International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 3 | Mar -2017 www.irjet.net p-ISSN: 2395-0072

REVIEW ON QUANTUM WATERMARKING TECHNIQUES

Taniya Panjiyar[1], Neha Sharma[2]

[1]Student, Department of Electronics and Communication Engineering, Regional College for Education Research and Technology, Jaipur, Rajasthan, India
[2]Assistant Professor, Department of Electronics and Communication Engineering, Regional College for Education Research and Technology, Jaipur, Rajasthan, India

---

Abstract - *In today's Era, communication broadcasts over the internet have shield difficulties of the digital information. Hence, safety of undisclosed messages through transmission develops a hard issue. Digital watermarking has given that safety of digital information or finding information in contradiction of illegal misuses and sharing. Watermarking is a technology that assures and marks likely data certification, safety and copyright protection of the info. The purpose of watermarking is to contain secreted data in multimedia info to guarantee safety examination. It would be then possible to develop the enclosed info, even if the info was inaccurate by one or extra non-dangerous spasms. In this paper, we present the numerous kinds of watermarking methods and application section where watermarking method is compulsory. Furthermore a study on the some different effort is prepared in image watermarking area.*

Key Words: **Quantum watermarking, Pseudo Random sequence, DCT-DWT and DWT-DCT Algorithm**

1. INTRODUCTION

Security of digital info has become a widespread matter due to the rapid growth of the universal multimedia technology. Copyright safety of digital info has developed an important problem over growing usage of internet. Digital watermarking is that tools that delivers safety, data authentication and copyright safety of the digital info. Digital watermarking is the procedure of inserting secret digital info, signal hooked on the digital media such as image, video, acoustic and text. Later the implanted info is identified and removed out to disclose the actual identity of the digital media. Watermarking is used for Evidence of Rights, Copying Hang-up, data verification, Data Hiding and Recording Monitoring. Digital Image Watermarking technology has numerous uses for safety of digital info, warranty, supply of the digital media and label of the user info. Watermarking of data has developed a very significant area in info hiding. This paper explores the key technologies of Digital Image Watermarking and explores its applications and approaches for the safety sides.

1.1 WATERMARKING BASICS

The simple model of Digital Image Watermarking contains two parts:

1. Watermark embedding

2. Watermark extraction

The first technique is Watermark Embedding that is obtainable in Figure 1 and the second technique is the Watermark Removal that is obtainable in Figure 2.

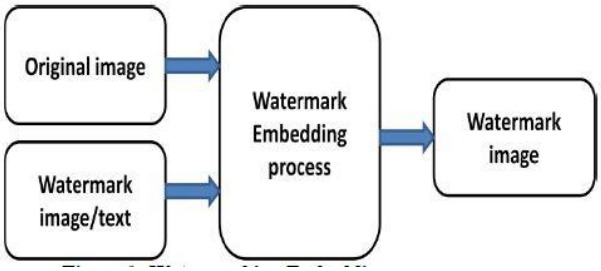

Fig -1: Watermarking Introducing approach

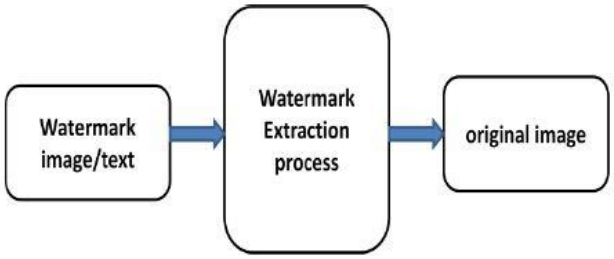

Fig -2: Watermarking Removal Procedure

Watermark Embedding is the method of implanting watermark into the unique image. The yield is the Watermarked image. This procedure is passed out at source's side. Watermark Removal is the Procedure of identifying watermark from the Watermarked image.

1.2 PROPERTIES OF WATERMARKING

The basic necessities of the digital watermarking can be treated as qualities, properties. Different uses require singular properties of watermarking. The different attributes of the watermarking yield different place in application

design. The basic attributes/properties of watermarking are as follow:

A. Robustness Strength refers to that the watermark inserted in data has the ability of perceiving watermark afterward a range of processing procedures and spasms. The watermark should not eliminated by simple treatment methods. Hence watermark should be robust against some spasm. Robust watermarks are intended to fight normal processing.

B. Fidelity
Reliability or Imperceptibility is the most significant condition in watermarking scheme. Watermark cannot be notice by human eyes or ear, only be noticed through different processing of watermark indicator. It can be noticed by an official person only. Such watermarks are used for content or writer authentication and for noticing illegal copies of the data. In other way reliability can be measured as an amount of perceptual ease.

C. Data Payload Data payload states that the quantity of bits implanted into the original image. It is the utmost quantity of info that can be hidden lacking corrupting image quality. It can be calculated by the quantity of secreted information in the original data. This property shows how much info should be embedded as a watermark so that it can be efficiently detected throughout extraction procedure.

