Data Hiding and Compression Encryption through Discrete Wavelet Transform and Block Coding

Shiva Dwivedi
M. Tech. Scholar
Department of Computer Science and Engineering
OCT, Bhopal

Sreeja Nair
Assistant Professor
Department of Computer Science and Engineering
OCT, Bhopal

ABSTRACT
The ubiquitous nature of digital network systems means that digital documents can be copied and distributed easily to large numbers of people with no cost. Individuals can download sound, picture and video records, and they can impart them to companions and they can control or adjust their unique substance. This is the reason there is an earnest need to ensure the copyright of such media. There are various advances that will give insurance from unlawful replicating. Advanced watermarking calculations were created to take care of this issue. To secure and less space data hiding and compression encryption through discrete shearlet transform (DST) and block based coding algorithm is present paper. According to efficient scheme is increase PSNR (peak signal to noise ratio), SSIM (similarity index) and decrease mean square error (MSE).

Keywords
DST, Block Coding, Data Hiding

1. INTRODUCTION
Watermarking calculations implant advanced marks or computerized information to demonstrate the proprietor's personality and stop copyright encroachment. A few business organizations around the globe offer copyright security administrations to their clients. The watermark can be visible [1], where it is easily seen by the observer and owner or invisible where it can be detected by the originator by certain decoding algorithms. For this application the watermark should be vigorous with the goal that it can't be annihilated by changing the computerized media. Another prerequisite for watermarking for copyright insurance is the calculation should be visually impaired. In visually impaired strategies the first media isn't required to separate the watermarking data. Security is an important issue which requires the watermark to be modified only by the owner [2].

A feasible solution is required, for telecommunication, consumer electronics and information technology industries, to provide secure transmission of content without sacrificing their security rights [3]. Emerging technologies for audio security has three main objectives: secure content transmission, authentication of audio information and copy control to protect audio data from illegal distribution and theft [4]. Cryptography has been set up as an innovation of essential significance for verifying advanced exchanges of information over unbound channels. By giving encryption of computerized information, cryptography empowers dependable point-to-point data trade and exchanges. When the beneficiary approves and decodes the information, the item can be hence taken from any substance distinguishing proof, verification of-proprietorship or other graphic data. This may prompt further duplication and re-appropriation leaving the rights holders weak and sovereignty less [5]. To enhance the security of audio data, digital watermarking and steganography techniques complement cryptography for protecting content even after it is deciphered [6].

The study of multimedia security therefore includes not just encryption but also watermarking and steganography. Steganography and Watermarking almost interchangeably, refers to hiding secondary information into the primary multimedia source. The primary multimedia sources can be audio, image, and video. There are unique techniques associated with each type of primary perceptual sources depending on their inherent redundancy and perceptual properties. These techniques have been proposed as elective strategies to implement the licensed innovation rights and shield advanced media from altering. In this thesis work the primary multimedia source is image [7].

A watermarking framework may be portrayed as a structure that contains two sections: an implanting part and a finder part. The installing part takes two data sources. One is the message we need to encode as a watermark, and the other is the host or the spread work in which we need to install the imprint. The watermarked work is either transmitted or recorded. The implanted message can be removed by utilizing the finder, which decides if the watermark exists or not. Computerized watermarking is utilized to offer proprietorship security, including distinguishing proof of the copyright proprietor and assurance [8].

The word steganography was started from Greek which implies secured composing. Steganography is the most established type of undercover channel. A renowned representation of steganography is Simmons' Prisoners' Problem [7]. Sound Steganography is the demonstration of implanting a mystery message inside a bigger message with the goal that others can't recognize the nearness of the mystery message [8]. Steganography can be utilized to conceal a message proposed for later recovery by a particular individual or gathering. Sound watermarking includes a procedure of inserting into host sound flag a perceptually straightforward advanced mark, conveying a message about the host data in order to stamp its ownership. The point in watermarking frameworks is to guarantee the strength of the concealed message; the nearness of the installed message itself does not need to be mystery [9].

