An Exploratory Review on Data Protection and Authentication for Digital Watermarking Scheme of Images

Madhu Kumari[1], Ritesh Sadiwala[2]
singhmadhumanoj@yahoo.com[1], ritesh14ci@gmail.com[2]
[1,2]Bhabha College of Engineering, RKDF University, Bhopal, Madhya Pradesh

***Abstract* – The rapid development of digital image processing Researchers used huge volume of data like medical image, satellite image, video image, digital image etc these data are retrieve through digital and electronic media. Digital communication plays a vital role in the world of Internet as well as in the communication technology. The secrecy of the communication is an essential part of passing the data or information. One noticeable technique is Digital Watermarking. Copyright owners seek methods to control and detect such reproduction, and henceforth research on digital product copyright protection has significant practical significance for E-commerce & E-Governance. In this paper, a survey on some previous work done in watermarking field is presented. Experimentally evaluated algorithms are collected to focus on the wide scope of encrypted digital watermarking for data transmission security and authentication.**

***Keywords* – DWT, DCT, Digital Watermarking, PSNR.**

I. INTRODUCTION

The growth of the Internet has been increasing availability of multimedia applications in a number of copyright issues. One of the areas that has fueled this growth is that the digital water. Digital water is the general method of incorporating information bubble in the original file, in order to obtain a variable file. And the media, and therefore included, serves as one of a variety of uses, for example, detect piracy and tampering of the sensor, or the safety of reassuring. Approach to a variety of water and can be substantially classified on the basis of the vision, duration, or frailty. The uses are also versatile, it can also be applied to text, images, audio or video.

With the growth and advances in digital communication technologies, multimedia have become easy to be delivered and exchanged. These forms of digital information can be easily copied and distributed through digital media. These concerns motivated significant research in image and video watermarking fields [1]. Watermarking is used primarily for authentication and ownership protection. New progress in digital technologies, such as compression techniques, has brought new challenges to watermarking. On the other hand,

High efficiency video coding (HEVC) or H.265 standard was introduced officially in 2013, it needs on average only half the bit rate of its predecessor, ITU-T H.264 | MPEG-4 Part 10 'Advanced Video Coding' (AVC), which was considered the most deployed video compression standard worldwide [2].

The new standard is designed to take into consideration advancing screen resolutions and is expected to be phased in as high-end products and services outgrow the limits of current network and display technology [2].

Various watermarking schemes that use different techniques have been proposed over the years [3-8]. To be effective, a watermark must be imperceptible within its host, easily extracted by the owner, and robust to intentional and unintentional distortions [6]. In specific, DWT has wide applications in the area of images and videos watermarking; this is because it has many characteristics and specifications that make the watermarking process robust. Some of these specifications are [4]: Space-frequency localization, Multiresolution representation, Superior Human Visual system (HVS) modeling, and its adaptivity to the original image. A wavelet-based watermarking technique for ownership verification was presented by Y. Wang [9]. It uses orthonormal filter banks that are generated randomly to decompose the host image and embed the watermark in it.

In this paper, our target is to develop a watermarking technique using discrete wavelet decompositions, and integrate it into the high efficiency video coding (HEVC)[10] process. The technique will be used for data hiding in encoded videos to meet the requirements of imperceptibility, robustness, storage requirements, security, and complexity.Digital watermarking is injected to prevent authentication of digital information. Digital watermarking is integrated permanently into host media in form of identification code or image that either visible or invisible and tends to discourage unauthorized copy [2].

If an intruder attempt to damage or temper the water marked digital data, Watermark help to catch the action performed by intruder on the basis of that copyright protection. Watermark having numerous characteristics like Imperceptibility, transparency, secure, and robust in order to server copyright protection, video authentication, and fingerprinting and copy control [3].

II. LITERATURE SURVEY

When digital service [6] is to protect the quality of its service, must focus on the importance of copyright. Digital watermarking is widely used as a mechanism to protect the files posted online. In recent years, the introduction of social networking sites has highlighted the importance of research in the security of digital content. In this study, the characteristics of digital watermarking and the factors that influence the management of digital rights have been used to analyze the needs of providers of online content for the digital rights management.

Digital image watermarking techniques provide a way to secure the rights of the content owner and help in establishing the ownership of the digital images. These techniques add some valuable information in the image in such a way that the perceptual quality of the image remains intact. Various techniques[11,12,15] have been proposed to achieve this purpose. Images are watermarked either at pixel level or transformed into some other transform domains such as Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and DWT, etc. Some techniques use hybrid combinations of these transforms to achieve improved results.

