A Survey on Digital Watermarking with its Techniques, Applications and Performance Measure

Yamini Gupta[1], Nirumpa Tiwari[2]
[1, 2] Department of CSE/IT
[1, 2] SRCEM College, Banmore, India

Abstract- *In today's era, transmissions information over internet have security digital information issue. Hence, secret information protection at the time of transmission becomes a challenging subject. Digital watermarking has provided identifying information or digital data protection against illegitimate allocations or exploitations. Watermarking is a technology to assurance and create possible information certification, security and information copyright defense. The watermarking intend is to involve of hidden information in multimedia knowledge to confirm security analysis. It would then possible to growth the surrounded information, even if the data was distorted through one or extra attacks of non-dangerous. In this paper, we present the numerous kinds of watermarking method and region of application where water creating method need. Also a survey on the few novel work is complete in field of image watermarking.*

Keywords- Digital Watermarking, DCT, DWT, DFT, LSB.

I. INTRODUCTION

Recent advancements in computer technologies offer many facilities for duplication, distribution, creation and manipulation of digital contents. Due to rapid development of network technology, multimedia such as text, image, video and audio has now been widely used [1]. Method of Digital Watermarking is utilized to secure multimedia information that transfer over an internet. Digital Watermarking is a means to implant copyright knowledge into a digital multimedia information for example image, video, audio etc. Digital watermarking is the procedure through which a discrete information stream known as a hidden watermark within a multimedia signal through impressive imperceptible changes on the signal. In numerous proposed methods this process entails the secret key use which must be used to positively set in and mine watermark. Watermarking has increased interest in applications connecting the multimedia signals security. One big driving force for research is the required for efficient scenarios of copyright protection for imagery of digital, video and sound. In the such number application is watermarked into the signal to defend to mark possession. It is expected that an attacker will attempt to eliminate the watermark through intentionally changing watermarked signal. Thus, we necessity strive to mark embed such that it is challenging to eliminate (without the key use) unless the marked signal is meaningfully distorted. In digital watermarking signal is transformed to domain of watermark in which alterations are imposed on domain coefficients to the embed watermark. The improved coefficients are then opposite transformed to create the markings signal1. Our proposed method to enhanced robust watermarking is applicable to the common class of watermarking approaches with following common properties: The watermark information stream binary elements contain. The host signal is not presented or exploited for watermark extraction. The complete watermark is continually embedded right done the signal and all duplication situated watermark in a distinct localized watermark domain region [2].

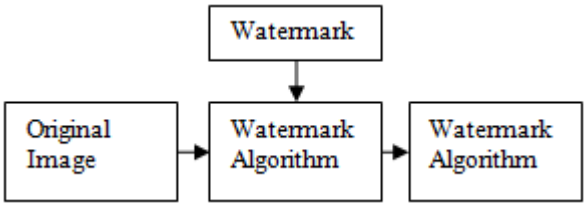

Fig 1: Watermarking Algorithm

II. TECHNIQUES OF WATERMARKING

I. Watermarking is the technique to hide secret data into the digital media applying few appropriate and strong algorithm. Algorithm perform a vital watermarking part as, if ustilised watermarking method is strong and efficient then watermark being embedded applying that method cannot be simply detected. The attacker can only detect or destroy the secret data if know algorithm otherwise it is dangerous to know the watermark. There are numerous algorithms present in the currently scenario that are used to hide the data [3]. Those algorithms come into two various domains.

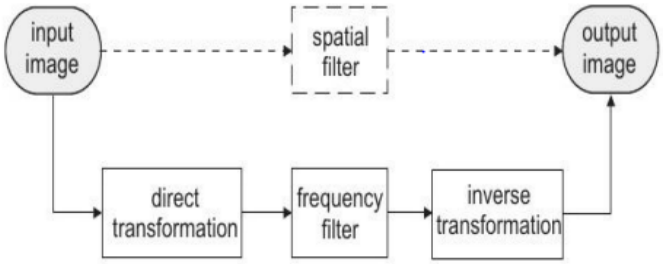

Fig 2. Brief Idea of Spatial and Frequency Domain [5]

