International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-4 Number-2 Issue-15 June-2014

Satellite Image Security Improvement by Combining DWT-DCT Watermarking and AES Encryption

Naida.H.Nazmudeen[1] , Farsana.F.J[2]

Abstract

With the large-scale research in space sciences and technologies, there is a great demand of satellite image security system for providing secure storage and transmission of satellite images. As the demand to protect the sensitive and valuable data from satellites has increased and hence proposed a new method for satellite image security by combining DWT-DCT watermarking and AES encryption. Watermarking techniques developed for multimedia data cannot be directly applied to the satellite images because here the analytic integrity of the data, rather than perceptual quality, is of primary importance. To improve performance, combine discrete wavelet transform (DWT) with another equally powerful transform; the discrete cosine transform (DCT). The combined DWT-DCT watermarking algorithm's imperceptibility was better than the performance of the DWT approach. Modified decision based unsymmetrical trimmed median filter (MDBUTMF) algorithm is proposed for the restoration of satellite images that are highly corrupted by salt and pepper noise. Satellite images desire not only the watermarking for copyright protection but also encryption during storage and transmission for preventing information leakage. Hence this paper investigates the security and performance level of joint DWT-DCT watermarking and Advanced Encryption Standard (AES) for satellite imagery. Theoretical analysis can be done by calculating PSNR and MSE. The experimental results demonstrate the efficiency of the proposed scheme, which fulfils the strict requirements concerning alterations of satellite images.

Keywords

Watermarking, DWT, DCT, AES encryption, Satellite images, MDBUTMF algorithm, PSNR and MSE.

Manuscript received June 18, 2014.

Naida. H. Nazmudeen, Electronics and Communication, Muslim Association College of Engineering, Venjaramoodu, Kerala, India.

Farsana. F. J, Electronics and Communication, Muslim Association College of Engineering, Venjaramoodu, Kerala, India.

1. Introduction

There is a great demand of satellite imagery security system, with the large-scale research and development in space sciences and technologies, for providing secure storage and transmission of satellite imagery over internet. This brings new challenges to protect sensitive satellite imagery from unauthorized access in order to keep the storage and transmission process secure [1]. Watermarking can be used for copyright protection of satellite images. Digital watermarking for satellite imagery is the method of embedding information into the digital imagery which can be used to verify the authenticity of its owners. The embedded information can be image chip, trademark, or any kind of information generated from the original images.

Secure communication is when two parties are communicating and do not want a third party to listen in. For that they need to communicate in a way not susceptible to interception. Secure communication means method by which people can share information with varying certainty that third parties cannot intercept what was said. Watermarking techniques developed for multimedia data cannot be directly applied to the satellite images because the analytic integrity of the data, rather than perceptual quality, is of primary importance. Hence satellite images needs efficient watermarking techniques. Satellite image watermarking along with encryption technique can be used for secret satellite communication [2].

This paper presents a new method for satellite image security improvement using DWT-DCT watermarking and AES encryption. Using the proposed method satellite image security can be improved when compared to the previous works. Encryption technique is also used along with watermarking to enhance the secrecy of secret image.

Paper construction is as follows. The literature review is considered in section 2. The proposed method in section 3 includes noise removal; watermark embedding, watermark extraction and AES encryption. Simulation results are shown in section 4. Performance analysis is done in this section. Conclusion is discussed in section 5.

2. Literature Review

Within the field of watermarking, satellite image watermarking particularly has attracted lot of attention in the research community. There are several existing methods for satellite image watermarking. Some are shown below. In 2009 authors named A. Sangeetha and K. Anusudha proposed Digital Watermarking of Satellite Images Using Secured Spread Spectrum Technique [3]. This paper contains spread spectrum watermarking of the satellite images. This can be done by choosing a region of interest (ROI) and embed the watermark in the same. The reason for choosing a ROI is an area which contains main information and can be sent through media without any attacks. A particular region is selected as ROI. The disadvantage of this method is visible watermark and it is used to maliciously trace users of an anonymous communication networks. In detection process get an idea about the watermark signal, can easily change the data.

