



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

IJIRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 11, November 2022

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.118

 9940 572 462

 6381 907 438

 ijirset@gmail.com

 www.ijirset.com



Text Security through Digital Image Steganography using Different Transform Technique: A Review

Saurabh Singh¹, Prof. Satyarth Tiwari²

M. Tech. Scholar, Department of Electronics and Communication, Bhabha Engineering Research Institute, Bhopal, India¹

Guide, Department of Electronics and Communication, Bhabha Engineering Research Institute, Bhopal, India²

ABSTRACT:- In the era of information technology, the massive amount of information is transferred over public channels; some sensitive data and information pass through un-trusted communication channels. Means Information travels via computer networks worldwide. So, the main issue is delivery of the original message. Attackers and hackers attempt to break security over the sensitive data, thus exposing the actual information. And we do not want that our original message to be intercepted by anyone else excluding the recipient so to make our message safe many methods are used or we can say, various security mechanisms have been applied to improve data integrity and privacy. In this paper the study of different transform for digital image steganography and analysis of best transform technique.

KEYWORDS: - Steganography, Least Significant Bit, Discrete Cosine Transform, Discrete Wavelet Transform

I. INTRODUCTION

Information security is also called cyber security or computer security, provides safeguard to computer systems by threatening or stealing to the software and hardware or data stored on them, other than this, they also provide protection to interruption or misdirection of the services they offer. The importance of information security is of emergent significance due to the increasing dependence on digital system, use of the internet in the majority of sphere of life, wireless networks for instance Bluetooth, wifi in smart phones, communicating devices and the growth of internet of things which connect digital or electronic devices to internet. So importance of computer security is more consequential. In general computer security is the deterrence of, or defense against:-

1. Information access by illegal person.
2. Alteration to the information.
3. Destruction to the information and data.

Thus in other words it can be acknowledged as: "Security is the ability of a system to protect information and system resources with respect to confidentiality and integrity"

1.1 Aspects of Taxonomy of Information Security

Information security deals with three core concept, which may be precised by using the short form "CIA". Here "C" symbolizes confidentiality; "I" symbolizes integrity and "A" symbolizes authentication.

1. Confidentiality: - Confidentiality means protection of information by access or information should not be accessed by other than authorized person.
2. Integrity: - Integrity means protecting the information by alteration or information should not be altered by other than authorized person.
3. Authentication: - Authentication means verifying the users or verifying that users are the persons they insist to be. In addition to above three core areas of information or cyber security, nomenclature of information security also incorporate with:
 - a. Access control: - Authorized access is ensured. Only the users which have the access authority should only access the information and resources and the information also should be available as he or she desire.



- b. Non repudiation: - Responsibility is ensured. If anyone create or send the information then he or she cannot refuse that he did not do this.
- c. Availability: - The operational and functional performance of systems is ensured, failure of accessibility means denial-of-service of system.
- d. Privacy: - Access control is ensured. It gives anyone the authority that he or she can decide that what information or resources he want to share and what not, how the collected information used, who will be use this information and why.

The terms mentioned above concerning security taxonomy cannot be integrated to define a single aspect of security as each and every term has its own practical and theoretical meaning. Privacy is related to individual's security or we can say it is related to computer software and hardware whereas confidentiality is related to data. If we talk about practical point of view the conceptions are concerned with each other. Means if any system avoids or cannot protect data privacy and confidentiality then it's just a theoretically secure system not practically.

II. LITERATURE REVIEW

He Huang et al. [1], in order to promote the development of digital image steganography, the status and new direction of digital image stenography is analyzed. This paper summarized the development of traditional digital image steganography and illustrated that steganography based on adversarial example and steganography based on Generative Adversarial Networks are new directions in the field. Besides, the importance of digital image steganography and steganography analysis in the field of information security is also analyzed, and the method of steganography analysis for detecting and judging the secret information contained in the image is discussed. The paper also analyzed the current problem and proposed the future improvement direction.