D. Security A watermark system is said to be safe, if the unofficial person cannot eliminate the watermark without having packed consciousness of embedding algorithm, detector and arrangement of watermark. The safety is most significant feature of watermarking system. Only the official person can notice watermark. Thus, the copyrights security can attain in watermarking scheme.

E. Computational Complexity Calculation complexity is well-defined as the quantity of time occupied by the watermarking algorithm for embedding and removal procedure. More computational trouble is required for the robust security and validity of the watermark. On the other hand, real-time applications include equally speed and proficiency.

F. Inevitability well-defined as the probability to produce the original data throughout the watermark removal. The optimization of the constraints is equally competitive and cannot be simply done all together. A rational compromise is continuously a requirement. Otherwise, if toughness to strong warp is a subject, the message that can be often secreted need not be excessively long.

1.3 CLASSIFICATION OF WATERMARKING

In this part the digital watermarks, features, their methods and application are categorized and segmented into numerous classes.

1) According to human observation
A. Detectable watermarking

In this kind of watermarking methods the watermark is observable to the casual watcher. Watermark is an image or a data that is noticeable on primary image the watermark seems is a secondary glowing covered into the primary images.

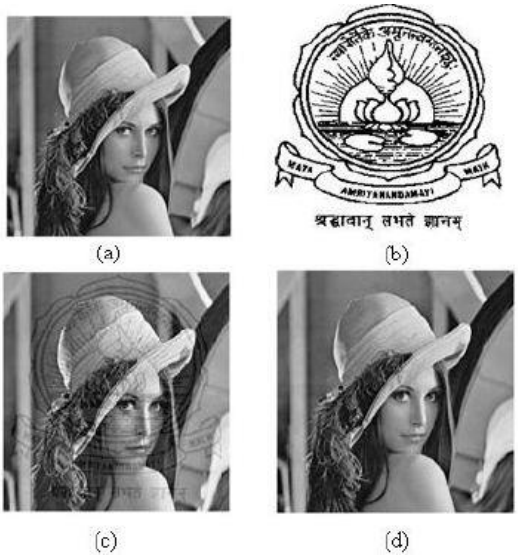

Fig-3: (a) the original Lena copy (b) the symbol to be watermarked (c) observable watermarked image and (d) unseen watermarked image [10]

B. Undetectable watermarking

Undetectable watermark is buried in the original content. It can be noticed by a certified person only. Watermark is implanting in such a way that interchanges made to the pixel content are perceptually not observed and it can be recovered only with suitable decoding process.

1.4 WATERMARKING APPLICATIONS

Applications are listed as:

A. Copyright protection one of the most significant application of watermarking is copyright protection from the illegal person. Ownership of digital media can be recognized in the case of a copyright clash by means of the implanted data as evidence.

B. Broadcast Monitoring This application is used to display illegal broadcast station. It can authenticate whether the content is truly spread or not.

C. Tamper Detection Delicate watermarks are used for loss detection. If the watermark is despoiled or smashed, it displays presence of interfering and hence digital data cannot be trusted.

D. Authentication and Integrity Verification The watermark is implanted to notice if the image has custom-made or not, this process can be used for verification. Reliability verification can be accomplished by means of delicate or semi fragile watermark which has little toughness to amendment in an image.

E. Fingerprinting
The main aim of fingerprinting is to shield clients. If somebody got an authorized copy of a product, but reallocated criminally, fingerprinting can stop this. This can be accomplished by finding the whole transaction by implanting single strong watermark for each receiver.

F. Content Description This watermark can comprise some complete info of the host image for example classification and captioning. The volume of watermark for this kind of application should be comparatively large and there is no harsh requirement of toughness.

G. Medical Applications In medical area the watermarking is important for the purpose of defending the hospital's info from illegal people such as patient's record etc. Security and proof of such data are now becoming very important in medical field where the digital data are effortlessly distributed.