A. Spatial domain:

Algorithms of spatial domain in the digital watermarking straight load the raw knowledge into the original image [4]. Spatial watermarking can also be applied applying separation of color. In this way, watermark performs color bands. This renders watermark perceptibly subtle such that it is challenging to detect under regular viewing. Spatial domain is changing or using an image representing an object in space to improve image for a given application. The methods are based on the direct pixels manipulation in an image [10].

a) Least Significant bit (LSB)

In this technique watermark is embedded in the LSB of pixels. Two types of LSB techniques are proposed. In the first method the LSB of the image was replaced with a pseudo-noise (PN) sequence while in the second a PN sequence was added to the LSB. This method is easy to use but not most robust against attacks[6].

b) Patchwork Technique

In patchwork, image points, (a,b) with n pairs,were randomly chosen. The image data in a were lightened while that in b were darkened .High level of robustness against many types of attacks are provided in this technique. But here in this technique, very small amount of information can be hidden[6].

c) Predictive Coding Scheme

In this technique, a PN pattern says W(x, y) is added to cover image. It increases the robustness of watermark by increasing the gain factor. But due to high increment in gain factor, image quality may decrease[6].

B. Frequency domain:

Compared to the spatial-domain approaches, frequency-domain approaches are extra extensively applied. The goal is to embed watermarks in image spectral coefficients. The most usually used transforms are Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), the reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are improved captured through the spectral coefficients [7].

a) Discrete Cosine Transforms (DCT)

First of all image is segmented into non overlapping blocks of 8x8.Then forward DCT is applied to each of these blocks. After that few block selection criteria is applied and then coefficient selection criteria is applied .Then watermark is embedded through altering the selected coefficients and in the end inverse DCT transform is applied on each 8x8 block.

b) Digital Wavelet Transform (DWT):

Discrete Wavelet transform (DWT) is a mathematical tool for hierarchically decomposing an image [8]. It is useful for processing of non-stationary signals. The transform is based on the small waves, called wavelets. Wavelet transform provides both frequency and spatial domain 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 mother wavelet. This section analyses suitability of DWT for image watermarking and gives advantages of using DWT as against other transforms. For 2-D images, using DWT corresponds to image processing through 2-D filters in all dimensions. Filters divide the input image into four various sub-bands LH1, LL1, HH1 and HL1. The sub-band LL1 represents coarse-scale coefficients of DWT, while the sub-bands LH1, HL1and HH1 represent DWT coefficients fine-scale. To find another wavelet coefficient scale, the sub-band LL1 is further deal with until few final scale N is reached. When N is reached we will contain 3N+1 sub-bands multi-resolution sub-bands LHx and LLN, HHx and HLx consisting where x ranges from 1 to N. Because of its properties of excellent spatiofrequency localization, the DWT is most appropriate to areas classify in the host image where is watermark can be embedded efficiently[8].

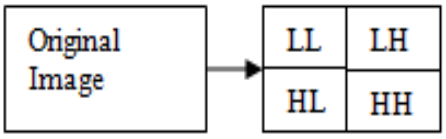

Fig 3: DWT Transform

c) Discrete Fourier transform (DFT):

Transforms a function which is continuous into its frequency components. It has robustness against attacks of geometric for example cropping, scaling, rotation, translation etc. DFT perform translation invariance. Spatial shifts in the image affect phase image representation but not magnitude representation, or circular shifts in spatial domain don't Fourier transform affect.

d) Singular value decomposition:

SVD is a rousing numerical method which is used to diagonally matrices in numerical analysis [9]. In applications change SVD is used as an algorithm. In this SVD transformation, One matrix can dissolved into 3 matrices. These matrices are original matrix Sine tort of significant component, Assume if formula is

$$A \in R^{nXn}$$

where A is a square image, R is the real number domain, Then SVD of A is denoted as

$$A = USV^T$$

Here U and V both are orthogonal matrices, and diagonal matrix is S, as

$$S = \begin{pmatrix} S1 & . & \\ & . & \\ & & Sn \end{pmatrix}$$

Here diagonal components i.e. s's are singular values and satisfy S1≥S2≥…....Sr≥Sr+1≥=……..=Sn=0 SVD is an optimal matrix decomposition method in a least square sense that it grids the vast energy of signal into various coefficients as feasible [10].

