in embedding a binary signature in color images using Discrete Cosine Transform (DCT). In [26], a logo embedding algorithm that is based on texturization method is proposed. The algorithm is firstly separate the host image into rich and poor textured areas. After that, the textured of the logo is transformed to a similar texture of the host image. The proposed algorithm showed a better performance compared to conventional embedding. One fact of strong embedding algorithm is that it introduces more distortion to the host image. This fact motivated the researchers to investigate other watermarking techniques like quantization and spread-spectrum modulations [27, 28].

In this paper, we propose a robust copyright algorithm using TPC to embed serial key information. The proposed

Manuscript received July 5, 2019
Manuscript revised July 20, 2019

algorithm is evaluated using different grayscale and color satellite imagery in the wavelet domain. Compared to other proposed solutions in the literature, the proposed algorithm will provide the following advantages:

- Due to the implementation of TPC encoding, the ownership information will be more secure in the proposed algorithm. Particularly, it will be difficult for unauthorized users to extract ownership information from watermarked satellite imagery without knowing the applied error correction code type.
- The proposed algorithm will survive cropping attacks more than most of the previously proposed algorithm such as in [22] and [23]. The multiple copies of TPC encoded ownership information can be embedded into satellite images to enhance the robustness against cropping.
- The proposed algorithm will use checksum-bits algorithm. Therefore, it can survive geometrical rotation attacks up to 30 degrees or sometimes even more without using any reference images.
- The proposed algorithm will use the voting method to extract the ownership information from multiple copies of decoded watermark information.
- Unlike most work in the literature, the proposed algorithm will evaluate by using wavelet domain based signal to noise ratio (WSNR), which was proved to be simple and more accurate than the spatial domain peak signal to noise ratio (PSNR) in terms of the objective assessment because it takes into consideration both image details and edge maps in the wavelet domain. In addition, it has low complexity in comparison with other assessment tools because it does not require the extraction of the human visual system coefficients. Moreover, it predicts the image quality based on a particular viewing distance.
- The proposed algorithm will evaluate using three models of images; RGB, YCbCr, and grayscale.

The rest of the paper is structured as follows. Section II provides background, the concepts of TPC, and hard decoding process; Section III describes the purposed watermarking methodology in details; Section IV shows extensive experimental results and analysis. Finally, Section V contains the conclusion.

2. Turbo Product Code

Turbo codes are a class of error correcting codes introduced by Berrou in [29, 30] that come close to approaching Shannon's limit than any other class of error correcting codes [29]. The general concept of the turbo codes is to construct two or more simple codes in order to achieve remarkable error performance with manageable complexity. By using turbo codes, large minimum Hamming distance (d_{min}) can be obtained from simple block codes. Hence, turbo codes do not suffer from error floor problem [30]. Turbo codes are formed using either serial or parallel concatenation. In parallel concatenation, the same information bits, but in different order input to two encoders. The outputs of the two encoders are then joined together. On the other hand, the output of one encoder is fed to the next encoder in serial concatenation.

Turbo product codes (TPCs), also known as a block turbo codes (BTCs) are a simple and efficient method used to construct powerful codes where high code rates are required. It is formed by the serial concatenation of two linear systematic block codes with block inter-leaver in between. It has been used as forward error correction (FEC) code in IEEE 802.16 standard for fixed and mobile broadband access known as worldwide interpretability for microwave access(WiMAX) [32].

TPCs are a multidimensional array of (n, k) block codes with (n_i, k_i, $d^{(1)}_{min}$), i={1; 2} parameters, here, n_i and k_i are the codeword length and number of information bits respectively. A two-dimensional product code is obtained from two systematic linear block codes $C^1(n_1, k_1, d^{(1)}_{min})$ and $C^2(n_2, k_2, d^{(2)}_{min})$.

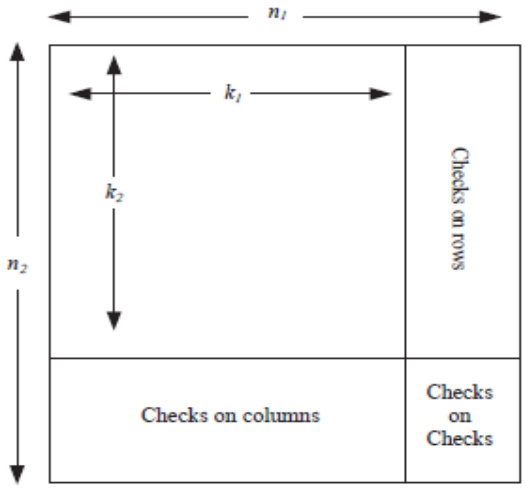


Fig. 1 TPC Construction

With reference to Fig.1, the codeword C is constructed as follows;

1. Placing (k_1 x k_2) information bits in a rectangle shape with width k_1 and height k_2;
2. Coding the $k_1$bits in each row using code C^2;
3. Coding the n_2 bits in each columns using code C^1.

The codeword length, number of information bits and minimum Hamming distance of the constructed product code C are $n = n_1 \times n_2$, $k = k_1 \times k_2$ and $d_{min} = d^{(1)}_{min} \times d^{(2)}_{min}$ respectively. Hence the correcting capability, t, of the new constructed TPC is given by:[31]

$$t=\left\lfloor \frac{d^{(1)}_{min} d^{(2)}_{min} - 1}{2} \right\rfloor \quad (1)$$

where $\lfloor a \rfloor$ denotes the largest integer less than or equal to a.

