International Journal of Advanced Computer Technology
ISSN: 2319-7900 www.ijact.org Volume 11, Issue 1, January-February 2022

An Efficient Digital Image Watermarking Based on DCT and Advanced Image Data Embedding Method

Akhaleshvari Jhade, Kedar Nath Singh
Department of CSE, TITS, Bhopal, M.P., India
akhaleshvarijhade@gmail.com, cseknsingh@gmail.com

Abstract-- *Digital image enhancement and digital content or data image secure using DCT and advanced image data embedding method (AIDEM). AIDEM improved robustness based on particle shifting concept is reproduced secure image data and manipulated there's a robust would like for a digital image copyright mechanism to be placed in secure image data. There's a necessity for authentication of the content because of the owner. It's become more accessible for malicious parties to create scalable copies of proprietary content with any compensation to the content owner. Advanced Watermarking is being viewed as a potential goal to the current downside. Astounding watermarking plans are arranged assaults on the watermarked picture are twisted and proposed to give insurance of proprietorship freedoms, information treating, and information uprightness. These methods guarantee unique information recuperation from watermarked information, while irreversible watermarking plans safeguard proprietorship freedoms. This attribute of reversible watermarking has arisen as an applicant answer for the assurance of proprietorship freedoms of information, unfortunate to alterations, for example, clinical information, genetic information, Visa, and financial balance information. These attacks are also intentional or unintentional. The attacks are classified as geometric attacks. This research presents a comprehensive and old method of these techniques that are developed and their effectiveness. Digital watermarking was developed to supply copyright protection and owners' authentication. Digital image watermarking may be a methodology for embedding some information into digital image sequences, like text image, image data, during this research analysis on image watermarking and attacks on watermarking process time image data, classification of watermarking and applications. We aim to secure image data using advanced image data embedding method (AIDEM) improved robustness based particle shifting concept is reproduced secure image data. To develop compelling digital image watermarking methodology using mat lab tool and reliable and robust.*

Keywords: Watermarking, Transform Domain Technique, DCT, LP-DWT, Visibility, Security, Robustness, AIDEM.

I. Introduction

The rapid development of computer communication and the Internet makes it very easy to lose exchange data via Networks. On the other hand, it also becomes crucial to protect the digital copyright of various digital media. Watermarking has been studied for more than ten years as a possible solution. In addition to copyright protection, watermarking can also be designed for other purposes such as hiding communication, data authentication, data tracing). Many data types can be used as the cover data for watermarking, e.g., digital image, audio, video, text, bar-code, 3D model, CAD data, 2D vector data, software's, VLSI [1]. The field of digital watermarking is relatively new; indeed, at this point, many of its terms are not well defined. They define watermarking as a process that embeds data, Called a watermark, into a multimedia object to help protect the owner's rights to that object. A digitally watermarked image is obtained by invisibly hiding signature information in the host image. The signature is recovered using an appropriate decoding process.

The challenge is to ensure that the watermarked image is perceptually indistinguishable from the original and that the signature is recoverable even when the watermarked image has been compressed or transformed by standard image processing operations. This paper describes various digital watermark algorithms studying their strengths and weaknesses and considering texture, luminance, corner and edge information in the image to generate a mask that makes the addition of the watermark less perceptible to the human eye. The operation of embedding and extraction of the watermark is done in both the spatial and frequency domains, thereby providing us information about the robustness against common attacks, including image compression and filtering. We use pseudo-random sequences to embed the watermark. Weighted Peak Signal to Noise Ratio evaluates the perceptual change between the original and the watermarked image [2].

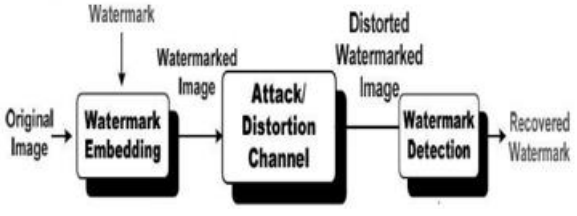

Fig1: Watermarking Diagram

Types of Transform Domain Technique: Several transform domain watermarking technologies are available in the literature.