2. DIGITAL WATERMARKING
The accessibility of PCs and simple access to the web has led to a critical increment in the downloading of computerized media documents. These advanced records can be pictures, music, recordings and different archives. The web moved toward becoming easy to understand with the presentation of the principal broadly utilized internet browser in November 1993. The web is an amazing dissemination framework for advanced media since it is economical and permits helpful downloading and sharing among people and associations. In this manner, replicating and changing these records and archives have turned out to be prevalent. The unlawful duplicating of certain sorts of

media has been a subject of worry for a long time. Subsequently, a critical answer for copyright insurance and verification is required [1]. Computerized watermarking is a compelling answer for ensure scholarly properties and copyrights by concealing data, for example, logos, marks or content into interactive media information, for example, pictures, recordings, or sound documents. Be that as it may, content proprietors (particularly expansive Hollywood studios and music marks) additionally observe a high danger of robbery. Before, utilizing simple gadgets represented a lower chance than with computerized media; replicating a simple document permits results in a corruption of the quality.

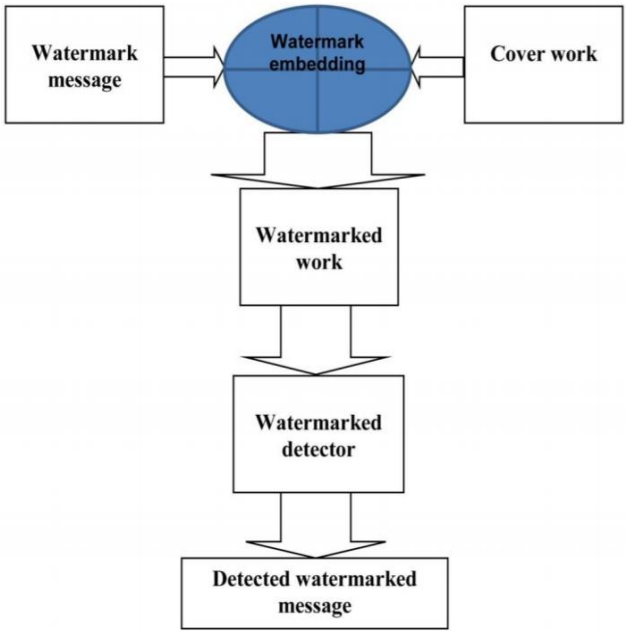

Figure 1: The watermark embedding and detection process

In the watermarking procedure, generally one mystery key is utilized. This mystery key is the essential component to tell the client that the substance is substantial or not by identifying the watermark. Setting the watermarking inside the framework is called inclusion or implanting. The way toward taking out the watermark is called extraction or discovery. In this way, the utilization of a watermark is an answer for copyright insurance and possession confirmation; the advanced information turn out to be progressively secure and are shielded from altering. Various types of watermarking strategies are accessible. Every one of them gives distinctive highlights and capacities which can be utilized for various purposes. For example, for altering check, a delicate watermarking can be utilized with computerized article sent through the web. On the collector side, the article is gotten. The substance will be confirmed by separating the implanted watermark. In the event that no watermark can be extricated, it implies the article got has been messed with [2, 3].

3. PROPOSED METHODOLOGY

DST includes decay of picture into recurrence channel of steady data transmission. This causes the comparability of accessible disintegration at each dimension. DST is executed as multistage change. Level shrewd deterioration is done in multistage change. S is an askew lattice of solitary qualities in diminishing request. The key idea behind SVD technique of watermarking is to find SVD of picture and the adjusting the specific motivator to embed the watermark. In Digital watermarking plans, SVD is utilized because of its essential properties:

A little irritation joined the photograph, does not cause colossal collection in its particular attributes. The specific regard addresses natural logarithmic picture properties.