2.1 Hard Iterative Decoding of TPC

Assume that additive white Gaussian noise (AWGN) channel and binary phase shift keying (BPSK) modulation, $\{0 \rightarrow -1, 1 \rightarrow +1\}$ are used. Let the received sequence be

$$R = W + Z \quad (2)$$

where $W = (w_{1,1}, \ldots\ldots, w_{n1,n2})$ is the signal transmitted and $Z = (z_{1,1}, \ldots\ldots, z_{n1,n2})$ is the Gaussian noise sample with zero mean and $N_0/2$ variance. Hard-input hard-output (HIHO) decoding of TPCs can be achieved by applying the conventional hard decision decoding to decode the component codes that form the TPC. The decoding process starts by converting the received matrix R into binary matrix $H = (h_{1,1}, \ldots\ldots, h_{n1,n2})$, where $h_{i,j} \in \{0,1\}$. The decoding process starts row-by-row (or column-by-column) till the last row. The resultant matrix is decoded in the same manner but in the other direction. The first decoder focuses on the row structure of the product code, while the second decoder focuses on the column structure. The execution of the first decoder is called half-iteration, while the execution of the second decoder is called full-iteration. Although this decoding process is suboptimal, it has much lower complexity compared to the maximum likelihood decoding (MLD) where the received matrix has to be compared with the entire code space and the decisions is made in favor of the codeword that is close in terms of Hamming distance to the received sequence.[34]

3. Proposed Methodology

The procedure of embedding the TPC encoded ownership information is described in Algorithm 1. The proposed ownership protection algorithm embeds the TPC encoded ownership serial key information into a desired channel of the color satellite imagery. There are different models for color images, however, the most commonly used models are the RGB and the YC_bC_r model. In the RGB model image, any color can be produced from the three basic colors; red, green, and blue. On the other hand, the YC_bC_r model image contains one luminance (Y) layer and two chrominance layers, which are formed by subtracting the luminance from red and blue layers. The main advantages of the YC_bC_r model are decoupling of luminance and color information. The luminance component can be processed without affecting image color components [35].

Based on the proposed algorithm, after selecting the suitable channel of satellite imagery, a multi-level DWT of the selected channel is applied. The DWT decomposes an image into a lower resolution (*LL*), horizontal (*HL*), vertical (*LH*) and diagonal (*HH*) detail components. Accurate aspects of the human visual system (HVS) is the main advantages of the wavelet transform as compared to the DCT and this allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high-resolution detail bands *LH, HL, HH*. Embedding watermarks in these regions allow us to increase the robustness of our watermark with negligible impact on image quality [35]. For its simplicity, the Haar transform is used in the proposed methodology. It is basically a sequence of rescaled (square-shaped) functions which together form a wavelet family. After that, the TPC encoded ownership information is embedded into the selected *LL* sub-band coefficients using scaled odd/even embedding method. Here, the sub-band coefficient value is converted to their nearest odd or even integer, depending on whether the watermark information bit is 1 or 0, respectively. Suppose that the selected coefficient value is 4 and we wish to embed 0, then the pixel value gets mapped to the nearest even number, which is 4. For embedding 1, we use either sequence, with numbers in the range [-0.5, 0.5] which are produced by a pseudorandom generator, to decide whether to map 4 to 3 or 5. The embedding process is processed as follows:

$$\text{To embed } 1 \rightarrow q = \text{round}\,(p + 1 - \text{mod}\,(p - \eta, 2)),$$
$$\text{To embed } 0 \rightarrow q = \text{round}\,(p + 1 - \text{mod}\,(p + 1 - \eta, 2)), \quad (3)$$

where p, is the original coefficient value that is mapped to q. Also, η denotes the corresponding number obtained from the sequence, mod (p, 2) denotes the remainder obtained after dividing p by 2, and round denotes the rounding off operation. If p is an even number and 1 is to be embedded, it is mapped to ($p - 1$) or ($p + 1$) depending on whether belongs to the range [0, 0.5] or [-0.5, 0], respectively.

4. Experimental Results and Discussion

The proposed algorithm performance is tested on various satellite imagery from DubaiSat-2. Examples are shown in Fig. 3, where each satellite image size is 1024x1024 pixels. The serial key information is encoded using TPC with identical binary Bose-Chaudhuri-Hocquenghem (BCH) code component. All the results are evaluated using TPC $(31, 16, 7)^2$ that has a correcting capability = 24 bits. The distortion caused to the satellite imagery was assessed by

using the PSNR in the spatial domain, WSNR in wavelet domain and the structural similarity index measurement (SSIM).

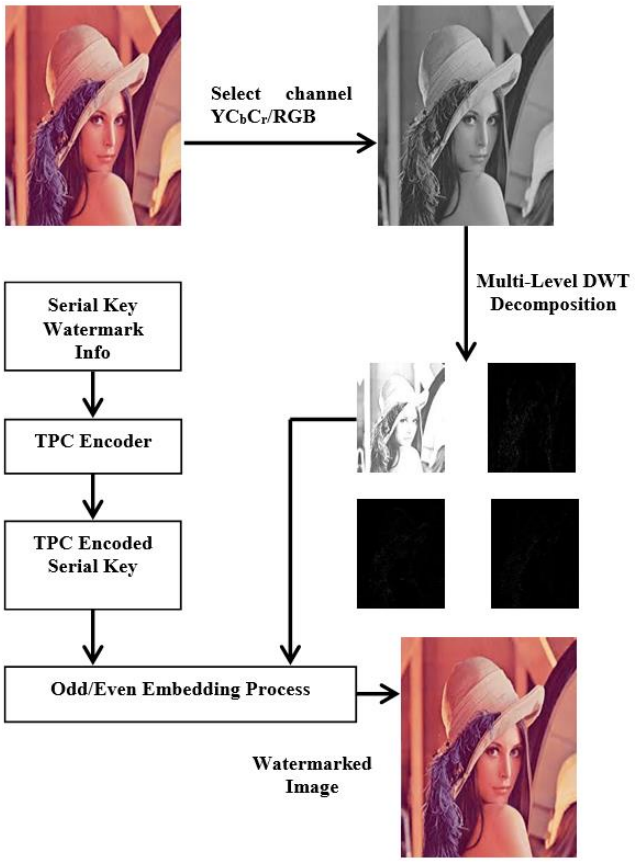


Fig. 2 Proposed Algorithm

Algorithm 1 Proposed Ownership Protection of Satellite Imagery

Initialize

Wavelet type and scaling factor, **Δ**

Inputs

1: Satellite imagery;
2: Serial key information.