A watermarking scheme should achieve higher values of three major quality parameters, i.e. robustness, imperceptibility and embedding strength of watermark information, which are non-commensurable in nature. Increase in one dimension may result in decrease in another dimension. The watermarking technique should suitably satisfy all the three constraints. Applicability[17] of a technique also depends upon the objective of the watermarking for the particular application on hand. DWT is a popular signal processing technique, now a day's used in various image processing applications. DWT of an image results in four different sub images named as

Approximate, Horizontal, Vertical and Diagonal sub-bands.

They are also represented as LL, LH, HL and HH frequency bands respectively, where L represents low frequency components and H represents high frequency components. Watermarking is done in either one or more of these regions according to the specified method [1, 2].

The results showed that the value of the action, the protection and management are four factors that may be used to analyze the needs of a provider of digital content. In addition, it was found that the online content providers give importance to the management of content they share, and when they share content online, they want to prevent illegal attacks. Several vendors were analyzed and it was found that the women interviewed often share digital content, so they need more digital protective male respondents. Older people[18] were found to be very careful about the value of digital content they publish on-line; they need protection to preserve this value. If the industry of digital content and the Internet can ensure the appropriate digital rights management for users, users will be happy to use it.

In those days,[7] people use social networking sites to share their moments of life like images. And another side

other users can access or download these digital images. Exploit Faker[12] changing and modifying the original image as possible. Change the images can then be downloaded and shared. Illegal use of personal image is subject to copyright. This research work presents an authentication system prototype digital image (DIAS). This system can play on the visible and invisible watermarking image. DIAS is applicable to color images and gray.

The input image can be of any size, and the size of the resulting image would be the same input image. DIAS identifies the property of the digital watermarking[19] with digital. The concept of digital watermarking is used to hide and detect image information. This is the best way to protect the user of copyright. By using watermarking, you cannot blame the forger for the property. This is known as an authentication system for identification of the structure. The complete system consists of two functions, one for the image and hide other information to detect image information. In this approach, the watermark performed using the discrete wavelet transform (DWT) and the results analyzed.

Wireless Sensor Networks (WSN) [8] is an emerging technology and have a great potential for use in critical situations like battlefields and commercial applications such as construction, traffic surveillance, habitat monitoring and smart, and many other scenarios homes. This article discusses the watermarking technique of acoustic signals of vehicles for identification of the vehicle by means of sensor networks. The vehicle identification means identifying the category of vehicle. Here assumes the category can be friend or foe. Watermarking technology[13] has been developed to make the beeps of the vehicle authenticated. Acoustic signals from the vehicle belong to the category of friend are authenticated using a digital watermarking technique and the signals are integrated into digital watermark to represent in a uniform way. Here is the step by step process of integration of the watermarking technology is discussed with the results. After insertion of the technique of digital watermark is done, the resulting signals are then used to identify the vehicle or classification.

In modern times, [9] the rapid growth of the Internet has made the protection of digital content, a critical issue of copyright. A system of digital rights management (DRM) aims to protect high-value digital assets and control the distribution and usage of those digital assets. Watermarking technologies are considered to be a fundamental tool of absolute protection of digital copyright. Digital watermarking is hiding in digital images, the information necessary for the identity of the property to provide protection of copyright. This paper proposes a scheme invisible tattoo blind and innovative for copyright protection of digital images in order to defend themselves against the rights of digital piracy.

In the proposed watermarking scheme, a binary image watermark is invisible built in the image of the host to ensure the protection of copyright. Integration in the watermark, each pixel in the image watermark is embedded in different blocks of the host image size 2a 2 In the proposed watermarking scheme, the watermark extraction process requires only image watermark and does not require the original image or one of its characteristics, and, therefore, the proposed watermarking scheme is blind. The effectiveness of the proposed watermarking system has been demonstrated by the experimental results.

A watermarking scheme should achieve

higher values of three major quality parameters, i.e. robustness, imperceptibility and embedding strength of watermark information, which are non-commensurable in nature.

Increase in one dimension may result in decrease in another dimension. The watermarking technique should suitably satisfy all the three constraints. Applicability of a technique also depends upon the objective of the watermarking for the particular application on hand.

DWT is a popular signal processing technique, now a day's used in various image processing applications. DWT of an image results in four different sub images named as Approximate, Horizontal, Vertical and Diagonal sub-bands.

They are also represented as LL, LH, HL and HH frequency bands respectively, where L represents low frequency components and H represents high frequency components.