1. Discrete Cosine Transform -The first efficient watermarking scheme was introduced by Koch et al. In their method, the image is first divided into square blocks of size 8x8 for DCT computation. A pair of mid-frequency coefficients is chosen for modification from 12 predetermined pairs. Bors and Pitas developed a method that modifies DCT coefficients satisfying a block site selection constraint. After dividing the image into blocks of size 8x8, certain blocks are selected based on a Gaussian network classifier decision. The middle range frequency DCT coefficients are then modified, using either a linear DCT constraint or a circular DCT detection region. A DCT domain watermarking technique based on the frequency masking of DCT blocks was introduced by Swanson. Cox developed the first frequency domain watermarking scheme. After that, many watermarking algorithms in the frequency domain were proposed. The popular block-based DCT transforms image non-overlapping blocks and applies DCT to each block. These results give three frequency sub-bands: low-frequency sub-band, mid-frequency sub-band and high-frequency sub-band. DCT-based watermarking is based on two facts. The first fact is that much of the signal energy lies at low- frequencies sub-band, which contains the most important visual parts of the image. The second fact is that high-frequency components of the image are usually removed through compression and noise attacks. Therefore, the watermark is embedded by modifying the middle-frequency sub-band coefficients. The image's visibility is not affected, and the watermark is not removed by compression [3].

2. Discrete Wavelet Transform- the DWT (Discrete Wavelet Transform) separates an image into four components, a lower resolution approximation image (LL), a horizontal (HL), a vertical (LH) and a diagonal (HH) detail component. The process can then be repeated to compute multiple "scale" wavelet decompositions. Discrete Wavelet Transform (DWT) is a mathematical tool for hierarchically decomposing an image. It is 0helpful for the processing of non-stationary signals. The transform is based on small waves, called wavelets, of varying frequency and limited duration. Wavelet transform provides both frequency and spatial descriptions of an image. Unlike conventional Fourier transform, temporal information is retained in this transformation process. Wavelets are created by translations and dilations of a fixed function called the mother wavelet. This section analyses the suitability of DWT for image watermarking and gives advantages of using DWT against other transforms. For 2-D images, applying DWT corresponds [4].

3. Singular Value Decomposition-SVD as a general linear algebra technique is used in various applications. SVD is optimal matrix decomposition in the slightest square sense packing the maximum signal energy into a few coefficients as possible. The SVD theorem decomposes a digital image A of size M × N, as A = USVT, (1) where U and V are of size M×M, and N ×N respectively. S is a diagonal matrix containing the singular values. In the watermarking trial, SVD is applied to the image matrix; then watermark resides by altering singular values (SVs)" [5]. Category of Watermarking: Digital image watermarking has constituted three classes, consequently supporting the various watermarks.

1. Visible Watermarking -These are the logos concept enlargement. These sorts of watermarks are solely applicable to the pictures. A transparency criterion evolves once these logos are embedded into the still pictures. The watermarks happiness to the current class is exhausting to get rid of or alter once cropping attack falls.

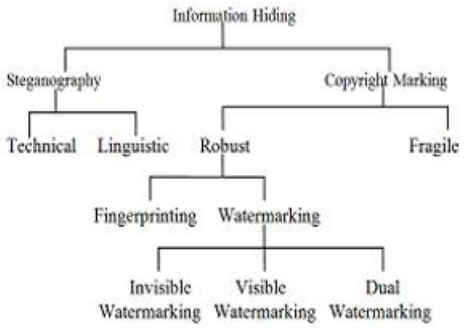

Fig2: Types of Watermarking

2. Invisible Watermarking -As the name clears, the watermark should be hidden from the surface world. The upper authority or agencies solely detect those sorts of the watermark. The watermarks happiness to the current class is utilized by the author authentication or creator or possession and for locating the unauthorized person.

3. Fragile Watermarking- The name knows these tamper-proof watermarks. The info management shatters the watermarks happiness to the current class and the image while not watermark indicates that a trial has been created on the initial image and forgery has evolved within the absence of watermark.

Applications of watermarking

1. Integrity Verification or Copyright Protection - When a new image is created, copyright information can be inserted as a watermark. In case of a dispute of ownership, this watermark can provide evidence.