In 2008 author named Yogesh Chauhan proposed Satellite image watermarking using LSB manipulation algorithm [4]. The simplest spatial-domain watermarking method is to embed watermark in the least significant bits (LSB) of some randomly selected pixels. Disadvantages of this method are the watermark can be destroyed if the image is low-pass filtered, Security level is very less, Least robust. In 2012 authors named C. Chen and P. Hsu proposed Watermarking based on the scale-space feature point [5]. Here proposed a novel algorithm that the digital watermark was embedded into the photogrammetric images, and the robustness of the embedded digital watermark and the impact on photogrammetric image quality are evaluated. Disadvantages are if suffers from the changes of rotation or scaling attack, the pixel sequence changes, results in failure of watermark extraction affects image matching, image classification and image measurements. In 2001 author Anthony Tung Shuen Ho proposed robust copyright protection of satellite images using a novel digital image in image watermarking algorithm [6]. This method uses a number of bits or characters to be embedded into the image. Anyway some of these methods could yield to some small attacks to the watermarked image due to the variation of the values of these characters. Due to this, legal ownership of the data under copyright protection would be questionable.

2.1 Discrete Wavelet Transform (DWT)

The basic idea of discrete wavelet transform (DWT) is multi-differentiated decomposition of the image into sub-images of independent frequency district and different spatial domain. Next transform the coefficients of sub-image. Then, it is decomposed into 4 frequency districts, that is one low-frequency district (LL) and three high-frequency districts (LH,HL,HH). If the information of low-frequency district is DWT transformed, then information of sub-level frequency district is obtained. A two-dimensional image after three-time discrete wavelet transform decomposed can be shown as Fig.1. Where, L shows low-pass filter, H shows high-pass filter. The original image can be decomposed to frequency districts of HL1, LH1, and HH1. The low-frequency information can be decomposed into sub-level frequency district information of LL2, HL2, LH2 and HH2. Hence the original image can be decomposed for n level wavelet transformation. An image can be decomposed into a pyramidal structure, with various band information, low-low frequency band LL, low-high frequency band LH, high-low frequency band HL, high- high frequency band HH [1].

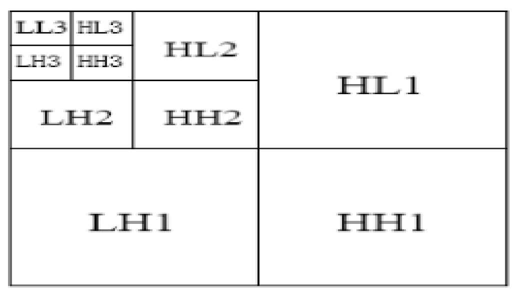

Fig 1: Sketch Map of Image DWT Decomposed

The signal is passed through a series of low pass filters to analyze the low frequencies and through a series of high pass filters to analyze the high frequencies. Filters of different cut-off frequencies are used to analyze the signal at different resolutions. Let us suppose that x[n] is the original signal, spanning a frequency band of 0 to π rad/s. The original signal represented as x[n] is first passed through a high-pass filter g[n] and a low-pass filter h[n]. After the filtering, half of the samples can be eliminated according to the Nyquist rule, since the signal now has the highest frequency of π /2 radians instead of π. The signal hence is sub-sampled by 2, simply by removing every second sample [11]. This represents one level of decomposition and can be mathematically expressed as follows [10]:

$$y_{high}[k] = \sum_n x[k]\, g[2k-n] \qquad (1)$$

$$y_{low}[k] = \sum_n x[k]\, h[2k-n] \qquad (2)$$

Where $y_{high}[k]$ and $y_{low}[k]$ are the outputs of the high-pass and low-pass filters, respectively, after sub-sampling by 2. The synthesis and analysis filters are identical to each other, except for a time reversal. Hence, the reconstruction formula is as shown below [12].

$$x[n] = \sum_n \left(y_{high}[k] g[-n+2k] + y_{low}[k] h[-n+2k] \right) \qquad (3)$$

