Review on Digital Watermarking Images

[1]Salma Hussainnaik, [2]Farooq Indikar [3]Reshma H Husennaik,
[1]PG Student in K.L.S. Gogte Institute of Technology, Belagavi, Karnataka, India
, [2]Research Scholar, [3]Research Scholar

***Abstract:* Digital watermarking technique provides a superior and robust solution for ownership problem. Considering following issues in the existing system and the aim is to provide an excellent security to the image, the message is embedded within the image. Watermark is used in addition to the content encryption, where the encryption provides the secure distribution method from digital watermarking. Another issue is to use of digital watermark as a contents authentication and tamper proofing. In this paper it gives reviews of many papers of digital watermarking techniques.**

***Keywords:* watermarking, DCT, DWT, SVD**

I. INTRODUCTION

Digital Watermarking is treated as a solution to secure the multimedia data. Digital image watermarking is a process of inserting a piece of digital content into the original cover image and also it protects digital content from illegal manipulations. Digital watermarking technique provides a superior and robust solution for ownership problem. Considering following issues in the existing system and the aim is to provide a excellent security to the image, the message is embedded within the image.
Watermark is used in addition to the content encryption, where the encryption provides the secure distribution method from digital watermarking. Another issue is to use of digital watermark as a contents authentication and tamper proofing.

To address these issues various types of watermarking technique are discussed. The discrete cosine transform (DCT) represents an image as a sum of sinusoids of varying magnitudes and frequencies, discrete wavelet transform (DWT) Wavelet transform is a time domain localized analysis method with the window's size fixed and forms convertible, singular value decomposition (SVD) SVD is robust and reliable orthogonal matrix decomposition method SVD is an attractive algebraic transform for image processing.

Types of Digital Watermarking

The following are the different types of watermarking based on different watermarks:

Visible watermark:Visible watermarks works on the principle of logos and it has some extended features of concept of logos. "These watermarks are used only on images. These logos are inlaid into the image and they are transparent. These watermarks cannot be removed by cropping the center part of the picture. Further, such watermarks are protected against such as statistical analysis. The drawbacks of visible watermarks are degrading the quality of image and detection by visual means only". Thus, it is not possible to detect them by dedicated programs or devices. This type of watermarks is mainly used in software user interface, maps and graphics.

Invisible watermark:Invisible watermark as name itself indicates, it is unseen in the content. It can be identified by only authorized persons or agency. "This type of watermarks is used most in author authentications. This invisible watermark helps in finding unauthorized printer".

Robust Watermark: It embeds invisible watermarks. It is resist to image processing or attacks. This has wide applications in copyright security and in validating the ownership.

Fragile Watermark:**"**Fragile watermarks are those watermarks which can be easily ruined by any attempt to tamper with them. Fragile watermarks are ruined by data management. In the following figure an example of fragile watermarking the first one represent the original image, the second is the modified image and the third the detected modification".

Semi Fragile Watermark: This watermark has characters of both robust and fragile watermark. This is sensitive to signal modification. It is used mainly to provide data authentication.

II. LITERATURE SURVEY

The methodology for digital water marking of images using DCT is proposed in [1]. There are many algorithms available for digital image watermarking. Each type of algorithms consists of its own advantages and disadvantages. No method has efficient solution for digital watermarking. Each type has robustness to some type of attacks but is less efficient to some other types of attacks. Each type of digital watermarking depends on the nature of application and requirements. In this method, we presented a new approach of embedding watermark into color image. The RGB image is converted to YCbCr and then it is watermarked by using discrete cosine transform (DCT). The luminance component Y of image is considered for embedding watermark. The PSNR, SNR, MSE and NC for RED, BLUE and GREEN are evaluated to measure the performance of the proposed method. Existing techniques have worked on the gray scale of image. The result of this proposed technique is very effective for watermarking and watermark extraction for authentication. It supports more security and exact correlation between original watermark and extracted watermark.

