International Journal of Scientific Research & Engineering Trends
Volume 1, Issue 6, Nov.-2015, ISSN (Online): 2395-566X

An Art to Protect Originality of Digital Data: Digital Watermarking

Pravesh Chaubey, Ashish Singhadia
Vedica Institute of Technology, Bhopal MP, India
Email: erpravesh9113@gmail.com

***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. But subsequently digital information undergo from copyright and integrity violations problem. Digital watermark play a crucial role to resolve copy rights and ownership violation of digital information. Recently number of watermarking scheme has been proposed but towards more imperceptibility and robustness of host image at receiving is need to be improved. This paper gives a bird's eye over recent research and different methodology of watermarking scheme.**

***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.

Digital Watermarking is an action of hiding a message that an digital signal (eg, images, songs and video) of the signal. It is a concept closely linked hide information, as both hide a message in a digital signal. But what separates them is their goal. Water trying to hide a message in relation to the actual content of a digital signal, hiding information in the digital signal is not related to the letter, and just use it as a cover to hide its presence.

Watermarking is a very active field of research, having number of applications. Even it is a relatively emerging field, has a important methodology to hide messages in digital signals. This can be defining by several models. these models are based on patterns like communication , geometric etc. The rapid development of digital technologies has improved the means of access to information. These new technologies allow us to store, transfer and manage digital content with less time, less complexity and efficiency. However, the analysis also brings disadvantages, such as illegal copying and distribution of digital content. Internet plays an important role in the flow of unauthorized and illegal digital content. [1] This increases the risk of violating copyright owner and prevents the authenticity of digital content. One way to protect digital content against illegal copying and distribution is to include additional information called watermark on it.

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. 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 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 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 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 can not 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 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.

Durability, [10] even if it is recognized as a fundamental property for digital watermarking, is not sufficient to demonstrate the properties of the image. The aim of the attacks is a reflection of creating ambiguity about the authorship of the images. To counter the attacks retroreflective models with strong otherwise tattoos, and not often stressed invertibility of water. 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

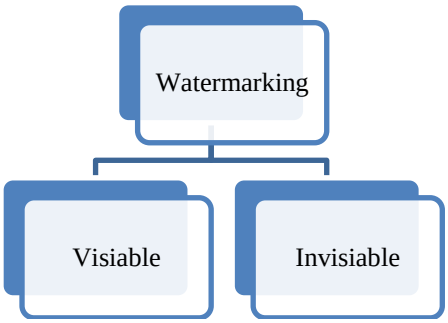

Fig.1. Classification of watermarking

- ***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:*** On the contrary, the watermark is visible, as the name suggests that this is not visible for the most part, and is used with a pattern last. While the obviousness of the water makes it invisible versions of licit and illicit distinctive easy visibility makes it less suitable for all applications. Water invisible revolves around the relevant factors which include the recognition of the recipients authentic, and to identify the real source and non-repudiation.

There are many other ways in order to classifying the watermarking approaches, these factors are bases on usage. For example: robust, fragile, and spatial some time spectral watermarks. and semi-fragile approach is also used.

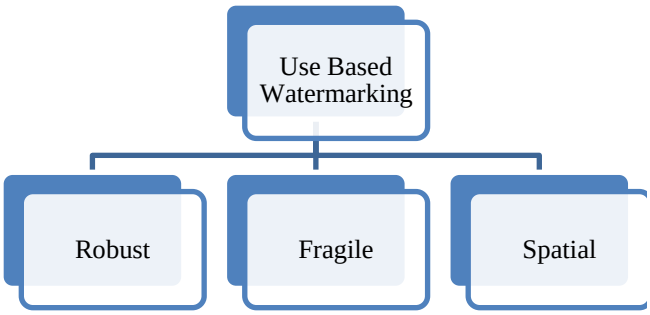

Fig.2. Use based classification of Watermarking

- ***Robust watermarks*:** Watermarks can be used to contain the knowledge of good. These watermarks need consistency on the original image to do what they announce. And integrity of the watermark is a measure of the degree of its strength. These watermarks must be able to withstand normal handling of images, such as reducing the size of the image, the image of loss, and change the contrast in the images, etc.
- ***Fragile watermarks*:** This is complementary to the watermarks powerful illusion, as a rule, and more sensitive to changes in strong watermarks. Lose their skills when subjected to even the smallest changes. Use is the ability to pin-point the exact area that has been a change in the original image watermark. The methods vary from water proof fragile and the pseudo-random sequence in language LSB segmentation tasks to sniff any changes to the watermark.
- ***Semi-fragile watermarks*:** These types of watermarks are in the category of middle ground. These are relying between fragile and fragile watermarks. They engulf the best of both worlds and are more resilient than fragile ones in terms of their robustness. It seems to be that they are better than robust 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.

V. The Watermarking Process

The watermarking process comprises of the following stages [9]:

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

Stage of Embedding: In this phase, the image pre-processed by the watermark by the President to include. This involves the conversion of the image to the desired conversion. This includes discrete cosine transform (DCT) and discrete Fourier transform (DFT) and wavelet domains. Watermark to be embedded can be a binary image, a bit stream or pseudo-random number is engaged, for example, a Gaussian distribution. Then to add to the watermark of the necessary operations (low-frequency or intermediate frequency) conversion, as recommended by searching the human visual system (HVS). Watermark image is the director of this process are obtained by performing the inverse transform to modify the conversion coefficients [9].

***Stage of Distribution*:** Watermark image obtained above are then distributed through the digital channels (on the website). In this process, and this was one of several events, such as the pressure, the image manipulation that reduce image size, and improvements such as rotation, for example, but not only. Peter Meerwald [9] refers to the above as "Attack of the coincidence." One of these has developed a plan to test the water, as we shall see in the following section. In addition, malicious attacks is also possible at this stage to fight with the watermark. This is indicated in the work Meerwald in [9] as "hostile attacks".

***Stage of Extraction*:** At this stage, an attempt is made to restore the water or the signature of the watermark image distributed. This step may need a special key or a joint public key, in conjunction with the original image, or just a watermark image [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

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] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

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

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

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

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

[10] 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