Output

1: Ownership protected Satellite imagery.
1: procedure OWNERSHIP PROTECTED SATELLITE IMAGERY
2: Insert the serial key information;
3: Add checksum digits to the serial key information;
4: Reshape and Duplicate binary formatted data I multiple times to get ($k_1 x\ k_2$) bits data;
5: Apply TPC encoding to convert ($k_1 \times k_2$) bits data to ($n_1 \times n_2$) bits TPC encoded data;
6: Select a suitable channel of satellite imagery as RGB model G channel, YC_bC_r model Y
channel, or gray channel;
7: Find M multi-level DWT of the selected channel of satellite imagery,

$[LL_1, LH_1, HL_1, HH_1] = \text{DWT}[C_k]$
$[LL_2, LH_2, HL_2, HH_2] = \text{DWT}[LL_1]$
1.1.1 ⋮

$[LL_M, LH_M, HL_M, HH_M] = \text{DWT}[LL_{M-1}]$,
where C_k indicates the selected channel of satellite imagery.
8: Embed HIHO-TPC encoded ownership information bits;
9: **if** $C(x, y) = 0$ **then**,

$$LL_2(x,y) = \begin{cases} \Delta Q_e\left(\dfrac{LL_2(x,y)}{\Delta}\right), \\ LL_2(x,y) \end{cases}$$

where Q_e represents even quantization to the nearest integer number, $1 < x < n_1$ and $1 < y < n_2$.

10: **else**

$$LL_2(x,y) = \begin{cases} \Delta Q_o\left(\dfrac{LL_2(x,y)}{\Delta}\right), \\ LL_2(x,y) \end{cases}$$

where Q_o represents odd quantization to the nearest integer number.

11: **end if**
12: **end procedure**

Table 1 shows the PSNR performance of the watermarked satellite images under various scenarios such as watermark information embedded in the RGB model, YC_bC_r model, and grayscale model, as well as satellite images under different watermark strength scaling factors, Δ. From Table 1 it has been noticed that as the watermark strength scaling factor increases, the PSNR start decreasing. For example, when Δ = 8, the PSNR is in the range 48dB to 49dB, while when Δ = 16, the PSNR is in the range of 43dB to 43.5dB. From Table 1 it has been noticed that RGB model gives better PSNR performance compared to YC_bC_r model watermarked Satellite images. Similarly, Table 2 shows SSIM performance of the RGB model, YC_bC_r model and grayscale model satellite images under different watermark strength scaling factors. From Table 2, it has been noticed that RGB model gives SSIM value as compared to YC_bC_r model and grayscale model. For example, the SSIM values for RGB model is 0.9963, 0.9796 for YC_bC_r model and 0.9875 for grayscale model for Sat1 image, when Δ = 8. Also from Table 2, it has been noticed that as the watermark strength scaling factor increases, the SSIM start decreasing. For example, for Sat1 image when Δ = 8, the SSIM value is 0.9963 and 0.9862 when Δ = 16.

Table 3 shows the WSNR performance of RGB model watermarked satellite images under different watermark strength scaling factors such as 8, 12, 16, 20 and 24.

Table 1: PSNR (dB) analysis of watermarked satellite imagery

	RGB		YC_bC_r		Gray	
	Δ = 8	Δ = 16	Δ = 8	Δ = 16	Δ = 8	Δ = 16
Sat1	48.856	43.033	42.263	36.825	44.045	38.245
Sat2	48.814	43.142	42.302	36.936	44.036	38.365
Sat3	48.901	43.152	42.321	37.011	44.036	38.316
Sat4	48.782	43.018	42.278	36.780	43.989	38.294
Sat5	48.745	43.061	42.215	36.841	43.986	38.276
Sat6	48.878	43.136	42.293	36.952	44.097	38.363
Sat7	48.753	43.074	42.212	36.846	43.968	38.343
Sat8	48.874	43.162	42.276	36.953	44.034	38.406

It can be noticed from Table 3 that as the watermark strength scaling factor increases, the WSNR start decreasing. For example, when Δ = 8, the WSNR is in the range 51dB to 51.5dB, while when Δ =24, the WSNR was in the range 41.5dB to 42.5dB.

Table 2: SSIM analysis of watermarked satellite imagery

	RGB		YC_bC_r		Gray	
	Δ = 8	Δ = 16	Δ = 8	Δ = 16	Δ = 8	Δ = 16
Sat1	0.9963	0.9892	0.9796	0.9484	0.9875	0.9636
Sat2	0.9996	0.9986	0.9984	0.9947	0.9988	0.9961
Sat3	0.9995	0.9980	0.9970	0.9907	0.9982	0.9935
Sat4	0.9985	0.9949	0.9909	0.9735	0.9963	0.9863
Sat5	0.9993	0.9975	0.9971	0.9897	0.9978	0.9922
Sat6	0.9995	0.9983	0.9979	0.9927	0.9985	0.9944
Sat7	0.9981	0.9935	0.9928	0.9746	0.9945	0.9811
Sat8	0.9998	0.9994	0.9993	0.9975	0.9995	0.9982

Similarly, Table 4 shows the WSNR performance of YC_bC_r model watermarked satellite images under various watermark strength scaling factors. From Table 3 and 4, it has been noticed that RGB model watermarked satellite images gives better Wavelet WSNR values compared to YC_bC_r model watermarked satellite images. Table 5 shows the WSNR performance of grayscale model watermarked satellite images under various watermark strength scaling factors and it is shown that as the watermarking strength scaling factor increases the WSNR start decreases. Also, it is noticed that the grayscale model gives better performance compared to YC_bC_r model watermarked images.

Table 3: WSNR (dB) analysis of RGB watermarked satellite imagery

	Δ = 8	Δ = 12	Δ = 16	Δ = 20	Δ = 24
Sat1	51.073	47.679	45.088	43.277	41.552
Sat2	51.127	47.906	45.464	43.502	42.019
Sat3	51.277	47.970	45.429	43.565	42.025
Sat4	51.076	47.741	45.220	43.309	41.725
Sat5	50.976	47.773	45.317	43.363	41.838
Sat6	51.237	47.950	45.431	43.547	41.978
Sat7	51.014	47.696	45.250	43.158	41.384
Sat8	51.265	47.960	45.478	43.575	42.049

