A Review on Enhanced, Robust and Invisible of Digital Image Using Discrete Cosine Transform Technique

Sneha Meshram[1], Santosh Kumar[2], *Seema Shukla[3]*
Department of EC, MITS, RGPV, Bhopal, India
[1]sneha11.meshram@gmail.com, [2]santoshkumar@gmail.com, [3]seematiwari.a@gmail.com

***Abstract* -** Digital media is the need of people now each day because of the alternate of paper media. Because the technology has grown up digital media required protection while exchange through the internet or web and therefore the widespread use of digital media medium. The mounting interest in digital watermarking throughout the last decade is certainly because of the rise within the need for copyright protection. Applications of video watermarking in copy control, broadcast monitoring, fingerprinting, image authentication, copyright protection, etc. the most aspects of data hiding are capacity, security, and robustness. The handiness of image data and detecting hiding data is security and robustness refers to the resistance to modification of the duvet content before concealed information is destroyed. It's required to protect the data from unauthorized access. The image watermarking techniques may divide on the idea of domain like spatial domain or transform domain or on the idea of wavelets. DCT algorithms are computation time increases and also low PSNR values image data hiding performance degradation. Our proposed technique increase PSNR values or increases robust and invisible digital image data.

Keywords: Encryption, Watermarking, Image Encryption, Image Decryption, Image Recovery, Robustness, Spatial Domain, Frequency Domain, DWT, DCT, PSNR.

I. Introduction

As the use of the internet is increasing day by day with this the insecurity of protection of copyright material, illegal copying of information, distribution, and modification of information is additionally increasing. Because of this copyrighting economic loss occurring, due to digital piracy of films and music. So there's a requirement of some technique that rise protection, security against Piracy, copyrighting. So Digital Watermarking is that technology that provides security, data authentication, and protection from copyright to the digital media. Digital watermarking may be a technique is used to protect multimedia data that transfer over the web. Digital Watermarking may be a means to embed copyright information into digital multimedia data like image, audio, etc. [1]. Digital watermarking is that the process by which a discrete data stream called a watermark is hidden within a multimedia signal by imposing imperceptible changes on the signal. In many proposed techniques this procedure entails the utilization of a secret key that must be wont to successfully embed and extract the watermark. Watermarking has gained interest in applications involving the protection of multimedia signals. One major drive for research during this area is the need for effective copyright protection scenarios for digital imagery, sound, and video. In such an application a serial number is watermarked into the signal to guard to mark ownership. It’s expected that an attacker will plan to remove the watermark by intentionally modifying the watermarked signal. Thus, we must strive to embed the mark such it's difficult to get rid of (without the utilization of the key) unless the marked signal is significantly distorted. In digital watermarking a number, the signal is transformed into a watermark domain during which modifications are imposed on the domain coefficients to embed the watermark. The modified coefficients are then inverse transformed to supply the marked signal1. Our proposed approach to improved robust watermarking applies to the overall class of watermarking methods with the subsequent basic properties: The watermark data stream consists of binary elements. The host signal (which refers to the first multimedia signal before watermarking) isn't available or exploited for watermark extraction. The whole watermark is consistently embedded throughout the signal and every duplication of the watermark is situated during a distinct localized region of the watermark domain. They’re going to discuss this later in greater detail. Digital watermarking is that technology which is employed for the security purpose of digital media like image [2]. In this technique, watermark i.e. secret information is inserted in digital media using some algorithms, and therefore the watermarked media is processed. Then, secret information is taken out (extracted) using the actual algorithm. This system, i.e. digital watermarking is employed for justification of information and protection of copyright. Image watermarking during this the image is employed to cover the digital data. It wont to protect the photos over the internet. This inserts special information to a picture and detects or takes it later for ownership confirmation. Consistent with Robustness Watermarks need robustness to guard the ownership from various attacks. The followings show the classification obsessed on the robustness of a watermark, Robust Resist various attacks, without affecting embedded watermark. Robustness watermarking is principally wont to sign copyright information of the digital works, the embedded watermark can protect against the common edit processing, image processing, and lossy compression, and therefore the watermark isn't cracked after some attack [3].