2. Corrupt detection -Fragile watermarks are used for tamper detection. If the watermark is destroyed or degraded, it indicates tampering, so digital content cannot be trusted.

3. Content Authentications: Content authentication can detect digital content changes by using a fragile or semi-fragile watermark with low robustness to modification in an image.

4. Content Descriptions: This watermark can contain detailed information about the host image, including labelling and captioning. The watermark capacity should be relatively large for this application, and there is no strict robustness requirement.

5. Communications Authentications -It includes exchanging messages embedded secretly within images. The main requirement is that hidden data should not be identified [6].

Attacks on Watermarking

Fragile watermarks are ready to be destroyed by random image processing methods. The change in the watermark is easy to detect, thus providing information for image completeness. Robust watermarks are robust under most image processing methods and can be extracted from heavily attacked watermarked images. Thus, it is preferred in copyright protection. Attacks on the watermarked image are distortions in the watermarked image. These attacks may be intentional or unintentional. An image watermarking method can be judged against such relevant attacks. The attacks are broadly classified as geometric attacks. Geometric Attacks: Geometric attacks include fundamental geometric transformations in an image. These include geometrical distortions like rotation, scaling, translation, cropping, row-column blanking, warping. Geometric attacks attempt to destroy the synchronization of detection, thus making the detection process difficult and even impossible [7].

II. LITERATURE SURVEY

A literature survey is the most significant step in the software improvement process. Before developing the tool, defining the time factor economy and company power is necessary. Once these things are satisfied, the next step is to define which operating system and semantic can be used to develop the tool by the programmers start building the tool the programmer wants much external support. This support can be achieved from senior programmers, books, or websites. Before constructing the system, the above thoughts are taken into account for developing the proposed system

T. K. Leung et al. [8] presents a new Steganography technique based on the spatial domain for encoding additional information in a picture by making minor alterations to its pixels. The proposed technique concentrates on one popular technique, Least Significant Bit (LSB) Embedding. In place of using the LSB-1 of the cover for embedding the message, LSB-2 has been used to increase the robustness.

X. Li et al. [9] examine the opportunity to use Genetic Algorithms (GA) for data hiding in digital images. Two spatial domain data hiding approaches are planned where GA is used distinctly for (i) improvement in discovery and (ii) optimum imperceptibility of secreted data in digital pictures, respectively.

Ankur Goyal et al. [10] developed a technique for hiding information using LSB steganography and cryptography where the secret information is encrypted first using RSA or Diffie Hellman algorithm, and then the encrypted ASCII value is converted to binary form. Here even the cover image is converted from pixels to binary form, and then the secret message is embedded in the cover image using the LSB technique, and the stego-image is formed. With the proposed method, time complexity increases, but high security is achieved at that cost.

Ali Al-Ataby et al. [11] developed a modified LSB method in which text messages are hidden treated as 8 bit ASCII codes using an encryption algorithm, and these codes are converted into 5-bit codes and then hidden in the cover image using LSB. As an encryption algorithm used, if anyone extracts bits from the image, he won't understand until he decrypts it. So, with this technique, more information can be hidden with a level of protection.

Tanmay Bhattacharya et al. [12] proposed a DWT based Dual steganographic technique. Using DWT, a cover image is decomposed into four sub-bands. Two intimate images are hidden within HL and HH subbands, using a pseudo-random sequence and a session key. After embedding the secret data, all four sub-bands, including two modified subbands, are combined to produce the stego-image using IDWT. Through this method, a large amount of information is transferred more securely and has an acceptable level of imperceptibility.

Amritha G. et al. [13] proposed method steganography is object-oriented as it is based on one of the image features. Here the feature used is the skin region of the image. Instead of using a full cover image, embedding data only within the skin regions provide an excellent secure location for data hiding. Encrypt intimate images using the RC4 algorithm before embedding enhances the security level. This cover image is converted to HSV form to detect the skin colour. After that, the skin segment is detected

and cropped. That region is transformed into DWT form and secret image encrypted with RC4 cryptography algorithm. This encrypted data is embedded within a high-frequency subband of the cover image, and IDWT is performed. At last, by merging this segment stego-image is generated.