In this approach digital water marking of images using DCT is proposed in [2]. The core object of this study is to design and employ a robust watermarking procedure for 24 bits digital color images. In the first step, color images are transformed from

RGB to YCbCr color space and then the luminance (Y) component of YCbCr color space is used for the embedding process. Next It is applied on the middle band DCT coefficients. The Y component of the cover image is divided into 8×8 blocks and then a binary watermark bit is added to each block. Experimental outcome of the proposed method denote that developed algorithm provides robust watermarking results for digital color images. We have been determined that there is some deterioration in few of the blocks in water marking and these blocks are aimed to be bought for watermarking. The average of adjacent pixels has been used in the DCT coefficients. The main idea of this proposed system is to prevent the loss of the watermark bit in DCT block is to reorganize the block method, the average of the adjacent pixels used, the changes made on the DCT coefficients, and the image deterioration to decrease to the minimum level. The corrected blocks are directly proportional to the magnitude of the watermark constant. During this process, the value of the PSNR is 38.5 dB levels fully recovered and the obtained watermark can be exactly as proposed method watermarking to ensure them to be effective and powerful. This proposed method is not only used in images compressed video (Mpeg) for media compatibility but it also offers an application domain and the potential for widespread impact.

The In the above approach of digital water marking of images using DCT is proposed in [3]. “Digital Image Watermarking can provide protection for images, videos, audios from unauthorized person, noise, copyright etc. DCT and DWT domain watermarking is much better than the spatial domain encoding because the attacks such as noising, compression, sharpening, and filtering can be prevented by DCT domain watermarking and can also be used for JPEG compression method. The high frequency sub bands of image compression scheme Embedded zero-tree wavelet (EZW) are used in DWT.”

The methodology for digital water marking of images using DCT is proposed in [4]. Our study is to focused on representing a joint DCT digital image watermarking algorithm. “To obtain further imperceptibility and robustness Proposed method exploits strength of two common frequency domains method; DCT and DWT. The idea of inserting watermark in the combined transform is based on the fact that jointed transform could remove the drawback of each other than an effective watermarking method could obtain. In this approach, watermark is implanted in most robust and imperceptible parts of image than previous methods. In this Watermarking the watermark is embedded in the special middle frequency coefficient sets of 3-levels DWT transformed of a host image, followed by computing 4×4 block-based DCT on the selected DWT coefficient sets. To detect watermark information during extraction process from the watermarked host image the pre-filtering operation, sharpening and Laplasian of Gaussian (LoG) filtering, is used. Then, the same procedure as embedding algorithm is applied on pre-filtered attacked image to extract middle frequency coefficients of each DCT block. Later, bits of watermark are extracted by comparing correlation between PN-sequences and these coefficients. Implementation result shows that the imperceptibility of the watermarked image is acceptable. This method can be tested by most of the common image processing attack such as different size of gaussian filtering as an enhancement attack, adding salt and paper noise, scaling with two common factors, 50% and 75%, cropping and compression attack. Proposed method shows a significant improvement in robustness compare to previous DWT-DCT based method by adding noise and enhancement attack. As much as, the watermarks are extracted from the image processing attack with lower MAE values, proposed method is more robust compare to previous method”.

In this methodology for digital water marking of images using DCT is proposed in [5]. “This method discusses the mapping technique to be used for watermarking of the biometric images. By varying the number of coefficients considered in this scheme the obtained image quality can be changed. Furthermore in this technique the face image itself can be retrieved from the watermarked fingerprint image. Thus authentication and compression of the fingerprint data is achieved. Biometrics based authentication systems are becoming gradually more popular as they provide enhanced security and user ease as compared to conventional token-based (I.D. card) and knowledge based (password) systems. With the increasing usage of biometric systems the trouble of storing the sensor data has become a main issue. In most of the cases the sensor data has to be transferred via a communication channel with high latency and low bandwidth. During the last decade a number of algorithms and standards for compressing biometric image data have been used because minimization of the amount of data is extremely desirable which is only done by compressing the data before transmission. The recent ISO/IEC 19794 standard says that face image and fingerprint data to be stored in loss manner in JPEG (Joint Photographic Experts Group), JPEG2000 and WSQ (Wavelet Scalar Quantization) format. Another major issue related to biometric system is the integrity and security of the stored templates. To solve this problem Existing literature focuses on encryption and watermarking techniques. In Encryption techniques security is not provided once the data is decrypted. Beside this, watermarking involves embedding information into host data to provide security even after decryption. A new watermarking technique was proposed in which facial information of a user in his/her fingerprint images are embedded. In the area of digital watermarking considerable work and research has been done during recent times. Most of the watermarking algorithms are incomplete (non-blind) because they need the original image to extract the watermark. In this approach, an efficient blind watermarking technique is proposed. In this method the face image is implanted into a fingerprint host image. Using mapping technique the fifteen DCT (Discrete Cosine Transform) coefficients of the face images (logo) are converted into binary bits. Into low frequency band coefficients of the DCT sub-blocks, these binary bits are embedded. It is seen that the algorithm offers outstanding compression without degrading the image quality”.