Watermarking is done in either one or more of these regions according to the specified method [1, 2]. We, in this work, using the Digital Signature Algorithm (DSA), proposed a new method for integrating non invertibility- in digital watermarking schemes, especially the private digital watermarking schemes. What we propose here is not only a new technique of water, but also a secure system is clear and irreversible, has the characteristics such as the melting time and the use of keys, asymmetric, all this vouchsafed by the use of the lower Digital Signature Algorithm (DSA), a standard that is well known in cryptography.

III. CLASSIFICATION OF WATERMARKING TECHNIQUES

Watermarking approaches might classify on the basis of their inherent characteristics: which are visible and invisible

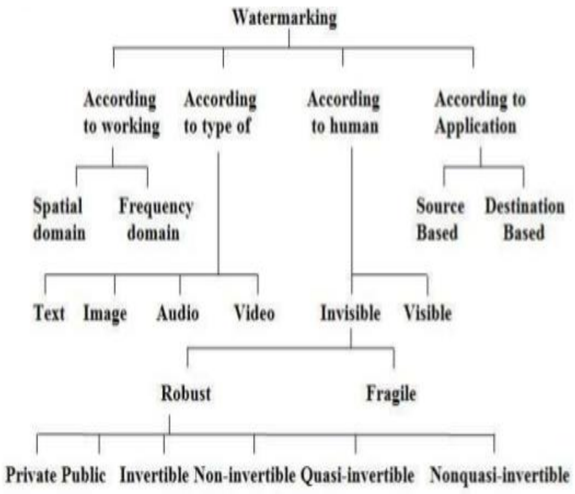

Fig.1. Classification of watermarking

- ***Visible Watermarks*:** In visible watermark or modification of the digital image by applying a "logo" on the image is known as the visible watermark. This approach maps directly to the pre-digital area in which it was printed watermark on the document and the possibility of imposing authenticity.
- ***Invisible Watermarks:*** Despite what might be expected, the watermark is obvious, as the name recommends this is not noticeable generally, and is utilized with an example last. While the conspicuousness of the water makes it undetectable adaptations of licit and illegal particular simple perceivability makes it less reasonable for all applications. Water undetectable spins around the pertinent components which incorporate the acknowledgment of the beneficiaries bona fide, and to recognize the genuine source and non-revocation.

There are numerous different routes so as to arranging the watermarking approaches, these components are bases on use. For instance: hearty, delicate, and spatial some time otherworldly watermarks. furthermore, semi-delicate approach is likewise utilized.

Utilize based characterization of Watermarking are:

- ***Robust watermarks***: Watermarks can be utilized to contain the learning of good. These watermarks require consistency on the first picture to do what they declare. Furthermore, uprightness of the watermark is a measure of the level of its quality. These watermarks must have the capacity to withstand typical treatment of pictures, for example, decreasing the measure of the picture, the picture of misfortune, and change the difference in the pictures, and so forth.

- ***Fragile watermarks***: This is integral to the watermarks capable dream, generally speaking, and more touchy to changes in solid watermarks. Lose their abilities when subjected to even the littlest changes. Utilize is the capacity to stick point the correct zone that has been an adjustment in the first picture watermark. The techniques differ from water evidence delicate and the pseudo-arbitrary succession in dialect LSB division errands to sniff any progressions to the watermark.
- ***Semi-Fragile watermarks***: These sorts of watermarks are in the class of center ground. These are depending amongst delicate and delicate watermarks. They overwhelm the best of both universes and are stronger than delicate ones as far as their power. It is by all accounts that they are superior to strong watermarks.

- ***Spatial watermarks:*** Watermarks which use to apply in

"spatial domain of an image" is known as spatial watermarks [5].

• ***Spectral watermarks***: These are watermarks use to applied in "transform coefficients of the image" called the spectral watermark. [5]

IV. CRITERIA FOR A GOOD WATERMARK

Though watermarks belong to different categories, some of the general characteristics that watermarks must possess are the following [6]:

- Watermark should be binding strongly the image and any changes to the watermark should be visible in the image.

- You should also be able to withstand the changes made in the image watermark 2. These changes include modifications and improvements of image adjustments such as size, cropping, and loss, for example, but not only.

- Watermark must not impair the visual impact of the images through its presence (in particular for the watermarks are not visible).

- Must be indelible watermark, and must be able to survive in linear or nonlinear operations on the image [2].

The following criteria are applicable for the visible watermark: [7]

- The watermark should be clear on all sorts of images.

- The size of the watermark image is an important issue. So the area of watermarked image not possible to modified without tampering to the original image .