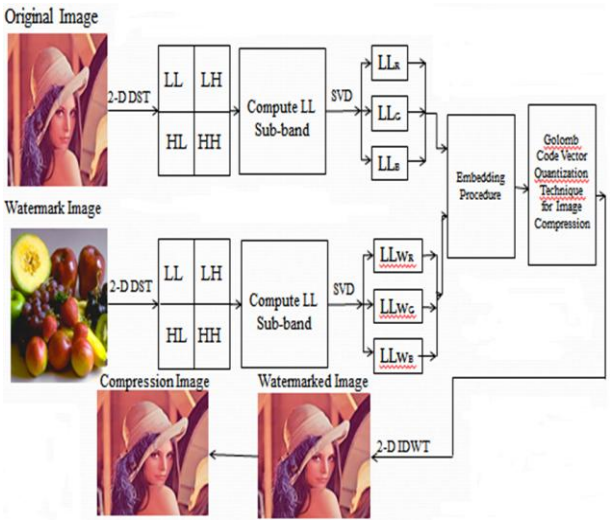

Figure 2: Block Diagram of Watermarking and Compressing Technique

Algorithm for Encryption & Decryption

Step 1: Input original image, take original image (OI).

Step 2: Apply 2-D DST on OI then four sub-parts of OI.

Step 3: Select sub-part LL2 of OI.

Step 4: Applied SVD in LL2 Sub-band

Step 5: Take watermark image (WI)

Step 6: Apply 2-D DWT on WI to decompose into four sub-bands.

Step 7: Select sub-band LL2 of WI.

Step 8: Applied SVD in LL2 Sub-band

Step 9: Embedding Process of CI and WI

Step 10: Applied Block Coding for Embedding Image

Step 11: Applied Decoder Process

Step 12: Finally get watermarked compressed image

DWT

DWT is a relative capacity containing a single parent Shearlet work that is parameterized by scaling, shear and interpretation parameters with the shear parameter catching the course of the singularities [8]. A vital preferred standpoint of this change over different changes is because of the way that there are no limitations on the quantity of headings for the shearing. There are likewise no requirements on the span of the backings for the shearing, not at all like, for example, directional channel banks [9] where utilizing a little window size would result in an exhibition misfortune. Along these lines, the Shearlet change is intended to manage directional and anisotropic highlights, commonly present in pictures, and can adequately catch the geometric data of edges.

We should indicate out that thought about shearlets created from the divisible capacities; shearlets produced from non-detachable capacities whose fundamental recurrence support. Can all the more successfully spread the recurrence plane. This demonstrates non-divisible creating capacities for shearlet framework can give the better casing limits or even tight casing.

In any case, the benefit of this divisible development is obviously the effortlessness of the development and one can without much of a stretch acquire shearlets with great properties, for example, conservative help and normality.

Single Value Decomposition

SVD is a mathematical tool used for reduction of any two dimensional matrix problems. picture can likewise be spoken to by two dimensional lattices. In this way, SVD can be utilized as a part of picture handling because of its properties, for example, transpose, solidness and so forth. The scientific model utilized as a part of SVD clarified here. SVD of a mxn lattice M is a factorization of M into a result of three grids given by (1).

$$M = U \sum V^T \quad (1)$$

Block Coding

Encoder part of the proposed calculation demonstrates that the first picture is separated into three sections for example R part, G segment and B segment. Every R, G, B segment of the picture is isolated into non covering square of equivalent size and edge an incentive for each square size is being determined.

Threshold value means the average of the maximum value (max) of 'k × k' pixels block, minimum value (min) of 'k × k' pixels block and m_1 is the mean value of 'k × k' pixels block. Where k represents block size of the color image. So threshold value is:

$$T = \frac{\max + \min + m_1}{3} \quad (2)$$

4. SIMULATION RESULT

MATLAB is high computing and technique language and MATLAB tool that can be used in several applications such as data visualization/analysis, numerical analysis, signal processing, control design, etc. Using the MATLAB software, solution can be achieved, accuracy and efficiency compared to other program languages. Different types of platform are used to MATLAB i.e. Editor Window, Simulink and Graphical user. In this paper Editor Window are used to implement DST and block based coding.