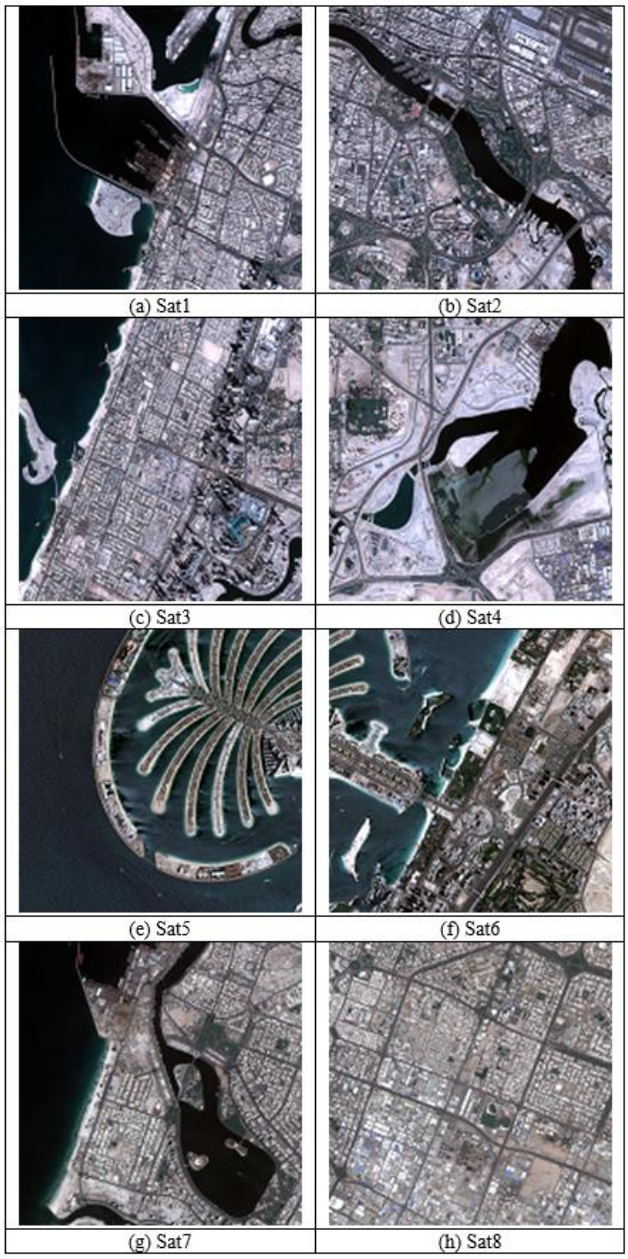


Fig. 3 Evaluated satellite images

JPEG compression techniques are used to reduce the size of an image file for more efficient storage and cut down the cost of bandwidth required for image transmission application. So it is very important to analyze the performance of proposed watermarking algorithms under various levels of JPEG compression of watermarked host images. As the JPEG compression rate increases, the quality of watermarked image starts to decrease. Hence, the watermark will be destroyed and become indiscernible. Fig. 4 (a) shows the extracted watermarked serial key count performance under JPEG compression attack for

different watermark strength scaling factors from the RGB model, Green channel, of Sat1 image; while Fig. 4 (b) shows the extracted watermarked serial key count from the YC_bC_r model, Y channel, for the same image. Similarly, Fig. 4 (c) shows the extracted watermarked serial key count under JPEG compression attack for different watermark strength scaling factors the grayscale version model. From Fig. 4 (a), 4 (b), and 4 (c) it is clear that under JPEG compression attack, YC_bC_r model gives better performance as compared to RGB model and grayscale model. It is also noticed that as watermark strength scaling factor increases, the extracted watermarked serial key count starts increasing for watermarked image Sat1 under JPEG compression attack.

Table 4: WSNR (dB) analysis of YC_bC_r watermarked satellite imagery

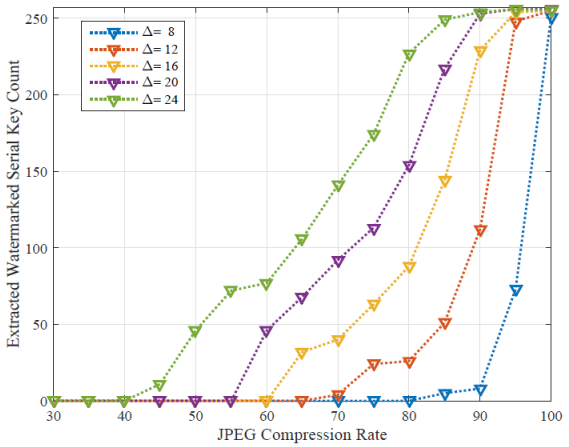
	Δ = 8	Δ = 12	Δ = 16	Δ = 20	Δ = 24
Sat1	44.963	41.911	39.018	37.206	35.819
Sat2	45.240	41.984	39.494	37.591	36.004
Sat3	45.213	42.048	39.575	37.599	36.175
Sat4	45.131	41.824	39.174	37.600	36.107
Sat5	45.061	41.837	39.333	37.445	35.887
Sat6	45.219	42.009	39.514	37.698	36.105
Sat7	45.039	41.737	39.174	37.464	35.867
Sat8	45.270	42.051	39.583	37.783	36.140

Table 5: WSNR (dB) analysis of gray watermarked satellite imagery

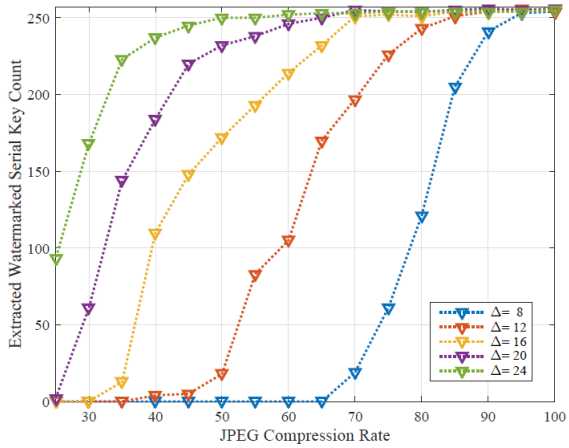
	Δ = 8	Δ = 12	Δ = 16	Δ = 20	Δ = 24
Sat1	46.372	42.909	40.436	38.488	37.206
Sat2	46.512	43.264	40.804	38.900	37.360
Sat3	46.498	43.340	40.700	38.963	37.279
Sat4	46.439	43.180	40.659	38.617	37.051
Sat5	46.424	43.137	40.684	38.795	37.220
Sat6	46.609	43.275	40.780	38.919	37.370
Sat7	46.405	43.129	40.645	38.458	36.726
Sat8	46.543	43.249	40.900	39.023	37.477

Fig. 5 shows the extracted serial key performance comparison of RGB model, YC_bC_r model, and grayscale model watermarked satellite image Sat1 under JPEG compression attack when watermarking Strength scaling factor, Δ, is 16. From Fig. 4, it has been noticed that under JPEG compression attack, YC_bC_r model gives better performance compared to RGB model and grayscale model.