Yıldırım Yiğit et al. [2], information security is a major problem today. Different approaches and methods are introduced every day for data protection. One of them is steganography. The word steganography combines the Greek words steganos , meaning "covered, concealed, or protected," and graphein meaning "writing". The purpose of steganography is to construct the stego object by placing important information invisible into the ordinary cover object (image, sound, video, text, etc.) and to transmit it to the recipient. In this study, it is aimed to strengthen the LSB technique which is one of the steganography methods by suggesting the use of mask which will provide the least change on the image while hiding the data into a digital image. In the proposed method, the data is also compressed by the LZW algorithm, thus allowing more data to be hidden.

Nazir A. Loan et al. [3], have proposed DCT domain watermarking can be classified into global DCT watermarking and block based DCT watermarking. Applying global DCT on image segregates the image into different frequency bands. He proposed spread spectrum based approach for watermark embedding using global DCT transform. Signal energy present in any frequency band is undetectable if a narrowband signal is transmitted over a much broader bandwidth. In this approach watermark is a narrow band signal which is spread over all frequencies so that the energy in any single frequency component is very small and is undetectable. Watermark is a pseudorandom sequence of fixed length and is produced using Gaussian distribution with zero mean and unit variance. It is embedded into the first one thousand largest AC coefficients. An objective measurement was proposed to evaluate the similarity between the original and extracted watermark. Block based watermarking algorithms differ either in block selection criteria or coefficient selection criteria. Pseudorandom subsets of the blocks are chosen, and a triplet of midrange frequencies is slightly altered to encode a binary sequence. Embedding of watermark information which is a pseudorandom sequence is performed by using inter block correlation of the DCT coefficients of the brightness of a color image. The strength of the watermark information to be embedded was varied with the visual features of the image.

Tomas Denmark et al. [4], it is widely recognized that incorporating side-information at the sender can significantly improve steganography security in practice. Presently, most side-educated plans use a high caliber "pre cover" picture that is in this manner handled and after that mutually quantized and inserted with a mystery. In this paper, we research an elective type of side-information– a lot of various JPEG pictures of a similar scene – for applications when the sender does not approach a pre-cover. The extra JPEG pictures are utilized to decide the favored extremity of implanting changes to regulate the expenses of changing individual DCT coefficients in a current inserting plan. The proposed exactly decided regulation of inserting costs is advocated utilizing Monte Carlo recreations by demonstrating that subjectively a similar adjustment limits the Bhattacharyya remove between a quantized summed up Gaussian model of cover and stego DCT coefficients ruined by AWG procurement commotion.



Morteza Heidari et al. [5], every day, people share their digital media on the virtual networks; therefore, protecting them against piracy is worthy of consideration. Advanced watermarking is a technique to accomplish this objective. In this paper, we propose a watermarking technique in Discrete Cosine Transform (DCT) area. For this reason, DCT coefficients of the entire picture are determined. It displays a framework without square ness impacts. We use scaling factors for watermark installing to enhance subtlety of the watermark. A vector of settled components, which is determined experimentally, is utilized as a lot of scaling factors. We install the watermark with a four-time repetition in the cover flag. It is helpful to take advantage of voting method for improving performance of the system in extraction phase. Trial Results show higher execution of the proposed strategy in correlation with comparative works in this area.

N. Senthil Kumaran et al. [6], the unlimited growth in internet and multimedia leads to large usage of images resulting in huge storage and distribution of multimedia contents. With expanding utilization of advanced transmission systems the potential dangers for mixed media content is high which lead to need of assurance for credibility and privacy. To ensure the classification, once cushion should be the most secure calculation. This paper proposes a safe calculation to ensure the watermark picture over an open system in computerized watermarking and is implanted in Discrete Wavelet Transformation (DWT). The special key same as size of watermark is produced from the cover picture. Once cushion is connected utilizing created special key to scramble the watermark picture. The encoded picture so shaped is inserted into cover picture in DWT area. The trial results demonstrate the adequacy and power of the calculation utilizing PSNR and NC figurings.