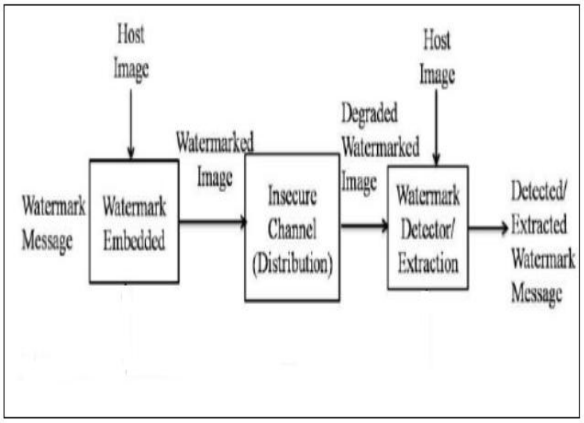
Host Image
Watermark Message
Watermark Embedded
Watermarked Image
Insecure Channel (Distribution)
Degraded Watermarked Image
Host Image
Watermark Detector/ Extraction
Detected/ Extracted Watermark Message

Fig1 processing of digital watermarking

Applications of Watermarking:

In the following, some existing application fields are explained alongside the reference technologies, and case studies are presented, highlighting a number of the foremost common world situation. Most of the examples shown ask the watermarking of digital images, but they're commonly applied to other media, like audio or video streams [4].

(a)Copyright Protection: the primary application area thereto watermarking is that the copyright protection of digital media. Within the digital world, nearly anyone can duplicate or manipulate digital information while not losing quality. This has allowed previously unseen infringement of copyright problems. Digital watermarking provides another layer of security to the content protection chain to discourage unauthorized use or duplication of content by embedding watermarks that establish original media and also the allowable uses of the content. In such a situation, devices scan the watermark throughout playback or copying of the content. If the watermark indicates that the utilization is unauthorized, the playback or copying is prevented and an informative message is additionally displayed. Effective content protection helps content, communicate copyright possession and uses rights of their content, protect it against common threats of piracy alongside TV camera recording, peer -to- peer file sharing, repetition format conversion, encryption and different types of re-processing [5].

(b)Image data security: a singular digital watermark is going to be simply embedded into every copy of a confidential document as they're being created and distributed. The knowledge contained within the watermark will include who are the recipients of each copy so that any information that's unknowingly or purposely leaked out is unquestionably copied back to the source. Additionally, companies are going to be network detectors and email filters to look at for digital watermarks within documents and pictures, providing notification if a trial is made at uploading to the internet or forwarding in email outside the corporate. Similarly, watermarked detectors are going to be enclosed in numerous printers, scanners, and different devices to look at for watermarks in confidential documents that somebody is making an effort to repeat. During this case the watermark will trigger an action, sort of a don't copy or scan. Therefore, document and image security helps to:

- Establish each copy of a confidential document and/or image with a unique digital identity;
- Traceback to the availability of leaks if sensitive materials are distributed intentionally or inadvertently;
- Filter documents being uploaded to the web or forwarded in the email to quickly determine confidential materials and stop distribution;
- Prevent the repetition of confidential documents on copiers and/or scanners [6].

II. Literature Survey

Behal et. al [7], presents the gap in Frequency domain and Spatial-domain methods, frequency-domain methods are more widely applied than spatial domain. The intent is to embed the watermarks within the spectral coefficients of the image. The foremost commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), the explanation for watermarking within the frequency domain is that the characteristics of the human sensory system (HVS) are better captured by the spectral coefficients.

Chang et. al [8], described that DCT (Discrete cosine transform) sort of a Fourier Transform, represents data in terms of frequency space instead of an amplitude space. this is often useful because that corresponds more to the way humans perceive light so that the part that isn't perceived is often identified and thrown away. DCT based watermarking techniques are robust compared to spatial domain techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring, etc. However, they're difficult to implement and are computationally more expensive. At an equivalent time, they're weak against geometric attacks like rotation, scaling, cropping, etc. DCT domain watermarking is often classified into Global DCT watermarking and Block based DCT watermarking. Embedding within the perceptually good portion of the image has its advantages because most compression schemes remove the perceptually insignificant portion of the image.

Wei Zheng et al.[9] in "Research during a Fast DCT Algorithm supported JPEG" presented a quick discrete cosine transform(DCT) algorithm which was implemented in compression supported JPEG would be presented. Firstly, supported the appliance of DCT in compression, several fast DCT algorithms were analyzed first, then the efficiency fast DCT algorithm, binary DCT, was demonstrated. Consistent with the experiment result. The performance of binary DCT in JPEG encoder might be comparable to the normal JPEG encoder. Within the algorithm, all coefficients are in binary and every one multiplication was replaced by shifting and addition operations which are easier and faster achieved by hardware and software. The complexity of transform was reduced by the binary DCT algorithm. Binary DCT is often implemented with a 16-bit data bus, making it very suitable for low-cost, fast, and low-power multimedia applications.