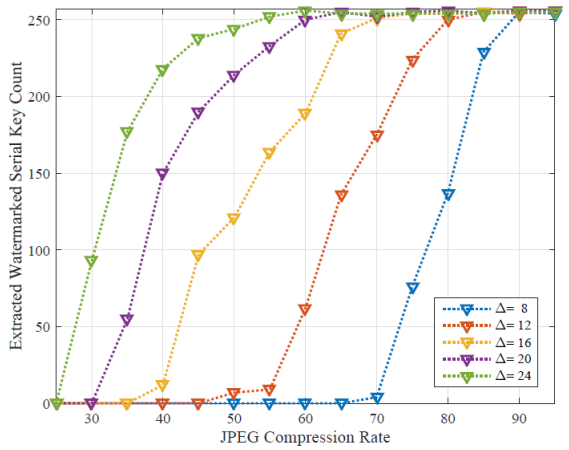
Image cropping is the process of removal of some outer parts of an image. In general, the attacker could try to remove the watermark information by cutting some parts of the watermarked image.



(a) JPEG attack using green channel in RGB model



(b) JPEG attack using Y channel in YC_bC_r model



(c) JPEG attack using grayscale image

Fig. 4 Performance analysis of Sat1 under JPEG attack

The performance of recovered watermark information from a watermarked cover image under a various level of cropping attack should be assessed. Robustness of watermarking against cropping attack depends on the

method of watermarking and redundancy of the watermark information.

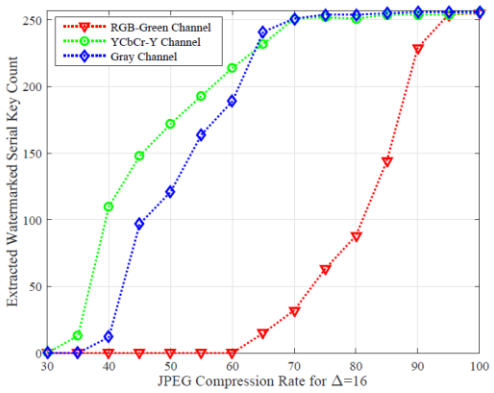


Fig. 5 Performance analysis of Sat1 under JPEG attack using different image models

Fig. 6 shows the extracted serial key count performance under cropping attacks for Green channel RGB model, Y channel YC_bC_r, and grayscale model of watermarked satellite image Sat1 under different watermark strength scaling factors. From Fig. 6, it is concluded that under cropping attack, all the three models give same performance and the extracted serial key count remain same under different watermark strength scaling factors.

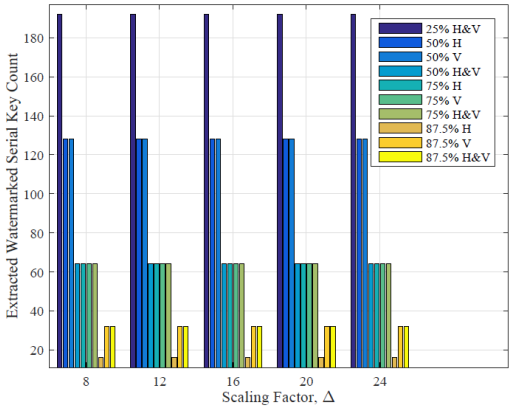
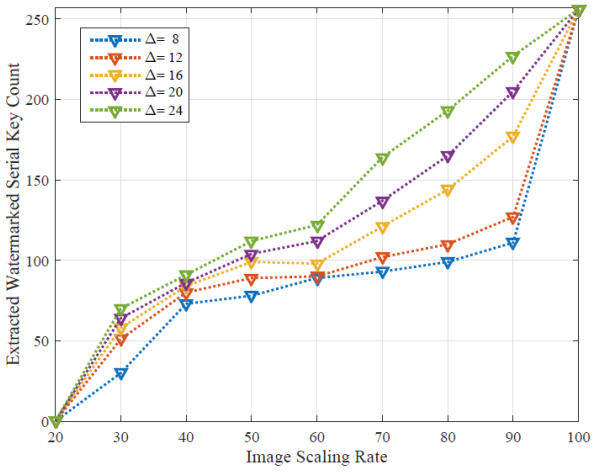
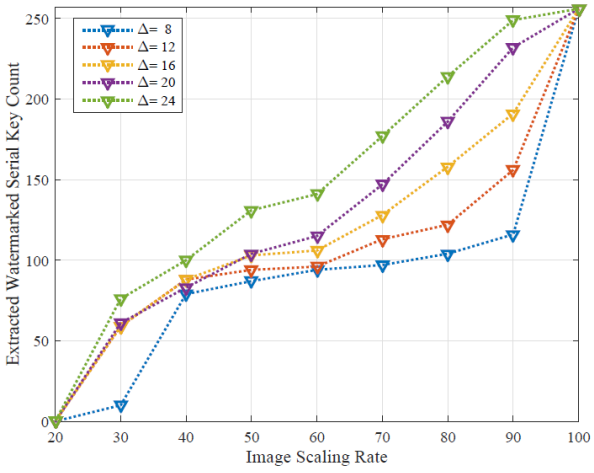


Fig. 6 Performance analysis of Sat1 under cropping attack

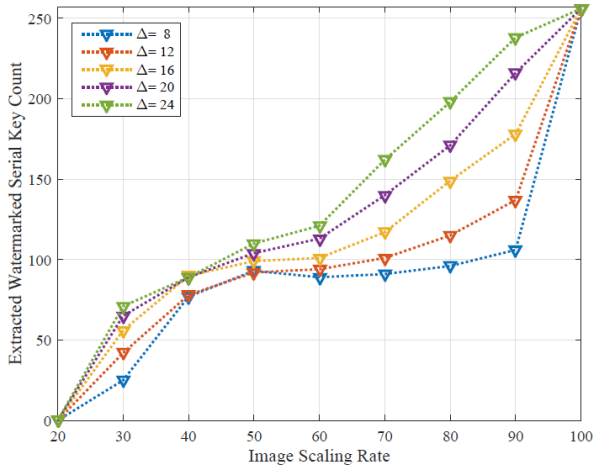
Image scaling is the process of resizing a digital image. Image scaling is a non-trivial process that involves a trade-off between efficiency, smoothness, and sharpness. Since scaling attack does not actually remove the embedded watermark itself, but aims to change the synchronization of the embedded watermark information, the accurate detection of watermark information under scaling attack is a difficult task. The detector can extract the watermark information only when perfect synchronization is regained. To extract the watermark information, the attacked image must be restored to its original resolution.