2.2 Discrete Cosine Transform (DCT)

The DCT transforms a signal from a spatial domain into a frequency domain [2]. Lower frequency are more apparent in an image than higher frequency so if we transform the image into its frequency component and remove a lot of higher frequency coefficients, we can decrease the amount of data needed to describe the image without surrendering too much image quality. The discrete cosine transform (DCT) is closely related to DFT (Discrete Fourier Transform). DCT expresses a sequence of many data points in terms of a sum of cosine functions oscillating at different frequencies. The use of cosine functions rather than sine functions is important in these applications. In case of compression, the cosine functions are more efficient, whereas for differential equations the cosine shows a particular choice of boundary conditions. In particular, a DCT is a Fourier-related transform similar to DFT, but using only real numbers. Cosine Transforms are equivalent to discrete Fourier transforms of twice the length, operating on real data with even symmetry, where in some variants the input and/or output data are shifted by half a sample [14].

3. Proposed method for satellite image security

This paper proposes a method to improve satellite image security by combining DWT-DCT watermarking and AES encryption. Here proposes an algorithm for satellite image watermarking based on Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) [1]. To improve performance, combine discrete wavelet transform (DWT) with another equally powerful transform; the discrete cosine transform (DCT). The combined DWT-DCT watermarking algorithm's imperceptibility was better than the performance of the DWT approach. For watermarking, the preferred colour model must be HSV (Hue, Saturation and Value) rather than RGB because it is the most closely related colour model with Human Visual System [3]. Salt and pepper noise of input colour satellite image can be removed by using MDBUTMF algorithm. Watermarked satellite image is obtained by implementing watermark embedding process. Original satellite image and secret image can be recovered back by using extraction process. The simulation output shows that the watermarked image obtained is invisible.

3.1 Algorithm for noise removal using MDBUTMF algorithm

A modified decision based unsymmetrical trimmed median filter (MDBUTMF) algorithm is proposed here for the restoration of satellite images that are highly corrupted by salt and pepper noise. The proposed algorithm changes the noisy pixel by trimmed median value when other pixel values, 0's and 255's are there in the window and when all the pixel values are 0's and 255's then the noisy pixel is replaced with mean value of the elements present in the window [7]. Flow chart of MDBUTMF is as shown in the figure.

3.2 Algorithm for watermark embedding

- Input color satellite image
- Remove impulse noise by using Modified decision based unsymmetric trimmed median filter (MDBUTMF) algorithm
- Convert RGB image to HSV image [3] and convert HSV to Hue, Saturation and Value components
- Apply DWT on satellite image to decompose into sub-bands LL, HL, LH and HH and apply DCT on HH band
- Select a secret image and perform AES encryption
- Make the size of the encrypted secret image equal to original image
- Apply DWT on secret image and apply DCT on HH band of secret image
- Embedding equation

$$I_w = I + k \times W \qquad (4)$$

I - DCT transformed matrix of satellite image
W - DCT transformed matrix of secret image
k - Embedding strength varies from 0 to 1
I_w - embedded matrix

- Apply inverse DCT to produce HH* and inverse DWT to LL, HL, LH and HH*
- Watermarked (Value) image is obtained. Now concatenate H,S,V back to HSV
- Convert back to RGB satellite image. Obtained watermarked satellite image.

3.3 Algorithm for watermark extraction

- Apply DWT on watermarked satellite image and apply DCT on HH band
- Do AES decryption of secret image and perform DWT on secret image
- Apply DCT on HH band of secret image
- Extraction process

$$I = I_w - k \times W \qquad (5)$$

I_w - DCT transformed matrix of watermarked satellite image
W - DCT transformed matrix of secret image
I - recovered matrix

- Apply inverse DCT to produce HH* and inverse DWT to LL, HL, LH and HH* sub-bands.
- Recover secret image and original satellite image
- Theoretical evaluation - Calculate Mean square error (MSE) and Peak signal to noise ratio (PSNR)