Bidyut Jyoti Saha et al. [7], in recent years, singular value decomposition has become a popular tool for image watermarking. In this paper, we propose another visually impaired watermarking plan by quantizing the solitary estimations of wavelet part. To upgrade the framework execution, we treat the picture watermarking as a multi-target enhancement issue dependent on non-overwhelmed arranging hereditary calculation II. In light of this new point of view, the inalienable clash existing in picture loyalty and watermark heartiness for picture watermarking can be equitably dealt with. The experimental study shows that our methods indeed provide superior performance.

Jiann-Shu Lee et al. [8], we present a new non-blind digital image watermarking method for embedding a binary logo in an image, based on the dual-tree complex discrete wavelet transform (DT-CDWT) and interval arithmetic (IA). As our experimental results demonstrated, since the high-frequency components obtained by using DT-CDWT and IA contained a low-frequency component, we may expect that the image quality and robustness is maintained even if we embed the watermark into the high-frequency components. A watermark was embedded in several high-frequency components. We describe our watermarking procedure in detail and report experimental results demonstrating that our method gives watermarked images that have better quality and that are robust against attacks such as marking, clipping, contrast tuning (MATLAB histeq and imadjust commands), addition of Gaussian white noise, addition of salt & pepper noise, JPEG and JPEG2000 compression, and rotation.

Teruya Minamoto et al. [9], initially, researchers worked with watermark encryption using a single chaotic map. The proposed a novel DCT-based watermarking, in which a binary visually meaningful information is embedded into the cover image to detect temperament. This technique is used to embed each byte information of watermark image in each DCT block by shifting any random coefficient to have a mapped value in a binary mapping coefficient function which is same as watermark bit.

III. STEGANOGRAPHY

Steganography strategy is the craft of hiding data subtly in a computerized cover medium, for example, picture, sound, and video. The word Steganography derived from the Greek words which mean covered writing in any object [7]. The principle goal of steganography is to disguise the presence of the data in the cover medium. Steganography, Cryptography and Watermarking are mostly used to hide the message in image and these techniques are closely related to each other [8].

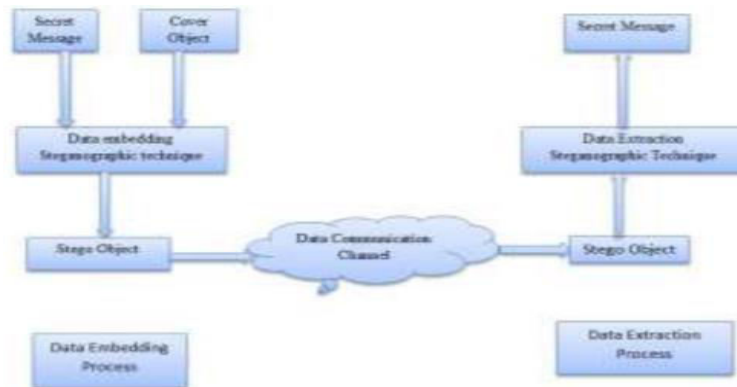


Fig. 1: Steganography system

The strong point of steganography over cryptography is that the hidden messages do not attract attention of third party when it transmitted to the desired recipients because of robustness and undetectably. As watched, amid the most recent quite a few years, an exponential development of utilization of interactive media information over the Internet as Digital Images, Video and Audio documents. The ascent of computerized information on the web has additionally upgraded the examination work committed to steganography. The few uses of steganography like secure mixed media watermarking, military interchanges and fingerprinting applications for the validation assurance to control the issue of advanced theft.

Numerous steganographic calculations can be utilized for these undertakings yet these are not ideal utilizations of steganography. The Stego picture outwardly is by all accounts same as cover picture however conceals the mystery information inside it and transmitted to the beneficiaries over the correspondence channels. At the point when the ideal beneficiary gets the Stego picture, at that point pursue the information extraction procedure to recoup the mystery information.