Table I. Comparisons of Different Watermarking Techniques[3]

Algorithm	Advantages	Disadvantages
LSB	1. Simply implement and understand 2. Image quality low degradation 3. High perceptual transparency.	1. It lacks common robustness 2. Vulnerable to the noise 3. Vulnerable to cropping, scaling.
Patchwork	1. Robustness of high level against most attacks kind	1. It can hide only most small quantity of knowledge
DCT	1. The watermark is embedded into various middle frequency coefficient, so the visibility of image will not get affected and watermark will not be eliminated through any attack kind.	1. Block wise DCT destroys the invariance system properties.
DWT	1. Permits good localization both in time and spatial frequency domain 2. Higher compression ratio which is relevant to human perception	1. Computing cost may be higher. 2.Longer compression time. 3. Noise/blur near images or video frames edges.
DFT	1. DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions	1. Complex implementation 2. Cost of computing may be higher.

III. PROPERTIES OF WATERMARKING

There are three main Properties of digital watermarking technique[11]:

A. Transparency or Fidelity:

The digital watermark should not affect the original image quality after it is watermarked. Watermarking should not be present visible distortions because if such distortions are introduced it reduces the commercial value of the image.

B. Robustness:

Watermarks could be eliminated unintentionally or intentionally through simple processing of an image operations for example brightness or contrast enhancement, gamma correction etc. Hence watermarks should be robust against variety of numerious attacks.

C. Capacity or Data Payload:

This property defines how much knowledge should be embedded as a watermark to effectively detect at the time of extraction. Watermark should be able to carry enough data to represent the image uniqueness. Various application has various payload requirements [1].

IV. APPLICATIONS OF WATERMARKING[12]

Copyright protection is a method used to the embed ownership rights in a multimedia work through its makers. Watermarking can be used to protective copyrighted material redistribution over untrusted network for example Internet or peer-to-peer (P2P) networks.

Tamper Detection

When database content is used for most critical applications for example medical applications or commercial transactions, it is important to assurance that content was originated from a particular source and that it had not been altered, falsified or manipulated. This can be done by embedding a watermark in the underlying data. Tamper detection is also valuable in court of law where digital images could used as a forensic tool to prove whether image is tampered or not.

Content Authentication is a technique that attempts to confirm media integrity through detecting attempted tampering of the original content. The content is typically watermarked with a semi-fragile watermark, which is designed to be affected through signal transformations. Tampering with content should destroy or alter this semi-fragile watermark, which could then be used to determine that the content is not authentic.

Digital Fingerprinting is a method used to identify digital content owner. Fingerprints are unique to the digital data owner. Hence a single digital content can have various fingerprints because they related to varioua users.

V. DIGITAL WATERMARKING FEATURES[13]

a. Robustness:

Robustness is vital digital watermarking property. In this the digital watermark is always presented in the image after attacks and can be simply visible through owner. It means image which is embedded should be protective against various attacks kinds. An algorithm of better watermarking should be robust against operations of signal processing, geometric attacks for example rotation, scaling and translation and lossy compression

b. Imperceptibility:

This refers to the perceptual similarity in the between watermark image and original image. Through the watermark presence host image quality cannot be destroyed. Invisibility is the most significant watermarked image concern. The embedded watermark in the cover image should not be visible. The capability should be maintained of the cover image.

c. Readability:

It is an essential watermark feature. A watermark should contain as much knowledge as possible.

d. Unambiguous:

The watermark reclamation should unambiguously recognize the data user.

e. Security:

A watermark should be secret and cannot be identity through unauthorized user. Only the authorized user can be accessible the watermark. An unauthorized user cannot be able to change or read watermark.

VI. LITERATURE REVIEW

Shoaib, S. et.al [15] watermarking authenticating is nothing but inserting a secreted object in the order to the detect deceitful alteration through hackers. Object may be in secret password or key terms etc. There are relatively various authentication technique are presented for videos. Present creators in the digital internet and video methodology helps general user to simply create illegal videos copies. In order to solve the problem of copyright protection and deceitful alteration through videos hackers, several watermarking method have been extensively used. Very some watermarking systems authenticating have been created for defining the digital video copyrights. The procedure of Digital watermark knowledge embeds called as a watermark in digital media for example image, video, audio file etc. so that it can for rights claimed. This article presents the full software 3-Level DWT algorithms implementation and to have extra secure information a protective key is used. The secret key is provide to watermark image at the time of embedding procedure and while watermark image extracting same secret key is used. To check watermark video PSNR and MSE effectiveness parameters are used.