- The watermark need to be fairly easy to embed in the host image.

Table 1: Table of Literature Review

Application	Algorithm	Performance
Online Secure ID card Authentication, Online passport Authentication System on Ecommerce model [3]	A Block based algorithm using Hadamard Pattern in spatial domain.	Accuracy is of 99% in average to achieve high quality watermarked images. PS distortion model of halftone effect (variable for scanners and printers) is not required. PSNR ratio is approx. 43 DB
Watermarking Technique applied in a QR code image [2]	Robust Invisible QR Code Image Watermarking Algorithm in SWT Domain (frequency domain)	A novel method to embed the QR code into digital images, lowering the JPEG degradation. It can achieve viable copyright protection and authentication. Most robust to attacks in different considerations. PSNR ratio on various images is approx. 47 DB
Colour Image Watermarking encrypted in QR code [4]	XOR operation for encryption of QR code and watermark, after applying DWT on the Cover image	This algorithm is robust and enhances the security. It does not change the quality of watermarked image. Simple XOR operation is used for encryption. PSNR ratio on various images is approx. 62 DB
Digital Image Watermarking for compressed image format (such as JPEG format) used on the web [5]	Robust and Invisible digital image watermarking algorithm through a 2D barcode and scrambling method based on DWT DFRNT transform. The Watermark extraction process is the inverse of watermark embedding process.	PSNR ratio is approx. 40 DB for various images.
Authentication of Medical Images [6]	Elliptic Curve Cryptography (ECC) algorithm, along with LSB data embedding and through Lossless Watermarking (LWM) Technique.	Lossless Watermarking Image Authentication with high embedding capacity with complete recovery of original images. PSNR ratio is approx. 73 DB for various images.

V. THE WATERMARKING PROCESS

The watermarking procedure includes the accompanying stages [9]:

1. Stage of Embedding
2. Stage of Extraction
3. Stage of Distribution
4. Stage of Decision.

Phase of Embedding: In this stage, the picture pre-handled by the watermark by the President to incorporate. This includes the transformation of the picture to the coveted change. This incorporates discrete cosine change (DCT) and discrete Fourier change (DFT) and wavelet spaces. Watermark to be implanted can be a twofold picture, a bit stream or pseudo-irregular number is locked in, for instance, a Gaussian dispersion. At that point to add to the watermark of the important operations (low-recurrence or middle of the road recurrence) change, as prescribed via looking the human visual framework (HVS). Watermark picture is the executive of this procedure are acquired by playing out the reverse change to adjust the transformation coefficients [9].

Phase of Distribution: Watermark picture acquired above are then conveyed through the advanced channels (on the site). In this procedure, and this was one of a few occasions, for example, the weight, the picture control that decrease picture size, and upgrades, for example, pivot, for instance, yet not just. Subside Meerwald [9] alludes to the above as "Assault of the incident." One of these has built up an arrangement to test the water, as we might find in the accompanying segment. Likewise, malevolent assaults is additionally conceivable at this phase to battle with the watermark. This is shown in the work Meerwald in [9] as "antagonistic assaults". Phase of Extraction: At this stage, an endeavor is made to reestablish the water or the mark of the watermark picture disseminated. This progression may require an uncommon key or a joint open key, in conjunction with the first picture, or only a watermark picture [9].

***Stage of Decision*:** In this phase, with respect to the extracted watermark with the original watermark to check for any differences have developed in the course of distribution. There is a common way to do this is by calculating the distance to exaggerate [9].

VI. CONCLUSION

In this paper, a brief investigation of several works in past decades on digital watermarking (literature review) is done to overview the development of Digital Watermarking Techniques. The encrypted digital watermarking can not only be used for data authentication but also for secured data transmission. The entrusted algorithms with little modification can be used in various fields starting from media industry to medical science and even for e-commerce transaction. The application area of digital watermarking is very wide. And new novel approaches can be sought. The information provided in this paper on this area may help the new researchers to gather knowledge in this domain. Furthermore,
researchers can even improve the existing techniques to make them more effective in various novel applications.

Water marking is a popular scheme among image processing in order to secure the data over image. This paper is an idea about the watermarking and its technique. This paper also throws some light on the previous work of watermarking. Where the PSNR value indicate the visual quality of the image where higher PSNR value lead better image quality. So main research gap need to developed a watermarking scheme which prevent authentication of digital information with maintain higher PSNR ratio also.

