Indo-Iranian Journal of Scientific Research (IIJSR)

(Peer Reviewed Quarterly International Journal) Volume 2, Issue 4, Pages 79-86, Oct-Dec 2018

Analysis of Digital Image Watermarking and its Application

A.Umapriya[1], P.Nagarajan[2]

[1]*PG Scholar, Department of ECE, Vivekanandha College of Engineering for Women, Namakkal, India.*
[2]*Assistant Professor, Department of ECE, Vivekanandha College of Engineering for Women, Namakkal, India.*

Article Received: 29 May 2018 *Article Accepted: 22 September 2018* *Article Published: 06 October 2018*

ABSTRACT

This paper surveys recent advances in watermarking techniques in digital pictures. The aim of digital watermarking is to incorporate imperceptible info in multimedia info to confirm an international intelligence agency or just a labeling application. It might be then attainable to recover the embedded message at any time, albeit the knowledge was altered by one or additional non-destructive attacks, whether malicious or not. Its business applications vary from copyright protection to digital right management. This paper then classifies the various watermarking techniques into several classes relying upon the domain within which the hidden information is inserted; the scale of the hidden information and therefore the requirement of that the hidden information is to be extracted. This paper aims to produce an in depth survey of all watermarking techniques specially focuses on image watermarking varieties and its applications.

Keywords: Watermarking, Copyright Protection.

1. INTRODUCTION

Digital image watermarking is truly derive from Steganography, a method within which digital content is hide with the opposite content for secure transmission of Digital data especially conditions steganography and watermarking at terribly similar once the info to be secure is hidden in method of transmission over some carrier. The main distinction between these two processes is in steganography the hidden information is on highest priority for sender and receiver however in watermarking larva supply image and hidden image, signature or information is on highest priority.

2. WATERMARK PROCESS

The process of watermark contains three processes which are as follows

- ✓ Watermark insertion
- ✓ Watermark extraction
- ✓ Watermark detection

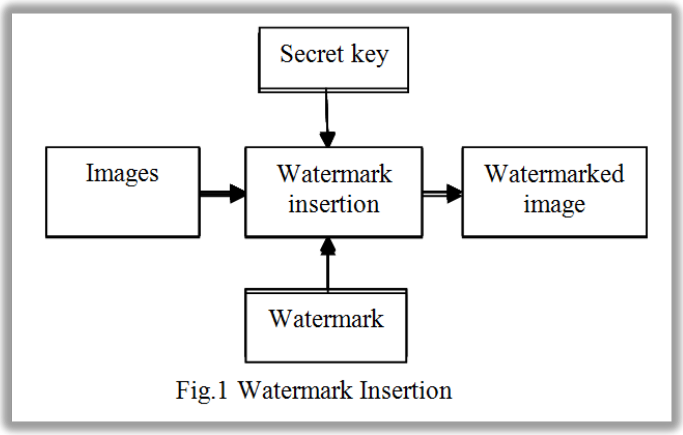

Fig.1 Watermark Insertion

2.1 Watermark Insertion

The watermark insertion process is done by using algorithms. And also we have the secret key for extracting the hidden data from the image [1-11]. Fig.1 shows the watermark insertion process.

2.2 Watermark Extraction

Watermark extraction is the process which is reverse for the insertion algorithm. By using the secret key we can extract the required data [12-25]. Fig.2 shows the watermark extraction process.

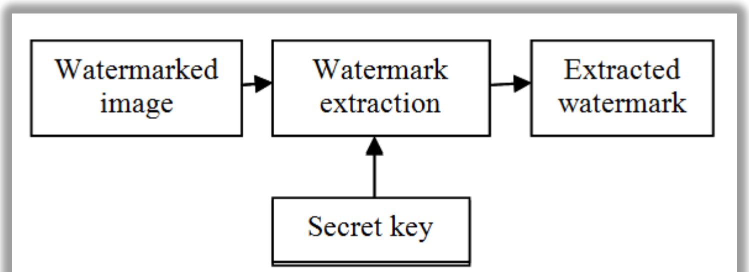

Fig.2 Watermark Extraction

2.3 Watermark Detection

Detection is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, the watermark still is present and it may be extracted.Fig.3 shows the watermark detection.