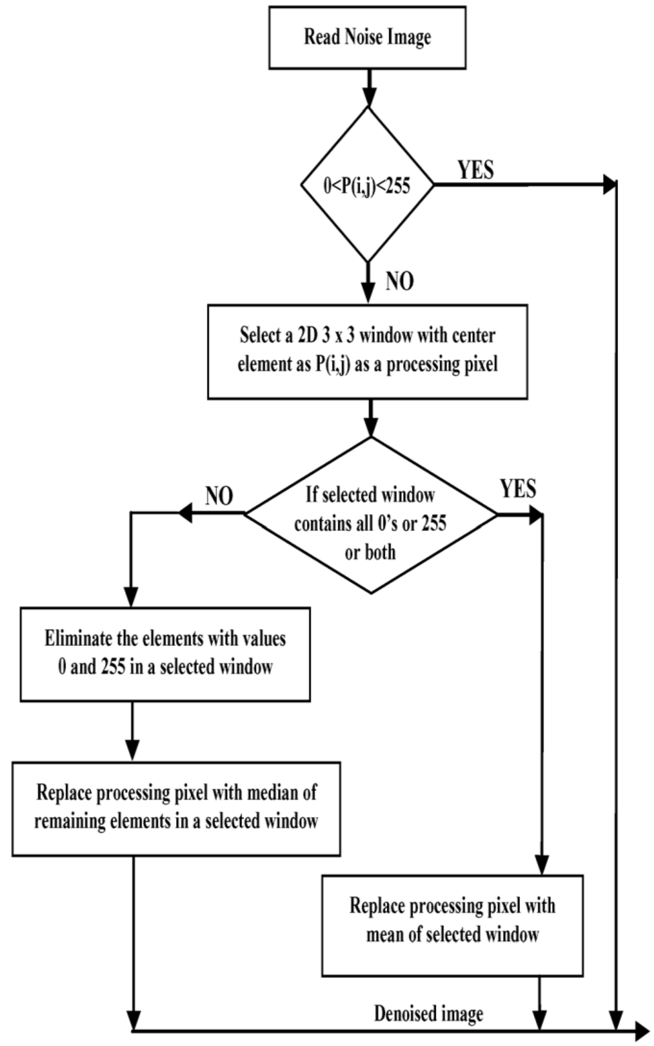

Fig 2: Flow chart of MDBUTMF algorithm

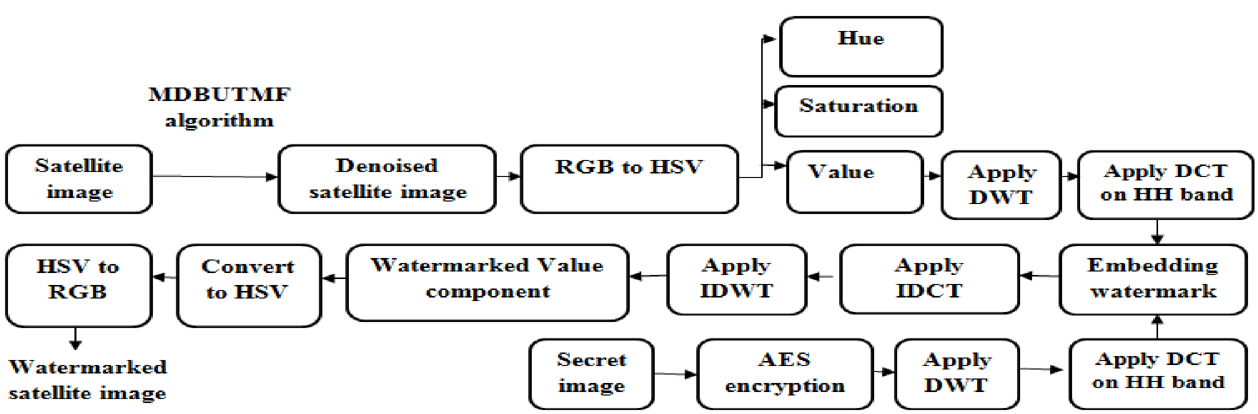

Fig. 3: Watermark embedding

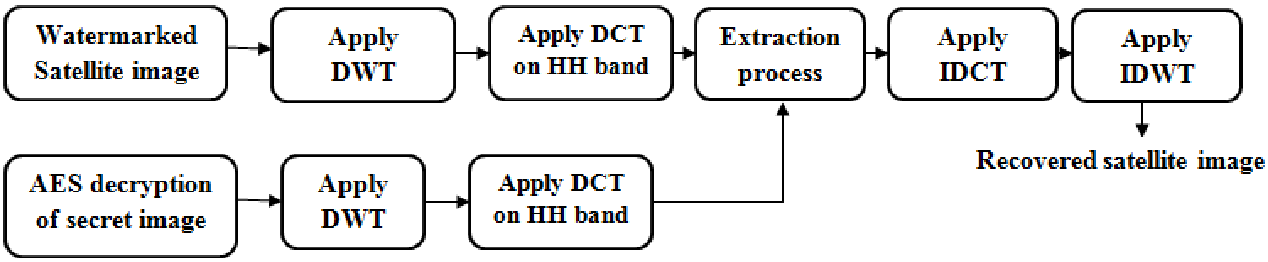

Fig. 4: Watermark extraction

3.4 Theoretical analysis

For theoretical analysis of the proposed algorithm some measures are used for assessment of quality of watermark and image. Image quality is theoretically measured using peak signal to noise ratio (PSNR) and mean square error (MSE) [7]. MSE is calculated pixel-by-pixel by adding up the squared differences of all the pixels and divide it by the total pixel count.

$$MSE = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \left(W_{ij} - W'_{ij}\right)^2 \quad (6)$$

Where m×n is the size of the image, W_{ij} is the original watermark pixel and W'_{ij} is the extracted watermark pixel in i^{th} row and j^{th} column. Lower the value of mean square error smaller the error and better the picture quality. As a measure of the quality of a watermarked image, the PSNR is typically used [11].

$$PSNR = 10 log_{10} \frac{255^2}{MSE} \quad (7)$$

Its unit is db. If PSNR value is greater, the better the watermark conceals.

3.5 Advanced Encryption Standard (AES)

For the protection of satellite images some cryptographic techniques are used. For providing high security Advanced Encryption Standard (AES) is used which is approved by NIST. Advanced Encryption Standard is a block cipher. It is used in various applications since it provides flexibility, simplicity, easiness of implementation and high throughput [8].

This algorithm is a symmetric-key cipher, where both the receiver and sender use a single key for encryption and decryption. The data length is fixed to be 128 bits, while the key size may be 128, 192, or 256 bits, respectively. AES algorithm is an iterative algorithm. Each iteration is called a round, and the total number of rounds is 10, 12, or 14, when the key length is 128, 192, or 256 bits, respectively. The 128-bit data can be divided into sixteen bytes. These bytes are mapped to a 4×4 array named as the State, and all the internal operations of AES are performed on the State. Each round, except the final round, consists of 4 transformations: Sub-Bytes, Mix-Columns, Shift-Rows and Add-Round-Key. Mix-Columns transformation does not present in final round. The decryption steps are simply the reverse of the encryption steps and each operation is the inverse of the corresponding operation in the encryption process [8].