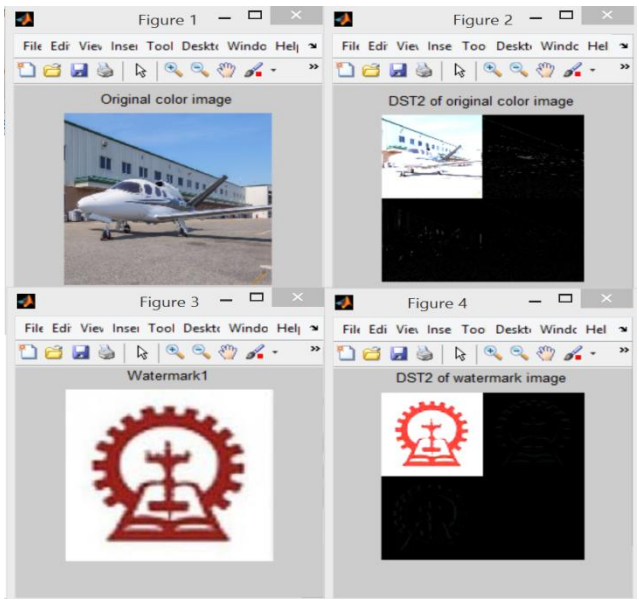

Figure 3: Simulation Result for Watermarking

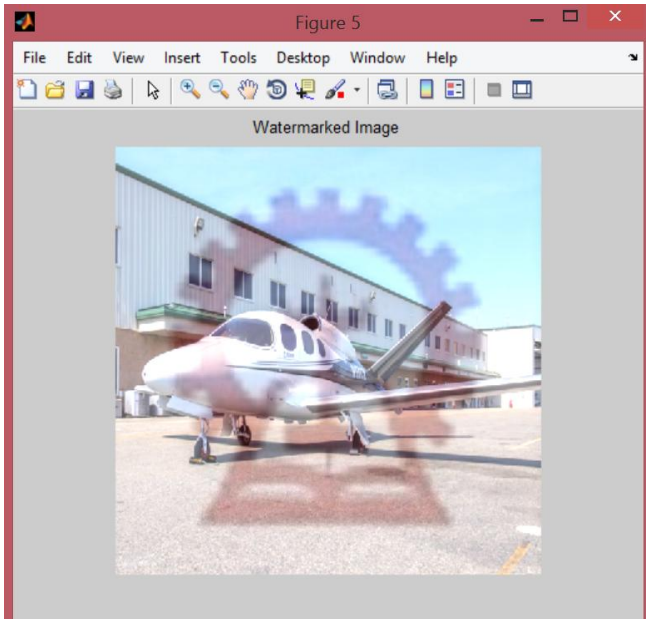

Figure 4: Watermarked Image

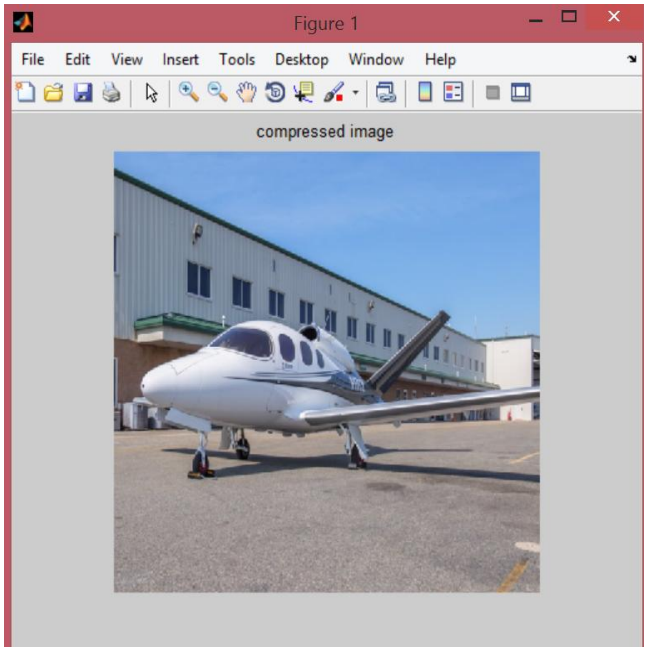

Figure 5: Compressed Image

Table 1: Experimental Results for Mean Square Error (MSE)