In this approach of digital water marking of images is proposed in [6]. “The study of many different watermarking techniques for digital images shows that its worth. There is still scope for enhancement while working on image watermarking and Still there are some attacks to which all the watermarking algorithm or methods results approximately no reluctance. In this approach of watermark embedding and extraction wavelet as well as DCT domain is exploited, we can says that it is robust against the intentional compression attack as our target images are those that can be put on the internet with least possible. With the high speed networks operating and exponential growth of internet throughout the world it’s a more challenging task to protect copyright of an individual’s creation. The high frequency sub band components are kept untouched and the embedding of watermark is done in the mid frequency band. The Digital watermarking provides a feasible solution to protect copyright and authentication of an intellectual property. In this technique, they have proposed a scheme which provides higher resistance for image processing attacks, the scheme is DCT based additive watermarking scheme".

The methodology for digital water marking of images is proposed in [7]. "Digital watermarking in the work presented was considered particularly on a satellite image by making use of the DCT algorithm after JPEG compression. By anticipating which coefficients will be modified by the succeeding transforms, it is possible to produce a watermarking method with good capacity, moderate robustness, and low visual impact. This method holds particularly true in the case of compression techniques, were the compression algorithms are well known. Additional work can be done as an enhancement of the single watermark to embed more than one watermark in a satellite image. The communication networks allows the widespread distribution of multimedia data in various ways because of its rapid growth. Since digital productions can be easily duplicated, encouraging illegal distribution of electronic documents and unauthorized cloning are issues that have to be resolved. This paper demonstrates a technique for digital watermarking using the Discrete Cosine Transform (DCT) Domain and for the purpose of authentication it introduces the use of pseudo random noise in watermarking to hide information. The underlying system is based on Code Division multiple Access (CDMA) is a form of spread spectrum communication. The main objectives are development of a watermark embedding strategy and the analysis of the results. A compression technique was considered as an image attack to perform the implemented approach. The proposed technique provided a robust watermark extraction and has been successfully tested on a simple satellite image".

In this methodology of digital water marking of images is proposed in [8]. "This technique deals with medical image watermarking, we aimed at using the Error Correcting Code and the DCT space. On other side, to improve the message integrity and the ECC to increase the security of the message against all types of alterations the hash function SHA-1 is used. The authenticity and the robustness of the obtained image are verified against various attacks. The insertions of the signature and the patient's recorder using this approach have lead to a good result in terms of image quality of the watermarked image. The robustness of this method is verified for the JPEG compression attack, "copy/paste" attack, and noise attack. The growth of information technology and communication domain in order to enhance the quality of life and increase the efficiency of medical services offers the medical sector many opportunities to practice the medicine at distance. At this stage, the watermarking contributes to keep secret to many data own to the patient and the keeping quality of the image. To preserve the image quality (the least modification of data contained in images implies a misdiagnosis) the watermarking applied on medical images is major problem on the one hand, and on the other hand, to extracting of the entirety of the data after many attacks (the least modification of data extracted implies a misdiagnosis). The proposed spaces in this system use the discrete cosine transform (DCT). In this perspective, we propose a watermarking method applied on the medical images".

The methodology for digital water marking of images is proposed in [9]. "The frequency domain technique, DCT based Digital watermarking methods and the earlier spatial domain LSB, are simulated and the results are represented in tabular format. Comparatively, the DCT based method is more robust than LSB based method in the tested possible attacks. This method can achieve by using the following two goals. The first one is that a legal user can retrieve the embedded watermark from the altered image. The second is illegal user, those are do not knowing the location of the embedded watermark in the image".