(a) Resizing attack using green channel in RGB model



(b) Resizing attack using Y channel in YC_bC_r model



(c) Resizing attack using grayscale image

Fig. 7 Performance analysis of Sat1 under resizing attack

Fig. 7 (a) shows the extracted watermarked serial key count performance under resizing attack for different watermark strength scaling factors for RGB model, Green channel, of satellite image Sat1; while Fig. 7 (b) shows the same results for the YC_bC_r model, Y channel. Moreover, Fig. 7 (c) shows the shows the results for the grayscale of Sat1. From Fig. 7 (a), 7 (b), and 7 (c) it has been noticed that under resizing attack, the extracted serial key count depends on the value of watermark strength scaling factor. As watermark strength scaling factor increases, the possibility of extracting the serial key count also increases. Fig. 8 shows the extracted watermarked serial key performance comparison for Sat1 under resizing attack for RGB, YC_bC_r, and grayscale model. From Fig. 7, it can be noticed that under resizing attack, YC_bC_r model gives slightly better performance compared to RGB and grayscale model.

Image filtering allows various effects on the watermarked images. The robustness of the watermarking techniques needs to be tested against various filter attacks like average filters, median filters, and sharpening filters. In general, the watermarked images can be recognizable when undergoing lower mask size filtering attacks, but as mask size increases it might spoil the quality of the watermarked image which by turn would spoil the watermark information. Fig. 9 shows the performance analysis of Sat1 image under filtering attack. It can be clearly seen that the grayscale model image outperforms RGB and YC_bC_r models in different scale factors such as 8, 12, and 20. This demonstrates the strong robustness of grayscale model image in the proposed embedding algorithm that goes under filtering attack.

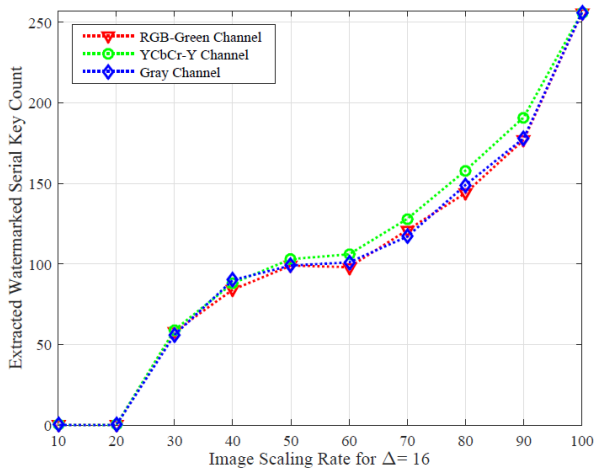


Fig. 8 Performance analysis of Sat1 under resizing attack

Geometric attacks like rotation attack is a fundamental issue in digital watermark system design. Watermark's resistance to geometric attacks that is, its ability to withstand an arbitrary displacement of all or some of its pixels by a random amount. Every geometric attack is defined by a set of parameters that determines the operation performed over the target image. The rotation operation perform a geometric transform which maps the pixel position (x_1 , y_1) of the original image into a position (x_2 , y_2) in an output image by rotating image through a specific angle θ about an origin 0. Fig. 10 (a), 10 (b), and 10 (c) shows the extracted serial key count under geometrical rotation attack for Green channel RGB model, Y channel YC_bC_r model and grayscale model of watermarked satellite image Sat1, respectively under geometric attack. It is also noticed that under geometric attack, as the watermark strength scaling factor increases, the robustness of extracting the serial key count starts to increase.

Fig. 11 shows the performance analysis of Sat1 image under geometrical rotation attack. It can be clearly seen that the extracted watermarked serial key count becomes less than 90 when the rotation is more than 15°. However, the probability of rotating the image more than 15° is very low. Based on our result analyses, we have concluded that YCbCr model gives better performance under JPEG compression attack; resizing attack and geometrical rotation attack as compared to RGB model and grayscale model. But under cropping attack, all models give same performance. Finally, we concluded that extracted serial count depends on the watermark strength scaling factors for all attacks mentioned above except cropping attack.

The performance of the developed turbo product code based watermarking algorithm using discrete wavelet transform has been compared to other algorithms mentioned in literature survey such as watermarking using Reed-Solomon code, BCH code and Walsh code respectively. It can be clearly seen that the developed algorithm gives better performance under geometrical attacks

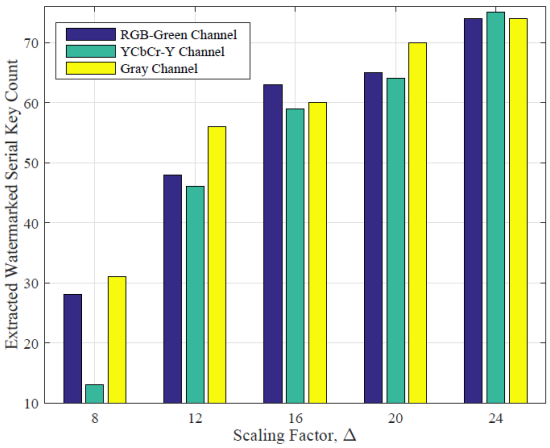
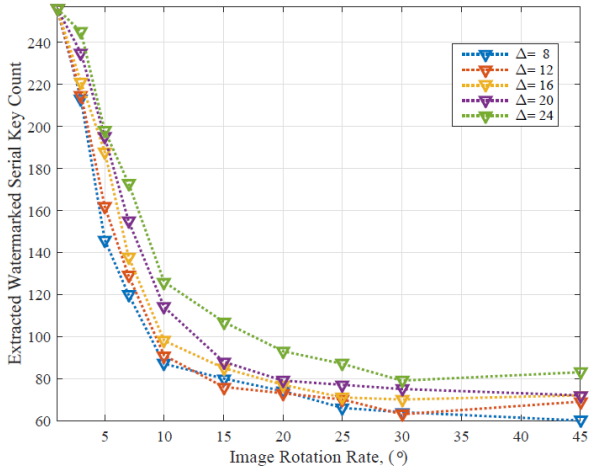
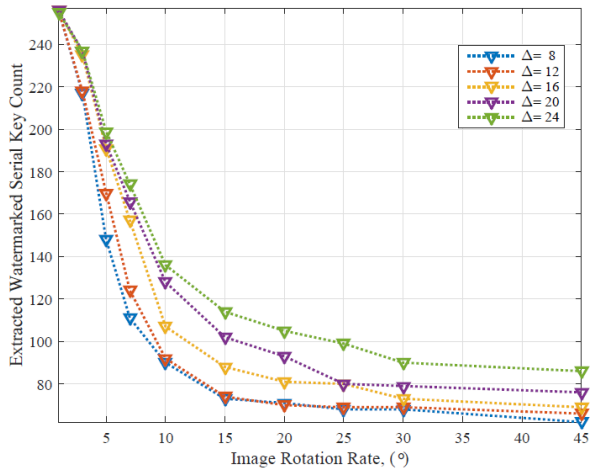