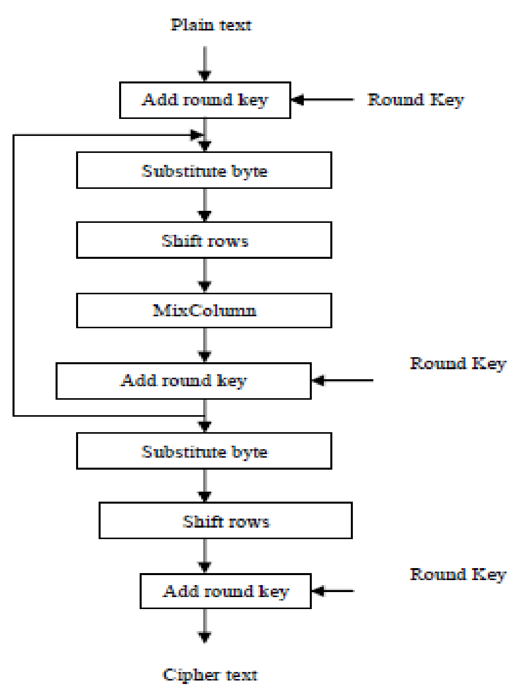

Fig. 5: AES encryption

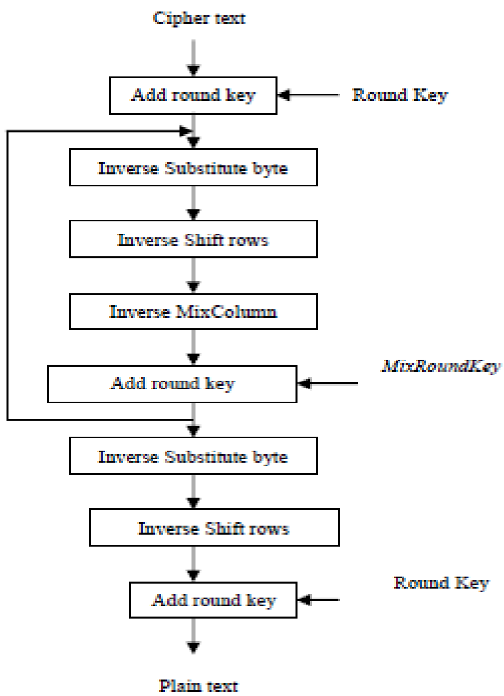

Fig. 6: AES decryption

4. Simulation results

Input noisy colour satellite image. A modified decision based unsymmetrical trimmed median filter (MDBUTMF) algorithm is used for the removal of salt and pepper noise. Convert denoised RGB satellite image to HSV image. Convert HSV image to Hue (H), Saturation(S) and Value (V) components. Next select a secret image (watermark image).

Make the size of this secret image equal to that of the original satellite image. Do AES encryption of secret image. Do watermark embedding process. Watermarked satellite image (Value component) is obtained. Concatenate Hue, Saturation and Value components back to watermarked HSV image. Convert this HSV satellite image back to RGB satellite image. Watermarked satellite image was obtained.

Do inverse operations for discrete cosine transform (DCT) and discrete wavelet transforms (DWT) [9]. Perform AES decryption of satellite image. Recover secret image and original satellite image back. Do theoretical evaluation by calculating Mean square error (MSE) and Peak signal to noise ratio (PSNR). Image quality is theoretically measured using peak signal to noise ratio (PSNR) and mean square error (MSE).Values of MSE and PSNR using the proposed method is as shown in the table.

Fig.7: (a) Noisy image (b) Denoised image

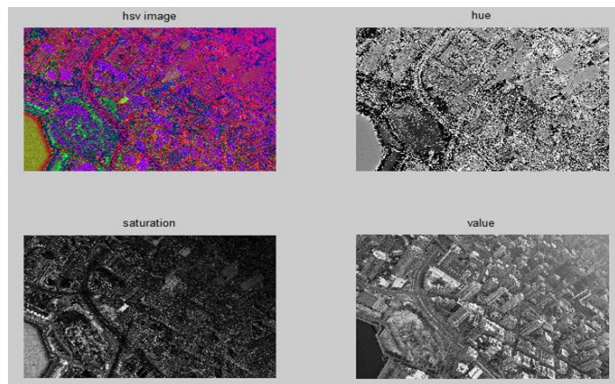

Fig.8: HSV images

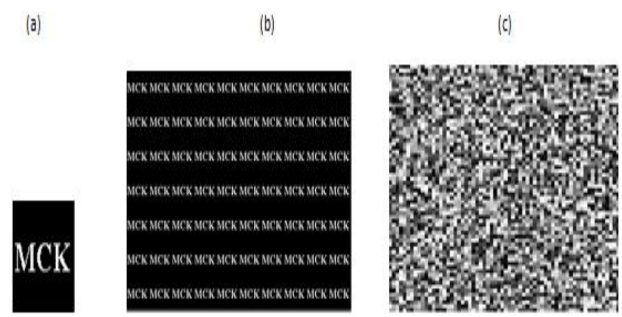

Fig.9: (a) Secret image, (b) Resized secret image (c) Encrypted secret image

Compare PSNR values of watermarking using DWT alone and by using the combination of DWT and DCT. Compare MSE values of watermarking using DWT alone and by using the combination of DWT and DCT. Processing time required is very less. Processing time required is 0.87 seconds.