Raval and Rage et al. [14] introduced a multiple marking algorithm. In which DWT is applied after the decomposition of the main image to achieve a high level of robustness, multiple watermarks are inserted into the high-frequency subbands and low-frequency subbands. However, this plan is robust against many malicious attacks but achieving a watermark is not up to the mark. This method is visible to all, and the main image is mandatory during the extraction process.

Ghazy et al. [15] proposed the method that divides the image into non-overlapping blocks, and then SVD is applied to these blocks. Only singular values of these bocks were used to implant the watermark on the main image. This algorithm's implementations provide better results against different attacks like compression, filtering, and noise but are inefficient against cropping and geometric attacks.

Chandra et al. [16] proposed a non-blind digital image watermarking scheme using the spatial domain technique. The singular values of the watermark images are inserted into the singular values of the original image. On the other hand, this scheme proposed by the author does not hold good transparency and are not robust against geometric attacks.

III. ENVIRONMENT SETUP

The Performance analysis of MATLAB software different version used for this thesis Implementation of data mining provides processor optimized libraries for fast execution and computation and performed on input cancer dataset. It utilizes its JIT (without a moment to spare) aggregation innovation to give execution speeds that rival conventional programming dialects can also further advantage of multi-core and multiprocessor computers. MATLAB software provides much multi-threaded linear algebra and numerical functions. These functions automatically execute on multiple computational threads in single MATLAB software to execute faster on multicourse computers. In this thesis, all enhanced efficient data retrieve results were performed in MATLAB software to get image processing.

MATLAB software is a high-level language and interactive environment used by millions of engineers and scientists worldwide. It lets them explore and visualize ideas and collaborate across different disciplines with signal and image processing, communication and computation of results. MATLAB software provides tools to acquire, analyze, and visualize data, enabling you to get insight into your data in a division of the time it would take using spreadsheets or traditional programming languages. It can also document and share the results through plots and reports or published MATLAB software code. MATLAB programming (lattice research facility) is a multi-worldview mathematical registering circumstance and fourth era programming language. It is developed by math work; MATLAB software allows matrix strategy, plotting of function and data, implementation of the algorithm, construction of user interfaces with programs. MATLAB software is mainly for mathematical computing; an optional toolbox uses the MuPAD symbolic engine, allowing access to symbolic computing capabilities. It uses an image processing tool and function.

IV. RESULTS ANALYSIS

Our main objectives in research are visually undetectable, and achieving the desired robustness through PSNR values are better in DCT watermarking method. It is a reliable digital image and authentication. It is good robustness and ownership.

(a) Case 1: Superposition Attack

(i) Experiment image using port _kiel_city_germany (cover image 512x512) & tits messge_image (data image 64x64) embedding time analysis show in table 1 below.

Table 1 embedding time analysis in case1

Experiment Images	Method	ETS*
Port _kiel_city_germany (cover image 512x512) & indain army logo (data image 64x64)	DCT	3.62
	AIDEM	3.30
*ETS=Embedding Times in Second		

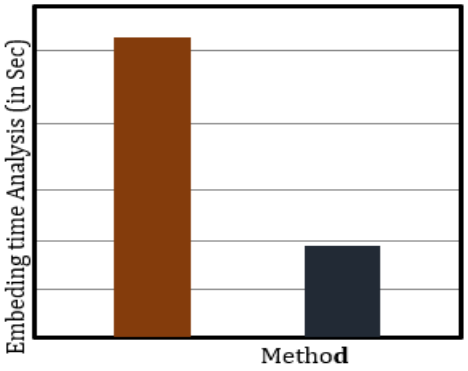

Fig3: embedding time analysis between DCT and AIDEM in case1

Experiment image using port _kiel_city_germany (cover image 512x512) and tits messge_image (data image 64x64) result analysis on base embedding time in seconds embedding time analysis and compare between DCT and AIDEM in show figure 3 below.

(ii) Experiment image using port _kiel_city_germany (cover image 512x512) & tits messge_image (data image 64x64) recovers time analysis shown in table 2 below.