2. PREVIOUS METHEDOLOGY

In 2000, Chen et al.'s [1] projected an adaptive watermarking structure. This system inserts a binary image as watermark in DCT method. The watermarked image is not visible by human visual scheme. It customs a feature based technique to trace the watermark places throughout embedding and extracting. The feature-based technique customs the sobel edge-detector to acquire the gradient magnitude and this outcome is proportional to the quantity of watermark bits. In 2008, Wang H. et al. [2] suggested a chaotic watermarking scheme for authentication of JPEG pictures. The quantized DCT coefficients afterward entropy decoding are plotted to the primary values of the chaotic scheme, and then the produced watermark data by chaotic repetition is inserted into JPEG compressed domain. Re-quantization process does not invalidate interfere recognition due to direct amendment of DCT coefficient after quantization. Removal is also done in the compression area. Extraction is quick and complexity of technique is demanded to underneath. In 2009, Chen et a, [3] suggested a spatial area watermarking method based on the notion of including block-wise dependency info in watermarking process for thwarting VQ spasm without do a deal on localization abilities of the system. The block-wise dependence bond among the chunks of the image is confirmed using fuzzy bunching standards; a fuzzy C-means procedure is used for this method. This technique lets one part of data to belong to two or extra clusters dissimilar other traditional tough clustering systems Like k means algorithm that give data points to a precise cluster. The system consists of validation of message inserting process and tamper recognition process. In 2011, Bhattacharya et al. [4] suggested a new method which creates usage of equally delicate and tough watermarking approaches. The embedded delicate watermark is used to assess the ruin undergone by the transferred images. Strong image features are used to construct the reference watermark from the established image, for judging the amount of ruin of the delicate watermark. In 2011, Yan et al. [5] offered a unseeing watermarking scheme to protect vector geo-spatial data from unlawful use. The presented method is rarely affected by info format alteration, accidental noise, likeness transformation of the data, and info editing. In 2012, Chen et al. [6] proposed a watermarking way based on the frequency area. An enhanced procedure is offered to get the mistake of the JPEG quantification so as to reduce the bit error rate (BER) of the recovered watermark picture. In Addition, two aspects called adjusting factors are used to amend the worth of the DCT coefficient in order to trade-off the potentials amongst the watermarked images and regain watermark. Furthermore, the suggested algorithm is design as a blind mechanism. Hence, the primary image and watermark are not necessary for eliminating watermark. In 2012, Kannammal et al. [7] calculated a digital watermarking framework in which the Electrocardiograph (ECG) and Patients demographic script ID perform as dual watermarks. By this technique the medical info of the patient is secured and mismatching of investigative information is prevented. Alter domain techniques are in greater use now a days in place of spatial field methods as much is known about the properties of these changes to attain better watermark features. In 2012, Chitla Arathi [8] presented a semi-fragile watermarking method based on block based SVD (singular value decomposition).Semi-fragile watermark is delicate to malicious alterations while strong to incidental manipulations .The method can remove the watermark without the original image. SVD alteration conserves both one way and non-symmetric types that are not accessible in DCT and DFT alterations. This scheme can too notice obstruct made on the picture.

3. CONCLUSION

From the above studied papers regarding the watermark techniques and its types and processes, it can be deduced that there are lot of ways by which the target can be achieved or by which the data can be covered behind an image. There has been lot of work which talk about the

watermarking techniques which only talks about the image decomposition techniques and significantly neglects the data hiding, however the data hiding is kept in the midst of the algorithm but not with greater priority.

Quantum watermarking can be the future if developed with the intent of developing the capacity of the existing techniques, however in this paper we have lot many techniques which deals with the intent of increasing the data capacity but only up to a certain limit.

4. REFRENCES

1. Chen, D.-Y., Ouhyoung, M., and Wu, J.-L., "A Shift Resisting Public Watermark System for Protecting Image Processing Software", Proceedings of IEEE Transactions on Consumer Electronics, Vol. 46, No.3,pp.404-414, 2000.

2. Manpreet kaur, Sonia Jindal, Sunny behal, " A Study of Digital image watermarking" , Proceedings of Volume2, Issue 2, Feb 2012.

3. W.-C. Chen,M.-S. Wang, "A Fuzzy c-Means Clustering based Fragile Watermarking Scheme for Image Authentication", Proceedings of Expert Systems with Applications, 2009, Volume 36, Issue 2, Part 1, pp. 1300-1307.

4. Ankan Bhattacharya, Sarbani Palit, Nivedita Chatterjee, and Gourav Roy "Blind assessment of image quality employing fragile watermarking", Proceedings of 7th International Sym. on Image and Signal Processing and Analysis Dubrovnik, Croatia, 2011, pp. 431- 436

5. Haowen Yan, Jonathan Li, Hong Wen, "A key points basesBlind watermarking approach for vector geospatial data", Proceedings of Elsevier Journal of Computers, Environment and Urban Systems, 2012, Volume 35, Issue 6, pp. 485–492.

6. Huang-Chi Chen, Yu-Wen Chang, Rey-Chue Hwang "A Watermarking Technique based on the Frequency Domain", Proceedings of Journal of Multimedia, 2012,Vol. 7, No. 1, pp. 82-89.

7. A. Kannammal, K. Pavithra, S. Subha Rani, "Double Watermarking of Dicom Medical Images using Wavelet Decomposition Technique", Proceedings of European Journal of Scientific Research, 2012, Vol. 70, No. 1, pp. 46-55.

8. Chitla Arathi," A Semi Fragile Image Watermarking Technique Using Block Based SVD", Proceedings of International Journal of Computer Science and Information Technologies, Vol. 3 (2), 2012, 3644-3647.

9. Deng Kai, Wang ke, Lu Changde. "Research of color design method based on 3D semantic space", Computer Engineering and Applications, Vol. 44 (7), pp. 106-108, 2008.

10. Shraddha S. Katariya,2012.Digital Watermarking: Review in International Journal of Engineering and Innovative Technology