Image	4×4 Block Pixel	8×8 Block Pixel	16×16 Block Pixel	32×32 Block Pixel
Jet	116.05	200.51	295.00	440.87
Tank	206.98	376.86	546.42	756.05
Truck	54.97	103.11	168.72	272.32
Airplane	104.03	187.45	275.45	356.33
Boat	95.03	154.59	237.23	315.49

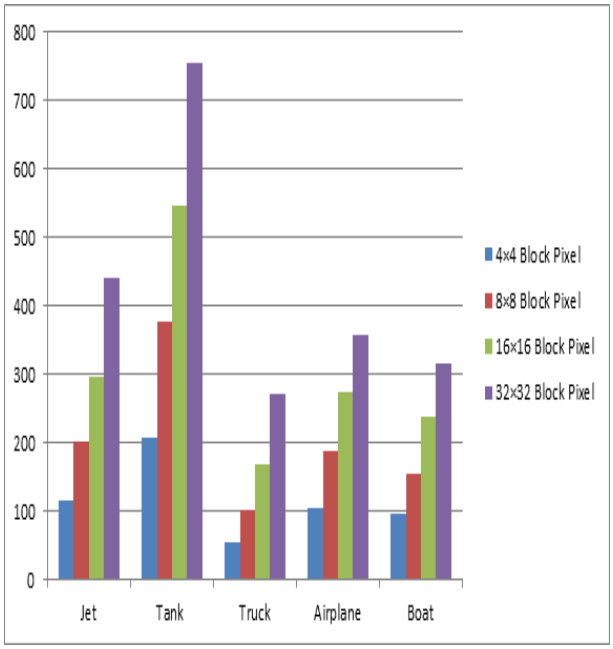

Figure 6: Bar Graph of the MSE for Different Image

Table 2: Experimental Results for Peak Signal to Noise Ratio (PSNR (dB))

Image	4×4 Block Pixel	8×8 Block Pixel	16×16 Block Pixel	32×32 Block Pixel
Jet	45.32	42.93	41.25	39.50
Tank	42.78	40.18	38.57	37.16
Truck	48.89	46.10	43.86	41.71
Airplane	43.06	41.56	39.43	38.33
Boat	46.76	44.05	42.19	40.96

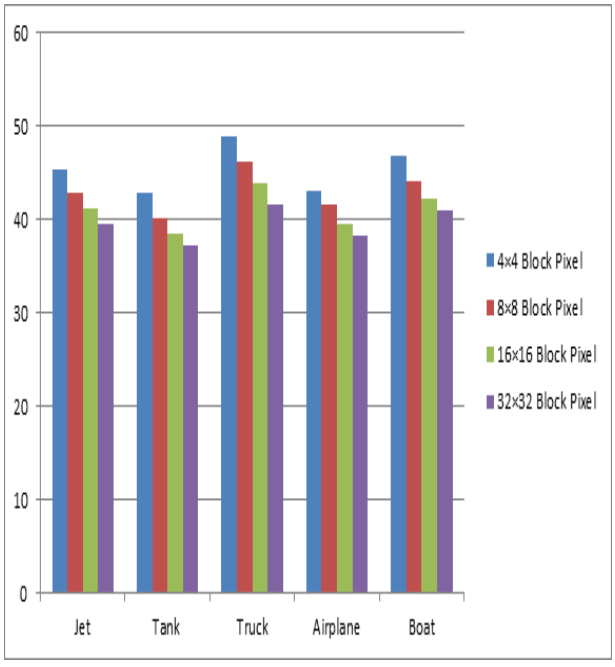

Figure 7: Bar Graph of the PSNR for Different Image

Table 3: Comparison Result for PSNR

Image	Previous Algorithm	Proposed Algorithm
Jet	36.83 dB	39.50 dB
Tank	36.70 dB	37.16 dB
Truck	36.65 dB	41.71 dB
Airplane	37.38 dB	38.33 dB
Boat	35.51 dB	40.96 dB