In this method of digital water marking of images is proposed in [10]. "To authenticate video stream in real time was presented by using Design of the hardware architecture of a digital video watermarking system. The implementation of the proposed system can be done by using FPGA and can be used as a part of an ASIC. In the recent implementation, FPGA was the simple and available way of the proof-of concept. The real-time image data protection can be achieved by implementing integration to peripheral video (such as surveillance cameras). The aim of this work was to achieve three goals. First, to propose a new digital watermarking system's HW architecture for video authentication and making it appropriate for VLSI implementation. Secondly, to make the watermarking system suitable for a real time video can be easily adapted with commonly used in digital video compression standards with the minor video frame degradation. The presented watermark system was capable of watermarking video streams in the DCT domain in real time. This paper presents insertion of invisible watermark information into compressed video stream in 3D DCT by making use of a hardware implementation of a digital watermarking system. The video compression and watermark embedding is processed in the discrete cosine transform domain. Instead of using the motion compensation algorithms the compression is performed using 3D DCT. Field programmable gate array is used to performed hardware implementation. The Results shows that hardware-based video authentication system using proposed watermarking technique features minimum video quality degradation and the hardware based watermarking system features are low power consumption, high processing speed and reliability".

In this methodology digital water marking of images is proposed in [12]. "In comparison with many watermarking algorithms, the proposed watermarking algorithm using SVD, DWT and DCT transformation are contributes more robust. In terms of imperceptibility The watermarked image quality is good. In this proposed watermarking algorithm all high bands HH, LH, HL are chosen which will cover the mid bands LH, HL and pure high band HH that provides more robust against various kinds of filtering noises and geometric noises. In future, the proposed algorithm can be enhanced using full band DWT-DCT-SVD and further can be extended to color images and video processing".

In this methodology for digital water marking of images is proposed in [13]. "In this they have used a combined DWT-DCT digital image watermarking algorithm where discrete cosine transform (DCT), discrete wavelet transform(DWT), Singular Value decomposition (SVD) and their cross combination have been applied. When compared with the DCT-SVD and DWT, the combination of these two transform with SVD has improved the watermarking performance. In addition the proposed algorithm can be improved using DWT-DCT-SVD and further can be extended to color video and images processing".

The methodology for digital water marking of images is proposed in [14]. "In this mechanism, a combined approach of Lifting Wavelet Transform (LWT) and Discrete Cosine Transform (DCT) is executed for copyright protection of digital images. The process of Lifting wavelet transform is used for decomposing of the real image. On the selected LWT sub-bands the discrete

cosine transform is applied. The watermark image is embedded in the Discrete Cosine Transformed of the selected Lifting Wavelet Transform sub-band of the original image. Consequently, the watermark image is taken from the watermarked image. The proposed system is blind watermarking because it does not make use original image for extraction. By the help of experimental results the efficiency of the proposed system is established".
In the above method of digital water marking of images is proposed in [15]. "After implementing my proposed work I am getting PSNR value of extracted watermark image is nearly between 88 to 92 and NC is 1.0000 which is good image quality and shows robust techniques Also, we get the robust watermarked image with high quality. It is more robust then the Spatial technique. It provides better result in case of Ownership identification and copyright protection. In this approach a robustly and multilayer security based color image watermarking algorithm in DWT-DCT domain is presented. To beneficial for improvement in results the use of YIQ color space for watermark embedding is applied Since pixel values are highly correlated in RGB color spaces. . This method is protects from various attacks like rotation, scaling, and Gaussian low-pass filtered etc. This algorithm provides multilayer security by using. Discrete Wavelet Transformed domain, Discrete Cosine Transformed domain, and color space conversions. In Future our Scope of our proposed techniques will be put into practice to make robust watermarking technique and extract watermarked image with more secure and high quality".
The methodology for digital water marking of images is proposed in [16]. "All the results which are obtained, we can be concluded that proposed approach is more efficient in terms of PSNR, computational time, complexity ,correlation with original watermark, and invisibility as compared to existing other methods for the same. The Combined algorithm of digital watermarking, which is based on DCT and DWT, as PSNR (i.e. 56.7416 dB) and computational time (i.e. 3.7284s) is very low whereas normalized correlation (i.e. 1) values are very high. The Performance of watermarking algorithm is improved by integrating two transforms which are purely based on discrete cosine transformed." The simulation result shows that this algorithm is much better for invisible watermarking and has good robustness for some common image processing operations".
In this method of digital watermarking of color images using DCT-DWT-SVD and DWT-DCT-SVD based watermarking algorithm is proposed [17]. "In this the images are tested for their efficiency using DCT, DWT, DCT-DWT-SVD and DWT-DCT-SVD watermarking algorithms. All the results obtained by testing the images conclude that the DWT-DCT-SVD based watermarking algorithm gives the better PSNR value better than the DCT, DWT, DCT-DWT-SVD based watermarking algorithms. Hence the imperceptibility is more in DWT-DCT-SVD based watermarking algorithm than other algorithms".