Giulia Fracastoro et al. [10] in compression, classical block-based separable transforms tend to be inefficient when image blocks contain arbitrarily shaped discontinuities. For this reason, transforms Incorporating directional information is an appealing alternative. During this paper, we propose a replacement approach to the present problem, namely a discrete cosine transform (DCT) which will be steered in any chosen direction. Such transform, called steerable DCT (SDCT), allows rotating during a flexible way pairs of basis vectors, and enables precise matching of directionality in each image block, achieving improved coding efficiency. The optimal rotation angles for SDCT are often represented as the solution of an appropriate rate-distortion (RD) problem. We propose iterative methods to look such a solution, and that we develop a fledged image encoder to practically compare our techniques with other competing transforms. Analytical and numerical results prove that SDCT outperforms both DCT and state-of-the-art directional transforms.

Hee-Dong et al. [11] proposed a strong watermarking scheme for DIBR 3D images using quantization on dual-tree complex wavelet transform (DT-CWT) coefficients. Approximate shift-invariance and directional selectivity are used to pick out a certain coefficient of sub-blocks and therefore the coefficient rows are grouped supported the properties of DIBR. During extraction, the threshold is carefully chosen with a low false-positive rate. it's shown during this paper that the embedded watermark is often stably extracted from the middle view and therefore the synthesized left and right views, although the synthesized left and right views are distorted by general attacks. Also, the proposed scheme is additionally shown to be robust to pre-processing of the depth image and baseline adjusting.

P. Dabas et al. [12] presented digital image watermarking is employed for copyright protection of digital information, with the widespread of the internet; the intellectual properties are accessible and manipulated easily. It demanded to possess alternative ways to guard data. Digital watermarking provides a viable and promising solution. during this paper, we've described the three different watermarking techniques (LSB, DCT, and DWT) alongside the varied performance parameters required to evaluate the simplest technique out of them. This will help us to propose and implement a new technique to realize maximum robustness against various attacks.

Khan et al. [13] propose a fragile zero watermarking scheme that detects and characterizes malicious modifications that are made to a database relation. Unlike other techniques, it doesn't leave any distortion within the database. This system also characterizes the type of tampering done to the database. The technique uses the local properties of database digits, data value length, and data value range. Sub-watermarks are created from all three characteristics and concatenated to make the watermark of the whole database. For watermarking of digits, the length of each value is calculated, and therefore the frequency of each digit and the total number of digits are calculated. The frequency of every one of the digits is calculated and concatenate to make the sub watermark. For the length sub watermark, an equivalent process is repeated. For a variety of sub watermark, different data ranges for features are defined. The frequency of information ranges is decided, then relative frequencies are calculated. These are then concatenated to make a sub watermark. These three are then concatenated to make the watermark of the whole database. Verification is completed just by creating a watermark for a suspicious database and comparing it with the watermark of the first database. A difference means the changes made to the database. A salient feature of the technique is that the characterization of malicious activity, that is, insertion, deletion, or modification. This scheme successfully detects subset deletion, addition, and modification attacks and doesn't alter the particular database.

Amirgholipour et al. [14]. During this paper, a replacement robust digital image watermarking algorithm supported Joint DWT-DCT Transformation is proposed. A binary watermarked logo is scrambled by Arnold cat map and embedded in certain coefficient sets of a 3-level DWT transformed of a number image. Then, the DCT transform of every selected DWT sub-band is computed and therefore the PN-sequences of the watermark bits are embedded within the middle frequencies coefficients of the corresponding DCT block. In the extraction procedure, the watermarked image, which may be attacked, is pre-filtered by a combination of sharpening and Laplacian of Gaussian filters to extend the distinction between the host image and watermark information. Subsequently, an equivalent procedure because the embedding process is employed to extract the DCT middle frequencies of every sub-band. Finally, the correlation between mid-band coefficients and PN sequences is calculated to work out watermarked bits. Experimental results show that prime imperceptibility is provided also as higher robustness against common signal processing attacks. In comparison to current watermarking algorithms which are supported the joint of DWT-DCT, the proposed system is achieved significantly higher robustness against enhancement and noise addition attacks.

Fotopoulos et al. [15]] decompose the first image into four bands using the Haar wavelet, then perform DCT on each of the bands; the watermark is embedded into the DCT coefficients of every band, A sub-band-DCT approach for image watermarking is proposed during this communication. The watermark is cast during a selected number of coefficients of all four bands of one-level decomposition. An excellent number of coefficients are getting used. Each band gives a special detection output. The result's taken because of the average detection results of all bands. it's shown that the ultimate result's better than the detection output of every individual band, thus resulting in a robust watermarking scheme.