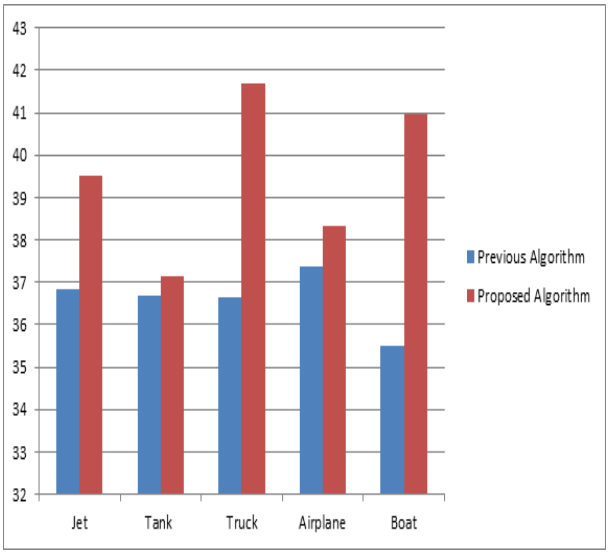

Figure 8: Result for Previous and Proposed Algorithm for PSNR

5. CONCLUSION

Security provided by the DWT technique and image compression by the block coding technique is presented. This paper applied proposed technique in different types of image and calculated some parameters like PSNR, SSIM and MSE. Particular attention is given to the proposed scheme to from the above descriptions, it have been shown that using Watermarking can ensure a secure message and less space.

6. REFERENCES

[1] Awdhesh K. Shukla, Akanksha Singh, Balvinder Singh and Amod Kumar, “A Secure and High-Capacity Data-Hiding Method using Compression, Encryption and Optimized Pixel Value Differencing”, IEEE Access, October 8, 2018.

[2] S. Thakur, A. K. Singh, S. P. Ghrera, and M. Elhoseny, ``Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications," in Multimedia Tools and Applications, pp. no. 01-14, Springer, 2018.

[3] R. Srivastava, B. Kumar, A. K. Singh, and A. Mohan, “Computationally efficient joint imperceptible image watermarking and JPEG compression: A green computing approach," Multimedia Tools Appl., vol. 77, No. 13, pp. no. 16447-16459, IEEE 2017.

[4] D. S. Chauhan, A. K. Singh, A. Adarsh, B. Kumar, and J. P. Saini, “Combining Mexican hat wavelet and spread spectrum for adaptive water-marking and its statistical

detection using medical images," in Multimedia Tools and Applications, pp. no. 01-15, Springer 2017.

[5] 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.

[6] Aase, S.O., Husoy, J.H. and Waldemar, P. (2014) A Critique of SVD-Based Image Coding Systems, IEEE International Symposium on Circuits and Systems VLSI, Orlando, FL, Vol. 4, Pp. 13-16.

[7] Ahmed, F. and Moskowitz, I.S. (2014) Composite Signature Based Watermarking for Fingerprint Authentication, ACM Multimedia and Security Workshop, New York, Pp.1-8.

[8] Akhaee, M.A., Sahraeian, S.M.E. and Jin, C. (2013) Blind Image Watermarking Using a Sample Projection Approach, IEEE Transactions on Information Forensics and Security, Vol. 6, Issue 3, Pp.883-893.

[9] Ali, J.M.H. and Hassanien, A.E. (2012) An Iris Recognition System to Enhance E-security Environment Based on Wavelet Theory, Advanced Modeling and Optimization, Vol. 5, No. 2, Pp. 93-104.

[10] Al-Otum, H.M. and Samara, N.A. (2009) A robust blind color image watermarking based on wavelet-tree bit host difference selection, Signal Processing, Vol. 90, Issue 8, Pp. 2498-2512.