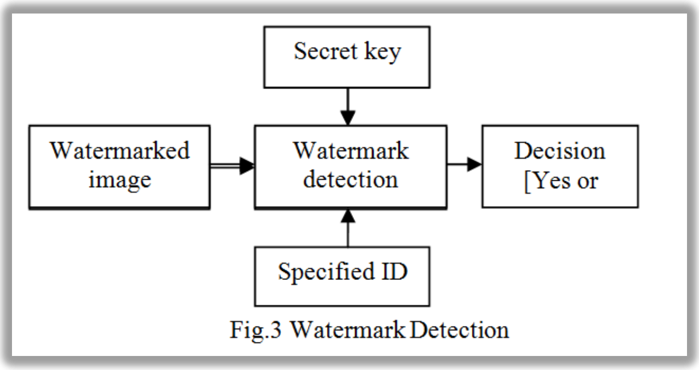

Fig.3 Watermark Detection

3. TYPES OF WATERMARKING SCHEMES

Watermarking scheme contains three types which are as follows

1. Private watermarking
2. Semi-private watermarking
3. Public watermarking

3.1 Private Watermarking

Private watermarking systems use the original cover data to extract the watermark from stego-data and use original cover-data to determine where is the watermark.

3.2 Semi-private Watermarking

Semi-private watermarking doesn't use the original cover data for detection, but tries to answer the same question.

3.3 Public Watermarking

Public watermarking neither cover data nor insertion watermarks are required for extraction-this is the most challenging problem.

4. TECHNIQUES FOR IMAGE WATERMARKING

Digital watermarking is very much popular now a days because it is easily available and it protects our data from illegal use. It has two major areas i.e.

1. Spatial domain watermarking
2. Frequency domain watermarking

In the spatial domain techniques, we embed the watermark by modifying the pixel values. On the other hand, in transform domain watermarking, the watermark is embedded into the coefficients of transform domain. Various types of transform domain techniques are DCT, DWT and DFT. From robustness and imperceptibility point of view, transform domain techniques are better than spatial domain techniques.

4.1 Spatial Domain Watermarking

In Spatial domain, digital watermarking algorithms directly load the raw data into the original image. There should be minor changes in the pixel value intensity. The significant portion of the low-frequency component of images should be modified in order to insert the watermark data in a reliable and robust way. Even if the Spatial domain watermarking is less robust against attacks, its computing speed is higher than transform domain. The spatial domain algorithm are specifically divided into two parts

a. Correlation based Techniques
b. Least Significant Bit

4.1.1 Correlation based Techniques

In this technique, the watermark W(x,y) is added to the original content O(x,y) according to the equation.

$$Ow(x,y) = O(x,y)+ kW(x,y)$$

where k is a gain factor and Ow is the watermarked content. As we increase the value of k, it will expense the quality of watermarked contents.

Advantages

Increases the robustness of watermark by increasing the gain factor.

Disadvantages

Due to very high increment in gain factor, image quality may decrease.

4.1.2 Least Significant Bit

It is an important technique to embed a watermark in the least significant bits of the cover image which are randomly selected pixels. There are two LSB techniques are available. 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.

Advantages

1. Low degradation of image quality
2. Easy to implement and understand
3. High perceptual transparency

Disadvantages

1. Very sensitive to noise
2. Vulnerable to cropping, scaling attacks
3. Very less robust against attacks

4.2 Frequency Domain Watermarking

The main aim of the frequency domain algorithm is to embed the watermarks in the spectral coefficients of the image. The most commonly used transforms are

- ✓ Discrete Cosine Transform (DCT),
- ✓ Discrete Fourier Transform (DFT),
- ✓ Discrete Wavelet Transform (DFT),
- ✓ Singular Value Decomposition (SVD).

4.2.1 Discrete Cosine Transform

It is generally used for the signal processing. In this we transform the image into the frequency domain. It is applied in many areas like pattern recognition, data compression, and image processing. This technique is more robust than spatial domain watermarking techniques. The main steps used in DCT are: Firstly, take the image and divide it into non-overlapping 8*8 blocks. Calculate forward DCT of each of the non-overlapping blocks. Use HVS blocks selection criteria. Now use highest coefficient selection criteria. Then embed watermark in the selected coefficient. Now take inverse DCT transform of each block.