III. CONCLUSION

The literature survey gives us the clear concepts of all the watermarking algorithms. Depending upon the application the watermarking algorithm can be chosen. For the efficiency and imperceptibility the DWT-DCT-SVD based watermarking algorithm gives us the better result. And for Robustness the DCT-DWT-SVD based watermarking algorithm gives the better result with attacks.

REFERENCES

[1] PravinM. Pithiya, "DCT Based Digital Image Watermarking, Dewatermarking& Authentication", International Journal of Latest Trends in Engineering and Technology (IJLTET)ISSN: 2278-621X ,Vol. 2 Issue 3 May 2013.

[2] M. Yesilyurt "A New DCT Based Watermarking Method Using Luminance Component", ELEKTRONIKA IR ELEKTROTECHNIKA, ISSN 1392-1215, VOL. 19, NO. 4, 2013.

[3] DarshanaMistry "Comparison of Digital Water Marking methods", International Journal on Computer Science and Engineering(IJCSE), Vol. 02, No. 09, 2010, 2905-2909.

[4] Saeed K. "Robust Digital Image Watermarking Based on Joint DWT-DCT".

[5] Ameya K Naik "'A Blind DCT Domain Digital Watermarking for BiometricAuthentication"©2010 International Journal of Computer Applications (IJLTET) 0975 – 8887, Volume 1 – No. 16, 2010.

[6] Tribhuwan Kumar Tewari "An Improved and Robust DCT based Digital ImageWatermarkingScheme"International Journal of Computer Applications 0975 – 8887 Volume 3 – No.1, June 2010.

[7] Mustafa B. Abugharsa "Digital Watermarking Enhancement for Satellite Images Using a DCT Algorithm" International Conference on Recent Trends in Computer and Information Engineering (ICRTCIE'2013) Dec. 20-21, 2013.

[8] Mohamed Ali Hajjaji "A Digital Watermarking Algorithm Based on DCT:Application on Medical Image".

[9] Hitesh Agarwal "IMPROVED DIGITAL WATERMARKING SCHEMESUSING DCT AND NEURAL TECHNIQUES".

[10] Ann Varghese "Hardware Implementation of a Digital Watermarking System Using 3D DCT" International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), Volume 3, Issue 9, September 2014

[11] A.H. Taherinia "Two Level DCT Based Digital Watermarking" Department of Computer EngineeringSharif University of Technology.

[12] MaklachurRahman"A DWT, DCT AND SVD BASED WATERMARKING", International Journal of Managing Public Sector Information and Communication Technologies (IJMPICT), Vol. 4, No. 2, June 2013'.

[13] Mohammad Ibrahim Khan "Digital Watermarking for Image Authentication Based on Combined DCT, DWT and SVD Transformation".

[14] Amy Tun "Digital Image Watermarking Scheme Based on LWT and DCT" IACSIT International Journal of Engineering and Technology, Vol. 5, No. 2, April 2013

[15] Nimesh P Vaidya "Digital Watermarking: Data Hiding Techniquesusing DCT-DWT Algorithm" International Journal of Advanced Research in Computer and Communication Engineering, ISSN : 2278-1021, Vol. 2, Issue 6, June 2013.

[16] Reena Anju,"Modified Algorithm for Digital Image WatermarkingUsing Combined DCT and DWT" International Journal of Information and Computation Technology. ISSN:0974-2239, Volume 3, Number 7 (2013), pp. 691-700.

[17] Salma Huusainnaik, A.V. Deshmukh and M. S. Chaugule, “IMPLEMENTATION AND PERFORMANCE ANALYSIS OF DCT-DWT-SVD BASED WATERMARKING ALGORITHMS FOR COLOR IMAGES” in International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE). ISSN(Online) : 2320-9801, Vol.5, Special Issue 4, June 2017.