Kumar, B et.al [16] This paper presents an algorithm spread-spectrum watermarking for the embedding text watermark in to digital images in the domain of DWT. The algorithm is practical for embedding text file presented in binary arrays applying code of ASCII into host digital image radiological for the potential tele medicine applications. In order to improve the text watermarks robustness for example patient identity code, BCH, ECC is applied to the text watermark ASCII representation before embedding. Algorithm performance is analysed through varying gain factor, subband decomposition levels, and watermark length. Robustness of the method is tested against numerous attacks for example filtering, compression, sharpening, noise, scaling and histogram equalization. Simulation outcomes present that proposed technique attains imperceptible watermarking for string watermarks. It is observed that the BCH code use increases the performance through reducing BER performance.

Benrhouma, O. et.al [17] In this paper, we present a partial encryption and commutative watermarking methods based on the wavelet transformation and also chaotic maps. Commutative property of the proposed technique permits us to cipher a watermarked image without any interfering with the embedded signal or watermark an encrypted image still permitting perfect deciphering. Both operations are achieved in a transform domain given through the DWT transform. Level 1 DWT transformation provide four different coefficients: One approximation coefficient which conclude the most significant image knowledge, and three details coefficients. The basic concept of Our method in to hide the approximation coefficient in the complete details and to encrypt that coefficient considering that it contains extra image information, so the approximation coefficient encryption leads to the whole image encryption.

Rajawat, M.et.al {18] Digital watermarking technique is most inspiring for image security or authentication for attacks. This paper presents digital watermarking for their attacks, application, classification, techniques and also detection f tampering in the digital watermarking. We proposed a novel algorithm for tampering detection and digital watermarking method, through combining these methods, we can increase the image security. We worked on components of RGB for example red, green and blue for increasing robustness and security. 2-DWT applied on RGB components for higher results. In the tampering procedure, we used a watermarked image as a reference image for detecting tampering. The experimental outcomes gave good PSNR value which is reached up to 55%.

In this paper, we have purposed a DWT-PCA based non-blind digital color image watermarking method. We have developed two different algorithms for extraction and embedding procedure. Original image is first DWT-decomposed, and then color watermark is implanted. Before embedding watermark, original image is segmented and principle component analysis is applied. Watermark embedding is applied in various image frequency bands and plots of NC or PSNR are drawn for each frequency bands. PSNR and NC are two different parameters which describe the correlation between the watermarked image and original image. A comparative study of plots of PSNR and NC present that embedding in HL and LH bands is extra robust and imperceptive than LL and HH band. Plots present the robustness of the method against numerous attacks. The basic goal of this paper is to present a method for purpose of copy right protection and colour image information authentification.

VII. PERFORMANCE MEASURES[14]

In order to evaluate the watermarked images performance, there are few feature measures for example BER, SNR, PSNR, and MSE.

a) MSE (mean square error)

It is defined as the average squared variance between an image which is refrence and an image which is distorted image.It is calculated through formula given below X and Y are height and width image respectively.

$$MSE = \frac{1}{MN}\sum\sum\left(W_{ij} - H_{ij}\right)^2$$

Where M,N is height and width in any image, and Hij = Pixel value in host image, Wij = Pixel in watermarked image.

b) Signal to Noise ratio (SNR)

It measures the imaging sensitivity. It measures strength of signal relative to the background noise. It is calculated through the formula :

$$SNR_{db} = \log 10 \log_{10}\left(P_{signal} \div P_{noise}\right)\pi r^2$$

c) PSNR (Peak Signal to Noise Ratio)

It is used to define the degradation in the embedded image with respect to host image .It is calculated as :

$$PSNR = 10\log_{10}\left(L * \frac{L}{MSE}\right)$$

Where L is the PSV of the cover image which is equal to the 255 for 8 bit images.

d) Bit error ratio (BER):

It is the ratio that calculates how numerous bits received in error over the various the complete bits received.

$$BER = \frac{P}{(H * W)}$$

Where, H and W are watermarked image height and width. P is the count number initialized to zero.