TYPES OF STEGANOGRAPHY:-

The sender composes a harmless message and after that covers a mystery message on a similar bit of paper. The principle objective of steganography is to impart safely in a totally imperceptible way and to abstain from attracting doubt to the transmission of concealed information. It isn't to shield others from knowing the shrouded data, yet it is to shield others from suspecting that the data even exists. The information can be obvious in fundamental configurations like: Audio, Video, Text and Images and so forth. These types of information are perceptible by human stowing away, and a definitive arrangement was Steganography. The different kinds of steganography include:

- a. Image Steganography: The Image Steganography is method in which we shroud the information in a picture so that there won't be any adjustment in the first picture.
- b. Audio Steganography: Sound Steganography can be utilized to shroud the data in a sound document. The sound record ought to be imperceptible.
- c. Video Steganography: Video Steganography can be utilized to conceal the data in video records. The video records ought to be imperceptible by the aggressor.
- d. Text files Steganography: Content Steganography is utilized to shroud the data in content records. The general procedure of steganography i.e., setting up a stego object that will contain no change with that of unique item is arranged yet utilizing content as a source.

IV. TRANSFORM TECHNIQUES

4.1 DISCRETE COSINE TRANSFORM

A discrete cosine transform (DCT) express a finite sequence of data points in expressions of a sum of cosine functions oscillating at different frequencies. DCTs are mainly important to numerous applications in science and engineering, from lossy compression of audio(e.g.-MP3) and image(e.g. JPEG) (where small and high frequency components can be rejected), to spectral method for the numerical solution of partial differential equations.

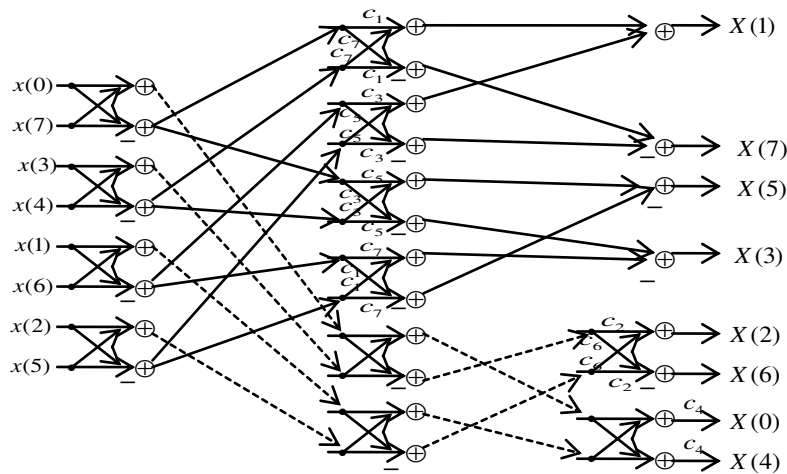


Fig. 2: 8-point Discrete Cosine Transform

The use of cosine function instead of sine is critical for compression, since it turns out (as explained below) that fewer cosine functions are required to approximate a typical signal, where for differential equations cosines function express a particular choice of boundary conditions.

DCT output:

$$\begin{aligned}
 F(0) &= 0.5[f(0) + f(1) + f(2) + f(3) + f(4) + f(5) + f(6) + f(7)] \cos \frac{\pi}{4} \\
 F(1) &= 0.5\left[\{f(0) - f(7)\} \cos \frac{\pi}{16} + \{f(1) - f(6)\} \cos \frac{3\pi}{16} + \{f(2) - f(5)\} \cos \frac{5\pi}{16} + \{f(3) + f(4)\} \cos \frac{7\pi}{16}\right] \\
 F(2) &= 0.5\left[\{f(0) - f(3) - f(4) + f(7)\} \cos \frac{2\pi}{16} + \{f(1) - f(2) - f(5) + f(6)\} \cos \frac{6\pi}{16}\right] \\
 F(3) &= 0.5\left[\{f(0) - f(7)\} \cos \frac{3\pi}{16} + \{f(6) - f(1)\} \cos \frac{7\pi}{16} + \{f(5) - f(2)\} \cos \frac{\pi}{16} + \{f(4) + f(3)\} \cos \frac{5\pi}{16}\right] \\
 F(4) &= 0.5[f(0) + f(3) + f(4) + f(7) - f(1) - f(2) - f(5) - f(6)] \cos \frac{\pi}{4} \\
 F(5) &= 0.5\left[\{f(0) - f(7)\} \cos \frac{5\pi}{16} + \{f(6) - f(1)\} \cos \frac{\pi}{16} + \{f(2) - f(5)\} \cos \frac{7\pi}{16} + \{f(3) + f(4)\} \cos \frac{3\pi}{16}\right] \\
 F(6) &= 0.5\left[\{f(0) - f(3) - f(4) + f(7)\} \cos \frac{6\pi}{16} - \{f(1) - f(2) - f(5) + f(6)\} \cos \frac{2\pi}{16}\right] \\
 F(7) &= 0.5\left[\{f(0) - f(7)\} \cos \frac{7\pi}{16} + \{f(6) - f(1)\} \cos \frac{5\pi}{16} + \{f(2) - f(5)\} \cos \frac{3\pi}{16} + \{f(4) + f(3)\} \cos \frac{\pi}{16}\right]
 \end{aligned}$$

4.2 Discrete Wavelet Transform

The model used in [8] to implement the tree structure of Direct Wavelet Transform (DWT) is based on the filtering process. Figure 1 depicted a complete 2-level Direct WT. In this figure G and H is the high pass and low pass filter respectively.

Computation period is the number of the input cycles for one time produces output samples. In general, the computation period is M= for a j-level DWT. The period of the 2-level computation is 8. Figure 1, The Sub band Coding Algorithm As an example, suppose that the original signal X[n] has N- sample points, spanning a frequency band of zero to π rad/s. At the first decomposition level, the signal passed through the high pass and low pass filters, followed by subsampling by 2. The output of the high pass filter has N/2- sample points (hence half the time resolution) but it only spans the frequencies π/2 to π rad/s (hence double the frequency resolution) [9].

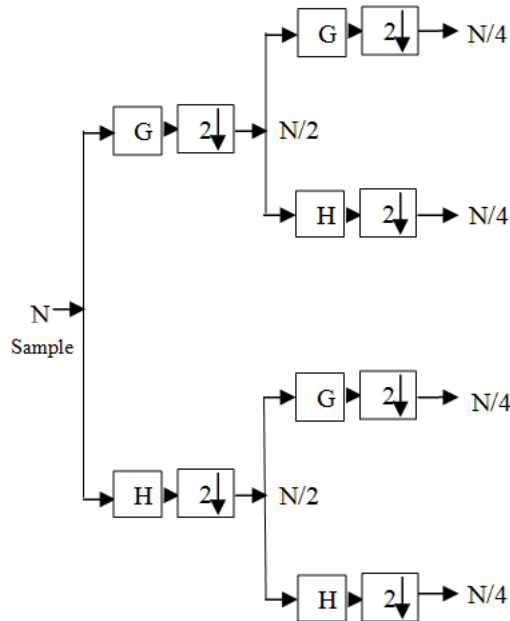


Fig. 3: 2- Levels for DWT. Where G, H are the high-pass and low-pass filter coefficient

The output of the low-pass filter also has $N/2$ - sample points, but it spans the other half of the frequency band, frequencies from 0 to $\pi/2$ rad/s. Again low and high-pass filter output passed through the same low pass and high pass filters for further decomposition. The output of the second low pass filter followed by sub sampling has $N/4$ samples spanning a frequency band of 0 to $\pi/4$ rad/s, and the output of the second high pass filter followed by sub sampling has $N/4$ samples spanning a frequency band of $\pi/4$ to $\pi/2$ rad/s. The second high pass filtered signal constitutes the second level of DWT coefficients. This signal has half the time resolution, but twice the frequency resolution of the first level signal. This process continues until two samples are left. For this specific example there would be 2 levels of decomposition, each having half the number of samples of the previous level.