Fig. 9 Performance analysis of Sat1 under filter attack

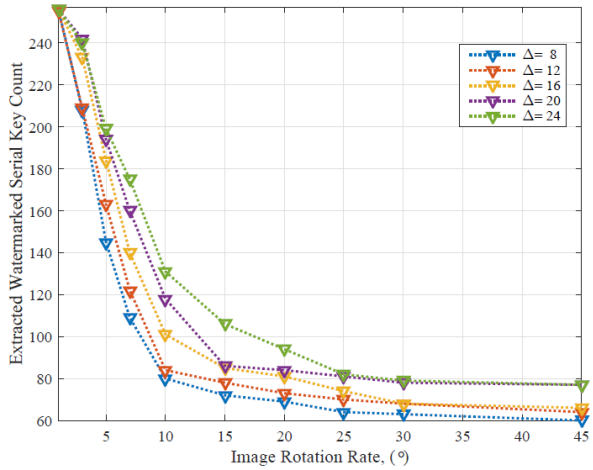
Table 6 shows the PSNR and SSIM comparison of the developed watermarking algorithms and other algorithms mentioned in literature survey.



(a) Geometrical rotation attack using green channel in RGB model



(b) Geometrical rotation attack using Y channel in YC_bC_r model



(c) Geometrical rotation attack using grayscale image

Fig. 10 Performance analysis of Sat1 under geometrical rotation attack

The developed turbo product code based watermarking algorithm gives better robustness performance under image scaling attack, image cropping attack, image geometrical rotation attack as compared to the BCH code, Reed-Solomon code and Walsh code based watermarking algorithms and the embedded watermark serial-key information can be extracted from up to 35 degrees rotated cover images. Moreover, the developed watermarking algorithm satisfies the major watermark requirements and can be implemented in few seconds. Furthermore, the developed turbo product code encoded watermarking algorithms using the discrete wavelet transform will reduce the watermarking process computation complexity. It is noticed from the experiment that the wavelet transform based multi watermarking algorithms are faster. The MATLAB execution time required for developed turbo product code encoded watermarking algorithms, under various scenarios, are shown in Table 7.

Table 6: Comparison between TPC algorithm and others

Algorithm	Domain	Δ	PSNR(dB)	SSIM
Reed-Solomon Code [23]	DCT	16	42.68	0.9815
BCH Code [24]	DCT	16	42.60	0.9800
Walsh Code [25]	DCT	16	37.50	0.9395
TPC Code in RGB	DWT	16	43.07	0.9936
TPC Code in YC_bC_r	DWT	16	36.85	0.9746

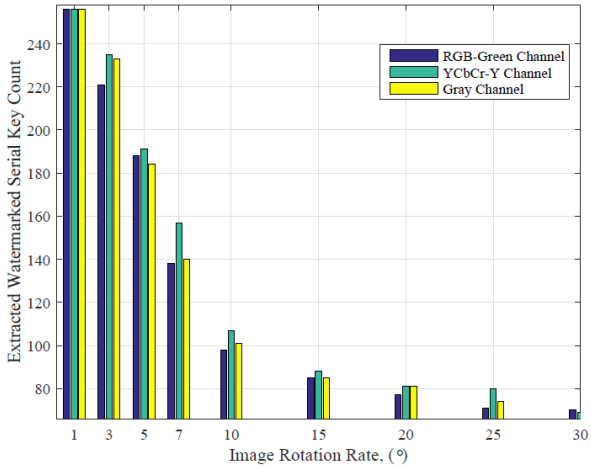


Fig. 11 Performance analysis of Sat1 under geometrical rotation attacks

Table 7: MATLAB execution time for TPC algorithm

Intel® Core i7, 64 bit OS, 3.4 GHz, RAM=8 GB	
Watermarking Scenarios	Processing Time
Serial-key watermark in Gray Sat1	8.45 seconds
Serial-key watermark in RGB colour Sat1	8.48 seconds
Serial-key watermark in YCbCr colour Sat1	15.69 seconds

5. Conclusion

This paper presents a novel blind digital watermarking technique for the ownership protection of satellites imagery. The distortions introduced to the satellite imagery are analyzed using the PSNR, WSNR, and SSIM. The performances of the developed ownership protection algorithm have been successfully tested on a variety of 1024x1024 pixel, 24-bit color satellite images, captured by DubaiSat-2 and their grayscale version. The ownership protection algorithm is implemented by embedding the TPC encoded ownership information into satellite images in the wavelet domain, which increases the security and robustness of the ownership information. Experimental results show that the proposed algorithm gives an acceptable performance with a strong robustness of watermark information for many intentional and non-intentional attacks. Also, the proposed watermarking algorithms satisfy the major watermark requirements and can be implemented in few seconds.

References

[1] H. Miyazaki, X. Shao, K. Iwao, et al., "An automated method for global urban area mapping by integrating aster satellite images and gis data," IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing 6, 1004–1019 (2013).

[2] C. M. Gevaert, J. Suomalainen, J. Tang, et al., "Generation of spectral-temporal response surfaces by combining multispectral satellite and hyperspectral uav imagery for precision agriculture applications," IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing 8, 3140–3146 (2015).