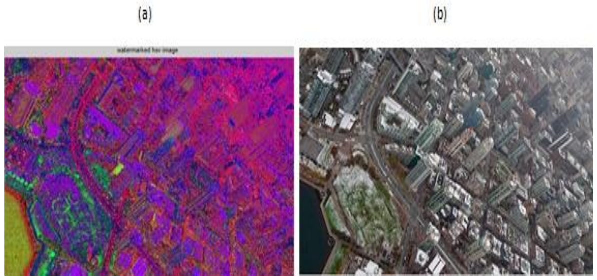

Fig.10: (a) Watermarked HSV image (b) Watermarked RGB images

Table 1: Values of MSE and PSNR

Images	PSNR in dB (DWT)	PSNR in dB (DWT and DCT)	MSE (DWT)	MSE (DWT and DCT)
1	54.587	65.718	0.226	0.014
2	49.1492	60.2774	0.7910	0.0610
3	51.6985	62.8290	0.4398	0.0339
4	49.9267	61.0418	0.6613	0.0512
5	54.5870	65.63	0.2261	0.014

Using the proposed method invisible watermark is obtained so that the purpose of the image must not be violated. When compared to the traditional work satellite image security is more in the proposed method. This can be theoretically analyzed by checking the values of MSE and PSNR. MSE value is less and PSNR value is more when compared to the previous work [13]. This shows the improved security level of satellite images.

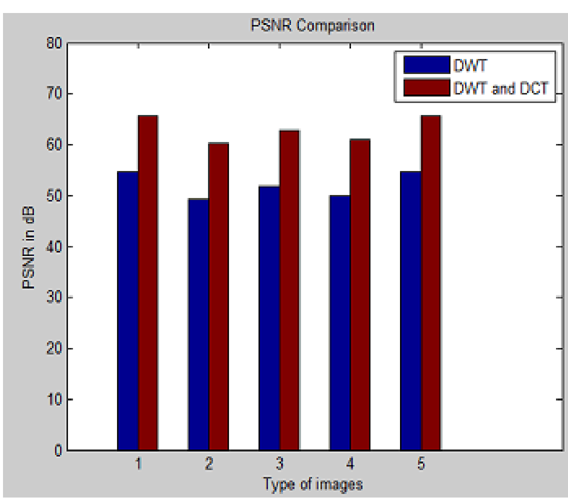

Fig.11: PSNR comparison

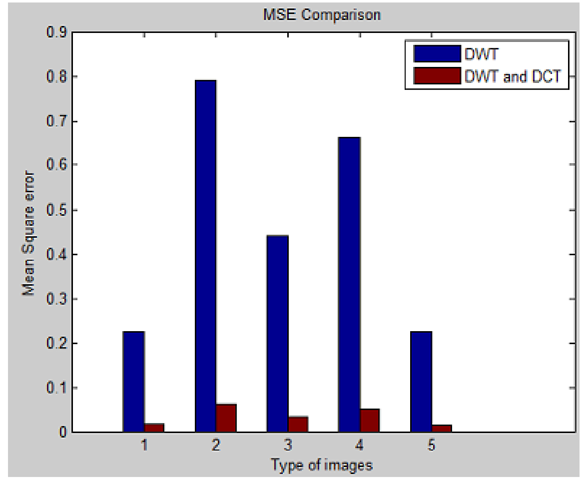

Fig.12: MSE comparison

5. Conclusion and Future Work

The proposed satellite image watermarking system not only can keep the image quality well, but also can be robust against many image processing operations like filtering, sharp enhancing, adding noise etc. This algorithm has very strong capability of embedding watermark signal and anti-attack. Matlab is used for simulation purpose. The comparability of the recovered watermark and the original watermark can be quantitatively analyzed by using peak signal to noise ratio (PSNR) and mean square error (MSE). Combination of DCT and DWT can be used to improve the PSNR. Combined DWT-DCT watermarking along with AES encryption provide more security for satellite images.