REFERENCES

[1] Nasrin M. Makbol, Bee Ee Khoo , Taha H. Rassem," Block-based discrete wavelet transform Singular value decomposition image watermarking scheme using human visual system characteristics" , IET Image Processing, Vol. 10, Iss. 1, pp. 34–52, 2016.

[2] Swathi.K, Ramudu.K,‖ Robust Invisible QR Code Image Watermarking Algorithm in SWT Domain‖, IEEE Transaction on Image Processing Vol.2, Special Issue 4, September 2014

[3] Peyman Rahmati, and Andy Adler, and Thomas Tran. ―Watermarking in E-commerce‖, IEEE Transaction on Circuits and Systems,Vol. 4, No. 6, 2013

[4] Vinita Gupta, Atul Barve, ―Robust and Secured Image Watermarking using DWT and Encryption with QR Codes‖, International Journal of Computer Applications (0975 – 8887)Volume 100 – No.14, August 2014

[5] M. Kim, D. Li, and S. Hong, ―A Robust and Invisible Digital Watermarking Algorithm based on Multiple Transform Method for Image Contents :Proceedings of the World Congress on Engineering and Computer Science 2013 Vol I WCECS 2013, 23-25 October, 2013, San Francisco, USA

[6] Arathi Chitla, M. Chandra Mohan,‖ Authentication of Images through Lossless Watermarking (LWM) Technique with the aid of Elliptic Curve Cryptography (ECC)‖, International Journal of Computer Applications (0975 – 8887) Volume 57– No.6, November 2012

[7] K.Ganesan and Tarun Kumar Guptha, ―Multiple Binary Images Watermarking in Spatial and Frequency Domains, Signal & Image Processing‖ : An International Journal(SIPIJ) Vol.1, No.2, December 2010

[8] Jeng-Shyang Pan, Hao Luo, and Zhe-Ming Lu, ―A Lossless Watermarking Scheme for Halftone Image Authentication‖, IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.2B, February 2006

[9] Gilani, J. and Mir, A.A. "Using Digital Signature Standard Algorithm to Incorporate Non-invertibility in Private Digital Watermarking Techniques", pp 399 – 404, IEEE 2009

[10] Md. Foisal Hussein and Mohammad Reza Alsharif, "Minimum Mean Brightness Error Dynamic Histogram Equalization For Brightness Preserving Image Contrast Enhancement", International Journal of Innovative Computing, Information and Control, vol. 5, no. 10 (A), pp. 3249-3260, October 2009.

[11] Xia odongXie, Zaifeng Shi, Wei Guo, Suying Yao, "An Adaptive Image Enhancement Technique Based on Image Characteristic", 2nd International Congress on Image and Signal Processing, CISP'09, pp. 1-5, Oct. 2009.

[12] HasanDemirel, CagriOzcinar, and Gholamreza Anbarjafari," Satellite Image Contrast Enhancement Using Discrete Wavelet Transform and Singular Value Decomposition", IEEE Geosciences' and Remote Sensing Letters, vol. 7, no. 2, pp. 333-337, April 2010.

[13] Hasanul Kabir, Abdullah Al-Wadud, and OksamChae, "Brightness Preserving Image Contrast Enhancement Using Weighted Mixture of Global and Local Transformation Functions", The International Arab Journal of Information Technology, vol. 7, no. 4, October 2010.

[14] Debdoot Sheet, Hrushikesh Grad, AmitSuveer, Manjunatha Mahadevappa, and Jyotirmoy Chatterjee, "Brightness Preserving Dynamic Fuzzy Histogram Equalization", IEEE Transactions on Consumer Electronics, vol. 56, no. 4, pp. 2475-2480, November 2010.

[15] Wei-Fan Hsieh, Pei-Yu Lin, "Analyze the Digital Watermarking Security Demands for the Facebook Website", IEEE 2012, pp 31-34.

[16] Bhargava, N., Sharma, M.M., Garhwal, A.S. and Mathuria, M., "Digital Image Authentication System Based on Digital Watermarking", IEEE 2012, pp 185-189.

[17] Padmavathi, G., Shanmugapriya, D. and Kalaivani, M., "Digital Watermarking Technique in Vehicle Identification Using Wireless Sensor Networks", IEEE 2010, pp 6-10

[18] Dorairangaswamy, M.A. and Padhmavathi, B. "An Effective Blind Watermarking Scheme for Protecting Rightful Ownership of Digital Images", IEEE 2009, pp 1-6

[19] Gilani, J.and Mir, A.A. "Using Digital Signature Standard Algorithm to Incorporate Non-invertibility in Private Digital Watermarking Techniques", IEEE 2009, pp 399 – 404