[3] 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).

[4] 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).

[5] 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).

[6] 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).

[7] Q. A. Kester, L. Nana, and A. C. Pascu, "A novel cryptographic encryption technique of video images using quantum cryptography for satellite communications," in 2013 International Conference on Adaptive Science and Technology, 1–6 (2013).

[8] B. Li, M. Wang, X. Li, et al., "A strategy of clustering modification directions in spatial image steganography," IEEE Transactions on Information Forensics and Security 10, 1905–1917 (2015).

[9] S. Ahani and S. Ghaemmaghami, "Colour image steganography method based on sparse representation," IET Image Processing 9(6), 496–505 (2015).

[10] F. Y. Shih, Digital Watermarking and Steganography: Fundamentals and Techniques, CRC Press, Inc., Boca Raton, FL, USA, 1st ed. (2007).

[11] M. Barni and F. Bartolini, Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications, CRC Press, Inc., New York, NY, USA, 1st ed. (2004).

[12] L. Liu and X. Li, "Watermarking protocol for broadcast monitoring," in 2010 International Conference on E-Business and E-Government, 1634–1637 (2010).

[13] A. Mehto and N. Mehra, "Article: Techniques of digital image watermarking: A review," International Journal of Computer Applications 128, 21–33 (2015). Published by Foundation of Computer Science (FCS), NY, USA.

[14] I. G. Karybali and K. Berberidis, "Efficient spatial image watermarking via new perceptual masking and blind detection schemes," IEEE Transactions on Information Forensics and Security 1, 256–274 (2006).

[15] S. Xiang, H. J. Kim, and J. Huang, "Invariant image watermarking based on statistical features in the low-frequency domain," IEEE Transactions on Circuits and Systems for Video Technology 18, 777–790 (2008).

[16] T. Pardhu and B. R. Perli, "Digital image watermarking in frequency domain," in 2016 International Conference on Communication and Signal Processing (ICCSP), 0208–0211 (2016).

[17] T. R. Van, "Electronic water mark," (1993).

[18] S. Rohith, K. N. H. Bhat, and B. K. Sujatha, "A secure and robust digital image watermarking scheme using repetition codes for copyright protection," in 2014 International Conference on Advances in Electronics Computers and Communications, 1–8 (2014).

[19] C. Nafornita, A. Isar, and M. Kovaci, "Increasing watermarking robustness using turbo codes," in 2009 IEEE International Symposium on Intelligent Signal Processing, 113–118 (2009).

[20] F. P.-G. Felix P. Balado, "Coding at the sample level for data hiding: turbo and concatenated codes," (2001).

[21] C. Nafornita, A. Isar, and M. Kovaci, "Increasing watermarking robustness using turbo codes," in 2009 IEEE International Symposium on Intelligent Signal Processing, 113–118 (2009).

[22] S. A. AlMaeeni, F. Kalbat, and H. Al-Ahmad, "Logo embedding in grayscale images using turbo product codes," in 2015 International Conference on Information and Communication Technology Research (ICTRC), 96–99 (2015).

[23] J. S. Y. Jeedella, H. A. Ahmad, and O. A. Shehhi, "Watermarking mobile phone colour images with aeed solomon error correction code," in 2012 16th IEEE Mediterranean Electrotechnical Conference, 375–378 (2012).

[24] 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).
[25] 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).
[26] M. Andalibi and D. M. Chandler, "Digital image watermarking via adaptive logo texturization," IEEE Transactions on Image Processing 24, 5060–5073 (2015).
[27] B. Chen and G.W.Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," IEEE Transactions on Information Theory 47, 1423–1443 (2001).
[28] B. Mathon, F. Cayre, P. Bas, et al., "Optimal transport for secure spread-spectrum watermarking of still images," IEEE Transactions on Image Processing 23, 1694–1705 (2014).
[29] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near shannon limit error-correcting coding and decoding: Turbo-codes. 1," in Communications, 1993. ICC '93 Geneva. Technical Program, Conference Record, IEEE International Conference on, 2, 1064–1070 vol.2 (1993).
[30] C. Berrou and A. Glavieux, "Near optimum error correcting coding and decoding: turbocodes," IEEE Transactions on Communications 44, 1261–1271 (1996).
[31] C. E. Shannon, "A mathematical theory of communication," SIGMOBILE Mob. Comput. Commun. Rev. 5, 3–55 (2001).
[32] "Unapproved draft ieee standard for local and metropolitan area networks corrigendum to ieee standard for local and metropolitan area networks - part 16: Air interface for fixed broadband wireless access systems," IEEE Std P802.16-2004/Cor1/D5, 2005 (2005).
[33] J. Proakis, Digital Communications, Electrical engineering series, McGraw-Hill (2001).
[34] S. A. A. Muaini, A. J. Al-Dweik, and M. A. Al-Qutayri, "Ber performance of non-sequential turbo product codes over wireless channels," in 2011 IEEE GCC Conference and Exhibition (GCC), 93–96 (2011).
[35] R. C. Gonzalez and R. E.Woods, Digital Image Processing (3rd Edition), Prentice-Hall, Inc., Upper Saddle River, NJ, USA (2006).

Sara AlMaeeni received PhD degree from Khalifa University in 2016 in communications engineering. For the PhD dissertation, she contributed with a novel mathematical frameworks for the bit error rate in cooperative communications. She is currently working as expert in space communications in Mohammed bin Rashid Space Centre. She is a member of different technical committees like IET communications, IEEE global communications conference, CommNet conference, and international conference on advanced Communication systems and information security. Her research interests are the satellite communications, channel coding, cooperative communications, and image processing.

Alavikunhu Panthakkan is a dynamic research scientist in electronics engineering and image signal processing. 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 bachelor degree (B.Tech) in electronics and communication engineering, master degree (M.Tech) in electronics engineering and Ph.D. in electronics engineering from India. He has 4 years industrial experience and 7 years of teaching/research experience. He has published more than 20 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).

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 conferences such as such as IEEE EDUCON 2016, ICCSPA 2015, Global Education 2013-2014, BCS IITC 2013-2014, IEEE ICECS 2013, ICCSPA 2013, ICTIST 2011, DeSE 2011, CTIT 2011, and IEEE GCC 2011. 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.