VIII. CONCLUSION

In this paper we have introduced three basic techniques for reversible watermarking of digital images, as well as touching on the limitations and possibilities of each. The three types are analysed and compared based on MSE, PSNR and processing time and the result shows that the LSB method is the best and simple technique as compared to the other two techniques because the higher PSNR, enhance the compressed or reconstructed image quality is obtained. For the future, we will try to improve these methods by increasing the payload, visual quality and security.

REFERENCES

[1] Manpreet Kaur, Sheenam Malhotra "Review Paper on Digital Image Watermarking Technique for Robustness" International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 5, May 2014.

[2] Rajni Bala "A Brief Survey on Robust Video Watermarking Techniques" The International Journal Of Engineering And Science (IJES) || Volume || 4 || Issue || 2 || Pages || PP.41-45|| 2015 ||.

[3] Prabhishek Singh, R S Chadha "A Survey of Digital Watermarking Techniques, Applications and Attacks" International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013

[4] Jiang Xuehua, ―Digital Watermarking and Its Application in Image Copyright Protection‖, 2010 International Conference on Intelligent Computation Technology and Automation. http://www.digimarc.com

[5] Deepti Shukla and Nirupama Tiwari "Survey on Digital Watermarking Techniques" International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.8, No.9 (2015), pp.121-126.

[6] Manpreet kaur, Sonia Jindal, Sunny behal, ―A Study of Digital image watermarking‖, Volume2, Issue 2, Feb 2012.

[7] Chaturvedi Navnidhi and Basha S.J, "Comparison of Digital Image watermarking methods DWT and DWT-DCT on the basis of PSNR," International Journal of Innovative Research in Science, Engineering and Technology(IJIRSET), ISSN: 2319-8753, Vol. 1, Issue 2, December 2012.

[8] Jaishri guru , Hemant damecha "A Review of Watermarking Algorithms for Digital Image" International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 9, September 2014.

[9] Mohammad Ibrahim Khan, Md. Maklachur Rahman and Md. Iqbal Hasan Sarker, "Digital Watermarking for Image Authentication Based on Combined DCT,DWT and SVD Transformation"

[10] Neha kalra, Pooja Nagpal "Review paper of digital watermarking" International Journal of Advances in Science and Technology (IJAST) Vol 2 Issue 3(September 2014)

[11] S.Elango , Dr.G.Thirugnanam , R.Shankari "A Survey of Digital Video Watermarking Techniques for Copyright Protection and Authentication" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 4, Issue 4, April 2015

[12] Shivanjali Kashyap "Digital Watermarking Techniques and Various Attacks Study for Copyright Protection" International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 3, March 2015.

[13] Mohan Durvey , Devshri Satyarthi "A Review Paper on Digital Watermarking" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 3, Issue 4, July-August 2014.

[14] Shoaib, S. ; Mahajan, R.C. "Authenticating using secret key in digital video watermarking using 3-level DWT" International Conference on Communication, Information & Computing Technology (ICCICT), 2015 IEEE.

[15] Kumar, B, Kumar, S.B. ;and Chauhan, D.S. "Wavelet based imperceptible medical image watermarking using spread-spectrum" International Conference on Telecommunications and Signal Processing (TSP), 2015 IEEE.

[16] Benrhouma, O. ; Mannai, O. and Hermassi, H. "Digital images watermarking and partial encryption based on DWT transformation and chaotic maps" 12th International Multi-Conference on Systems, Signals & Devices (SSD), 2015 IEEE.

[17] M Rajawat,. ; D.S Tomar,. "A Secure Watermarking and Tampering Detection Technique on RGB Image Using 2 Level DWT" Fifth International Conference on Communication Systems and Network Technologies (CSNT), 2015 IEEE.

[18] A .Kumar,. M. Gupta,. "Semi visible watermarking scheme based on DWT and PCA" International Conference on Green Computing and Internet of Things (ICGCIoT), 2015 IEEE.