The DWT of the original signal is then obtained by concatenating all coefficients starting from the last level of decomposition (remaining two samples, in this case). The DWT will then have the same number of coefficients as the original signal.

4.3 Least Significant Bit (LSB)

LSB is the most common method used in Steganography. In digital computing, there are two important exertions: the first one is the Least Significant Bit (LSB) and the second one is the Most Significant Bit (MSB). Least Significant Bit (LSB) is sometimes called right most bit. It is a bit position in binary values. It is called least significant bit, because the value of the bit has lowest change in the binary value. Most Significant Bit (MSB) is called high order bit, it is a bit position in binary values. It is called most significant bit, because of the bit has the highest change in the binary value.

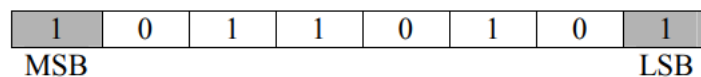


Fig. 4: LSB and MSB

For Example, if we have the decimal number (181) that is represented in binary number as (10110101) and if we changed the LSB from (1) to (0) then the binary number value of the (10110101) equals to (180) in decimal number value. If we changed the MSB from (1) to (0), binary number value of the (10110101) equals to (53) in decimal number value; so that means LSB has a low change of the value number and the MSB has a high change of the value number. Figure 1.2 shows an example about the LSB and MSB. 1 0 1 1 0 1 0 1 MSB LSB Fig. 4: LSB and MSB Least Significant Bit is used in Steganography because of the change of the resolution in image pixels may be increased or decreased by one or stayed at the same resolution [55]. If the Must Significant Bit of the cover media is used then the change of the cover media becomes visible. Least Significant Bit technique is used to in steganography process to hide



the secret message bits in the least Significant Bit of the image pixels. The following Figure 1.3 shows an example to hide the number 188 in the Least Significant Bit.

The number (188) is represented in binary as (10111100) and we want to hide every one bit in one image pixel. So, we need eight pixels (or eight bytes because each pixel is represented as one byte) to hide the number (188).

Byte 1	Byte 2	Byte 3	Byte 4
1010010 <u>0</u>	1010011 <u>0</u>	1010100 <u>1</u>	1000010 <u>1</u>
1	0	1	1
10100101	10100110	10101001	10000101
Byte 5	Byte 6	Byte 7	Byte 8
0101100 <u>1</u>	0111010 <u>1</u>	0110101 <u>0</u>	1010011 <u>0</u>
1	1	0	0
01011001	01110101	01101010	10100110

Fig. 5: Example to hide the number 188 in LSB

V. PARAMETER

It is most commonly expressed in terms of means squared error (MSE) or peak-signal-to-noise ratio (PSNR). The performance of image compression systems is measured by the metric defined in equations (1) and (2). It is based on the assumption that the digital image is represented as $N_1 \times N_2$ matrix, where N_1 and N_2 denote the number of rows and columns of the image respectively. Also, $f(i, j)$ and $g(i, j)$ denote pixel values of the original image before compression and degraded image after compression respectively.

Mean Square Error (MSE)

$$= \frac{1}{N_1 N_2} \sum_{j=1}^{N_2} \sum_{i=1}^{N_1} (f(i, j) - g(i, j))^2$$

Peak Signal to Noise Ratio (PSNR) in dB

$$= 10 \times \log_{10} \left(\frac{256^2}{MSE} \right)$$

Evidently, smaller MSE and larger PSNR values correspond to lower levels of distortion. Although these metrics are frequently employed, it can be observed that the MSE and PSNR metrics do not always correlate well with image quality as perceived by the human visual system.