As the future work some post processing operations such as image restoration and correlation can be used to further improve the watermark recognition process and hence can increase the success rate against different types of image attacks.

Acknowledgement

We would like to thank Dr. Ibrahim Sadar, HOD, EC department, MACE for his valuable guidance and encouragement in pursuing this paper. We also acknowledge our gratitude to other members of faculty in the Department of Electronics and Communication Engineering, MACE and all our friends for their whole hearted cooperation and encouragement.

References

[1] Mehdi Khalili, David Asatryan, "Colour spaces effects on improved discrete wavelet transform-based digital image watermarking using Arnold transform map", IEEE Journal ,2013, Vol. 7, Iss. 3, pp. 177187.
[2] Alavi Kunhu and Hussain Ahmad, "Multi Watermarking Algorithm Based on DCT and Hash Functions for Color Satellite Images" , IEEE 2013.
[3] K.Anusudha1 A.Sangeetha , "Digital Watermarking Of Satellite Images Using Secured Spread Spectrum Technique", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.
[4] Yogesh Chauhan. P. Gupta. K. L. Majumder, "Digital Watermarking of Satellite Images", Department of Computer Sc. Engg. Department of Computer Sc. Eng,2008.
[5] P. Hsu, and C. Chen, "Feature based digital watermarking for remote sensing images", International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Volume B3, 2012.
[6] Anthony Tung Shuen Ho, "Robust Copyright Protection of Satellite Images Using a Novel Digital Image in Image Watermarking Algorithm", IEEE, Geosciences and Remote sensing, 2001.
[7] S. Esakkirajan, T. Veerakumar, Adabala N. Subramanyam, and C. H. PremChand, "Removal of High Density Salt and Pepper Noise Through Modified Decision Based Unsymmetric Trimmed Median Filter ", IEEE Signal Processing Letters, VOL. 18, NO. 5, MAY 2011.
[8] Jeba Nega Cheltha, C. ; Velayutham, R , "A novel error-tolerant method in AES for satellite images" ,Emerging Trends in Electrical and Computer Technology (ICETECT), 2011 International Conference A new method for satellite image security using DWT-DCT watermarking and AES encryption .
[9] Ali Al-Haj , "Combined DWT-DCT Digital Image Watermarking" , Journal of Computer Science : 740-746, 2007 ISSN 1549-3636.
[10] Sha Wang, Shital Gupta, Dr Sanjeev Jain, "A Robust Algorithm of Digital Image Watermarking Based on Discrete Wavelet Transform", IJCCT Vol.1 Issue 2, 3, 4; 2010 for International Conference [ACCTA-2010], August 2010.
[11] Mohammad Ibrahim Khan, Md. Maklachur Rahman and Md. Iqbal Hasan Sarker , "Digital Watermarking for Image Authentication Based on Combined DCT, DWT and SVD Transformation", International Journal of Recent Trends in Engineering, Vol. 1, No.1, May 2009.
[12] Natasa Terzija, Markus Repges, "Digital image watermarking using discrete wavelet transform: Performance comparison of error correction codes", Faculty of Engineering Sciences, Institute of Information Technology, 2008.
[13] Rakhi Dubolia , Roop Sing, "Digital image watermarking by using discrete wavelet transform and discrete cosine transform and comparison based on PSNR", International Conference on Communication Systems and Network Technologies, 2011.
[14] Mahasweta J.Joshi, Prof. Zankhana H.Shah, Keyur N.Brahmbhatt, "Watermarking in DCT-DWT Domain ", Mahasweta J.Joshi et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (2), 2011, 717-720.

Naida. H. Nazmudeen took her B Tech from University of Kerala with her major as Electronics Communication engineering. She is currently pursuing her Masters in Microwave Engineering from University of Kerala.

Farsana F.J. took her B Tech from University of Kerala with her major as Electronics Communication engineering. She took her masters in VLSI and Embedded systems from CUSAT and is currently working as Ass. Prof at Muslim Association College of Engineering.