Table 2 recover time analysis in case1

Experiment Images	Method	RTS
Port _kiel_city_germany (cover image 512x512) & indain army logo (data image 64x64)	DCT	1.33
	AIDEM	1.33
RTS=Recover time in second		

Experiment image using port _kiel_city_germany (cover image 512x512) and tits messge_image (data image 64x64) result analysis on base recover time in second recover time analysis and compare between DCT and AIDEM in show figure 4 below.

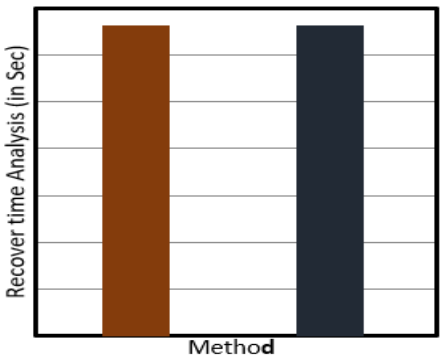

Fig4: recover time analysis between DCT and AIDEM in case1

(iii) Experiment image using port _kiel_city_germany (cover image 512x512) & tits messge_image (data image 64x64) PSNR values analysis shown in table 3 below.

Table 3 PSNR values analysis in case1

Experiment Images	Method	PSNR (in DB)
Port _kiel_city_germany (cover image 512x512) & titsmessge_image (data image 64x64)	DCT	156.20
	AIDEM	157.86

Experiment image using port _kiel_city_germany (cover image 512x512) and tits messge_image (data image 64x64) result analysis on base PSNR values. PSNR values analysis and comparison between DCT and AIDEM in show figure 5 below.

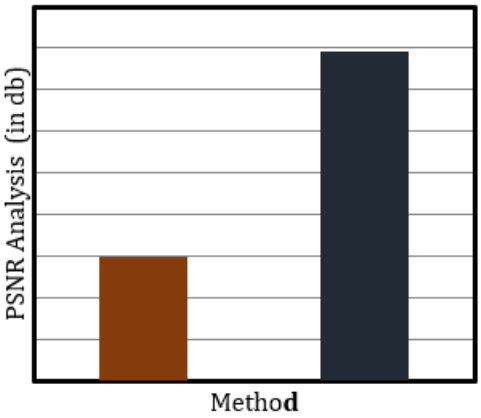

Fig 5: PSNR values analysis between DCT and AIDEM in case1

V. CONCLUSION

An efficient digital image watermarking based on DCT and advanced image data embedding method (AIDEM). AIDEM focuses on digital image watermarking in the frequency domain and digital watermarking techniques like DCT, their advantages, disadvantages and applications. Comparative study between DCT and AIDEM includes embedding time, extraction time, and PSNR values. For checking the robustness of these methods, various attacks on watermarked images are performed like noise attack, geometric rotation attack and superposition attack. AIDEM shows better results among these methods than PSNR after the attack on the watermarked image. I have introduced some basic concepts in digital watermarking, including its foundation, properties, requirements, and the comparison between digital watermark techniques. The digital image irreversible watermarking method changes the data to such an extent that data quality gets compromised. Advanced image data embedding method (AIDEM) provides such scenarios because they can recover the original data from watermarked data and ensure data quality. The proposed calculation's presentation assessment shows high intangibility by keeping the picture quality as the first pictures in the wake of watermarking, notwithstanding the high imperceptibility of the watermark. The advanced image data embedding method's result performance analysis deals with various parameters to check the method's robustness. The main goal of the proposed method (AIDEM) is to resist both geometric and noise attacks. Since no proposed method (AIDEM) resists all the attacks, one can still find the better-proposed method that gives a more robust watermark by performing various calculations. The point of assault is to disable watermark identification or annihilate the implanted watermark. Robustness against attacks is essential

for watermarking the proposed method (AIDEM). Finally, it highlighted the analysis system of the proposed method (AIDEM) various parameters like recover time analysis, embedding time analysis and PSNR values analysis graph showing in the result. Advanced image data embedding methods are more reliable and image data authentication against different attacks. The proposed method is determined to provide more reliable and higher PSNR values.