III. Expected Outcome

The digital watermarking technique using image data hiding in terms of Optimization means improved robustness and PSNR.

IV. Conclusion

The DCT and discrete wavelet transform are different transform domain techniques and thus provide different, but complementary, levels of robustness against an equivalent attack Image watermarking is that the efficient process of sending the information securely. Security is that the major factor that's taken into consideration while the info is transferred over the web. Many watermarking techniques are proposed earlier for secure data transmission. Digital Watermarking is an extremely active rapidly evolving field of research and development with various applications. In Digital Watermarking for hiding any message, embedding the signals is completed by a different algorithm, MATLAB code, etc. watermarking also contains some transformations like DCT, DWT, DFT, etc. during this field of Image Processing today there's also research goes on for more betterment of robustness, transparent and secure watermarking techniques for various digital media like images, audio, video. The common requirement application for the watermark is that they resist attacks that will remove it. Another technique's blind watermarking, blind watermarking uses multiple numbers of watermarks and also there's no need for the original image at the watermark recovery. Hence can say that Digital Watermarking is that the easy and easy techniques by using it Data are often shielded from unauthorized duplication of information. Further implementations are often done on this idea to supply security to the watermark image which is to embed in image data and improved PSNR values.

References

[1]. Podilchuk, Christine I., and Edward J. Delp. "Digital watermarking: algorithms and applications." IEEE signal processing Magazine 18, no. 4: 33-46, 2001.

[2]. Cox, Ingemar J., Matthew L. Miller, and Ryoma Oami. "Robust digital watermarking." U.S. Patent 6,154,571, issued November 28, 2000.

[3]. Voyatzis, George, Nikolaos Nikolaidis, and Ioannis Pitas. "Digital watermarking: An overview." In 9th European Signal Processing Conference (EUSIPCO 1998), pp. 1-4. IEEE, 1998.

[4]. Wu, Min, and Bede Liu. "Watermarking scheme for image authentication." U.S. Patent 6,285,775, issued September 4, 2001.

[5]. Jiansheng, Mei, Li Sukang, and Tan Xiaomei. "A digital watermarking algorithm based on DCT and DWT." In Proceedings. The 2009 International Symposium on Web Information Systems and Applications (WISA 2009), p. 104. Academy Publisher, 2009.

[6]. Huang, Jianyong, and Changsheng Yang. "Image digital watermarking algorithm using multiresolution wavelet transforms." In 2004 IEEE International Conference on Systems, Man and Cybernetics (IEEE Cat. No. 04CH37583), vol. 3, pp. 2977-2982. IEEE, 2004.

[7]. M. Kaur, S. Jindal, S. behal, "A Study of Digital image watermarking", Volume2, Issue 2, 2012.

[8]. V. M. Potdar, S. Han, E. Chang, "A Survey of Digital Image Watermarking Techniques," 3rd IEEE International Conference on Industrial Informatics (INDIN), 2005.

[9]. Wei Zheng; Yanchang Liu, "Research in a fast DCT algorithm based on JPEG," Consumer Electronics, Communications and Networks (CECNet), 2011 International Conference on, 16-18 April 2011.

[10]. Fracastoro, Giulia, Sophie M. Fosson, and Enrico Magli. "Steerable discrete cosine transforms." IEEE Transactions on Image Processing 26, no. 1: 303-314, 2016.

[11]. Hee-Dong, Kim, "Robust DT-CWT watermarking for DIBR 3D images", In IEEE Transactions on Broadcasting, 58,4 pp.533-543, 2012.

[12]. P. Dabas, K. Khanna, "A Study on Spatial and Transform Domain Watermarking Techniques", International journal of computer application, vol.71, No.14, pp. 38-41, 2013.

[13]. Khan A, Husain SA. A fragile zero watermarking Scheme to detect and characterize malicious modifications in database relations. The Scientific World Journal 2013, 16 pages, 2013.

[14]. Amirgholipour, Saeed K., and Ahmad R. Naghsh-Nilchi. "Robust digital image watermarking based on joint DWT-DCT." International Journal of Digital Content Technology and its Applications 3, no. 2: 42-54, 2009.

[15]. V. Fotopulos, A.N. Skodras "A Subband DCT Approach to Image Watermarking," 10th European Signal Processing Conference 2000 (EUSIPCO'00), Tampere, Finland, Sept 2000.