VI. CONCLUSION

Steganography is the art that allows us to write secretly. It's an art in which information is protected by hiding it into another message so that secret messages can be kept secret inside it, so that normal readers cannot read it and only the intended readers can read it. Data steganography is hiding the contents of data like text, images, audio and videos into another secret format during data transmission over the network. Its main aim is to keep information secure from unauthorized access. The process of covering plain text (original message) into cover text (message in which hide the original message) is called hiding and converting it back into plain text is called steganalysis.



REFERENCES

- [1] He Huang;Yinghui Xue;Linna Fan;Mo Li, “The Development and New Direction of Digital Image Stenography”, International Conference on Robots & Intelligent System (ICRIS), IEEE 2020.
- [2] Yildray Yigit;Murat Karabatak, “A Stenography Application for Hiding Student Information into an Image”, 7th International Symposium on Digital Forensics and Security (ISDFS), IEEE 2019.
- [3] Nazir A. Loan, Nasir N. Hurrah, Shabir A. Parah, Jong Weon Lee, Javaid A. Sheikh, and G. Mohiuddin Bhat, “Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption”, Received January 4, 2018, accepted February 7, 2018, date of publication March 16, 2018, date of current version April 25, 2018.
- [4] Tomas Denmark, and Jessica Fridrich, “Steganography with Multiple JPEG Images of the Same Scene”, IEEE Transactions on Information Forensics and Security, Volume: 12, Issue 10, 2017.
- [5] Morteza Heidari, Nader Karimi, and Shadrokh Samavi, “A Hybrid DCT-SVD Based Image Watermarking Algorithm”, Iranian Conference on Electrical Engineering (ICEE), IEEE 2016.
- [6] N. Senthil Kumaran, and S. Abinaya, “Comparison Analysis of Digital Image Watermarking using DWT and LSB Technique”, International Conference on Communication and Signal Processing, April 6-8, 2016, India
- [7] Bidyut Jyoti Saha, Kunal Kumar Kabi and Arun, “Non Blind Watermarking Technique using Enhanced One Time Pad in DWT Domain”, International Conference of Digital Signal and Processing, ICCCNT, IEEE 2014.
- [8] Jiann-Shu Lee and Fei-Hsiang Huang, “A New Image Watermarking Scheme Using Non-dominated Sorting Genetic Algorithm II”, International Symposium on Biometrics and Security Technologies, IEEE 2013.
- [9] Teruya Minamoto and Ryuji Ohura, “A non-blind digital image watermarking method based on the dual-tree complex discrete wavelet transform and interval arithmetic”, Ninth International Conference on Information Technology- New Generations, IEEE 2012.
- [10] Baloshi Mathews and Madhu S. Nair, “Modified BTC Algorithm for Gray Scale Images using max-min Quantizer”, Automation, Computing, Communication, Control and Compressed Sensing, PP. 01-05, 2013 IEEE.
- [11] Wang Santosh, U. V. S. Sitarama Varma, K. S. K Chaitanya Varma, Meena Jami, V. V. N. S Dileep, “Absolute Moment Block Truncation Coding For Color Image Compression,” International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-2, Issue-6, PP. 53-59, May 2013.
- [12] Chen and K. V. Karthik, “A Modified Three Level Block Truncation Coding _or Image Compression”, International Conference on Pattern Analysis and Intelligent Robotics, PP.31-35, June 2011 IEEE.
- [13] Fan, Arpana Parakale, Bharamgonda Madhuri Mahavir, Bharamu Ullagaddi, “Image Compression using Absolute Moment Block Truncation Coding”, International Conference on Pattern Analysis and Intelligent Robotics, PP.97-102, June 2011, Putrajaya, Malaysia.
- [14] Bin and Hon-Hang Chang, “A Data Hiding Scheme for Color Image Using BTC Compression Technique,” Proc. 9th IEEE International Conference on Cognitive Informatics, PP.845-850, 2010 IEEE.



INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118



ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 **9940 572 462**  **6381 907 438**  **ijirset@gmail.com**



www.ijirset.com

Scan to save the contact details