REFERENCE

[1]. A. Bors and I. Pitas, "Image watermarking using DCT domain constraints." in Proc. IEEE. Int. Conf. Image Processing, Lausanne, Switzerland, pp. 231-234, Sept. 1996.

[2]. R.C. Gonzalez, R.E. Woods, "Digital Image Processing", Upper Saddle River, New Jersey, Prentice Hall, Inc., 2002.

[3]. N Chaturvedi, S. J. Basha, "Comparison of Digital Image watermarking Methods DWT & DWT - DCT based on PSNR", International Journal of Innovative Research in Science, Engineering and Technology Vol. 1, Issue 2, Page no 147, December 2012.

[4]. Perez-Gonzalez, F.; Hernandez, J.R.;" A tutorial on digital watermarking" Security Technology, Proceedings. IEEE 33rd Annual 1999 International Carnahan Conference on. Oct. 1999, Page(s):286 – 292, 1999.

[5]. A Mansouri, A Mahmoudi Aznaveh And F Torkamani Azar, "SVD-based digital image watermarking using complex wavelet transform Volume 34, Part 3, pp. 393–406, June 2009.

[6]. Nag, Amitava, Sushanta Biswas, Debasree Sarkar, and Partha Pratim Sarkar. "A novel technique for image steganography based on DWT and Huffman encoding." International Journal of Computer Science and Security, (IJCSS) 4, no. 6: 497-610, 2011.

[7]. W. H. Lin, Y.R. Wang And SJ Horng, A wavelet tree-based watermarking method using distance vector of the binary cluster, Expert System with Applications, vol. 36, no. 6, pp. 9896-9878, 2009.

[8]. A. A. Efros and T. K. Leung, "Texture synthesis by non-parametric sampling," Sep.1999.

[9]. X. Li, B. Li, B. Yang, and T. Zeng, "General framework to histogram shifting-based reversible data hiding", June 2013.

[10]. Shailender Gupta, Ankur Goyal, Bharat Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography", International Journal Modern Education and Computer Science, Vol. 6, pp. 27-34, June 2012.

[11]. Ali Al-Atabey, Fawzi Al-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform", The International Arab Journal of Information Technology, Vol.7, October 2010.

[12]. Tanmay Bhattacharya, Nilanjan Dey, S. R. Bhadra Chaudhuri, "A Novel Session-Based Dual Steganographic Technique Using DWT and Spread Spectrum" International Journal of Modern Engineering Research, Vol.1, pp. 157-161, 2012.

[13]. Amritha G., Meethu Varkey, "Biometric Steganographic Technique Using DWT and Encryption", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue 3, pp. 566-572, March 2013.

[14]. M.S. Raval and P.P. Rege, Discrete Wavelet Transform based multiple watermarking schemes. Proceedings of the IEEE TENCON conference for Convergent Technologies for Asia-Pacific Region, Bangalore India, Vol.3, pp. 935-938, 2003.

[15]. Ghazy R A, El-Fishawy N A, Hadhoud M, Dessouky M I, and El-Samie F E A "An efficient block by - block SVD-based image watermarking scheme", Radio Science Conference, NRSC 1–9, 2007

[16]. DS. Chandra, Digital image watermarking using singular value decomposition, proc. Of 45th Midwest Symposium on circuits and systems (MWSCAS'02), Tulsa, OK, the USA, Vol. 3, pp. 264-267, 2002.

[17]. Mal Khalifa and al. "A Robust Non-blind Algorithm for Watermarking Color Images using Multi-resolution Wavelet Decomposition", International Journal of Computer Applications, Volume 37– No.8, pp 33-39, January 2012.

[18]. Y. Zhang, Blind Watermark Algorithm Based on HVS and RBF Neural Network in DWT Domain, WSEAS Transactions on Computers, Vol. 8, No. 1, pp. 174-183, 2009.

[19]. Wei-Bin Lee and Tung-Her Chen, "A public veriÞable copy protection technique for still images", The Journal of Systems and Software, Vol. 62, Issue 3, pp 195–204, 2002.

[20]. A. Piva, M. Barni, F. Bartolini and V. Capellini, "DCT based watermark recovering without restoring to the uncorrupted original image", In Proc ICIP, pp 520-523, 1997.