4.2.2 Discrete Fourier Transform

Discrete Fourier Transform (DFT) offers more robustness against geometric attacks like scaling, cropping, translation, rotation, etc. It decomposes an image in sine and cosine form. In this, embedding may be done in two ways: direct embedding and the template based embedding. In the direct embedding technique we modifying DFT magnitude and phase coefficients and then the watermark is embedded. The template based embedding technique introduces the concept of templates. In DFT domain, during embedding process, we embed the template, which is used to find the transformation factor. When the image is transformed, firstly this template is searched and it is then used to resynchronize the image. After this, detector is used to extract the embedded spread spectrum watermark.

4.2.3 Discrete Wavelet Transform

Signal can be analyzed both in time and frequency at the same time by using Wavelet transforms. These wavelets can be termed as non-linear bases of the input signal which can be selected based on the function being approximated. Generally wavelets represents the given signal in terms of the dynamic set of bases functions than static bases families, because dynamic basis represents the signal in efficient way than static bases families. Discrete wavelet transform efficiently identifies the frequency regions of the audio signal where watermark can be embedded effectively. So many watermarking methods use DWT. DWT produces two signals from the input signal, whose length is half of the original input signal, one signal is called as approximate coefficients and other is called as detail coefficients. Where approximate coefficients represent the low frequency part of the input signal, and on other hand details coefficients represent the high frequency coefficient of the signal. The Fig.4 represents the simple one level wavelet decomposition and reconstruction.

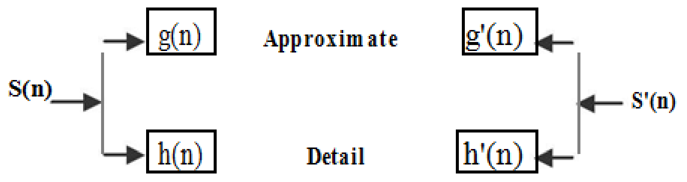

Fig.4 DWT decomposition and reconstruction

Depending on the application and length of the signal, either low frequency or high frequency coefficients can be further decomposed into multiple levels. This application uses four-level DWT and approximate coefficients are used as input for further levels.

4.2.4 Singular Value Decomposition

Singular value decomposition decomposes the input data into three sub matrices.

$$U*S*V^T=SVD(I);$$

Where I is input signal and input signal will be decomposed into left singular vector matrix U, right singular vector matrix V, and the diagonal matrix S, and S has eigen values of the input signal as diagonal elements. These eigen values (singular values) represents the energy of the signal. SVD has so many properties like translation, scaling properties so that it can be used in watermarking applications.

5. ATTACKS

When the watermarked media is transmitted, several attacks take place on that watermarked media. These attacks may be given as:

Removal Attack

In this, the unauthorized user tries to remove the watermark i.e. secret information from the watermarked data.

Interference Attack

In these types of attacks, the noise is inserted to the watermarked media. Some examples of this category are averaging, quantization, compression etc.

Geometric Attack

These types of attacks can change the geometry of the image. The examples of this category are cropping, rotation etc.

Low Pass Filtering Attack

This type of attack takes place when we pass the watermarked data from a low pass filter.

Active Attack

It is the most important attack. Here the unauthorized user tries to extract the watermark or simply makes the watermark such that it cannot be detected by any operation.

Passive Attacks

In this type of attack, unauthorized user simply tries to find out that the particular data contain the watermark or not.

Image Degradation

In these types of attacks, the parts of the image are removed, resulting in damage of robust watermarks. Examples of these attacks are partial cropping, row removal and column removal, insertion of Gaussian noise.

6. APPLICATIONS

Copyright protection

Digital watermarking can be used to identify and protect copyright ownership. Digital content can be embedded with watermarks depicting metadata identifying the copyright owners.

Content archiving

Watermarking can be used to insert digital object identifier or serial number to help archive digital contents like audio, video. Basically digital contents are recognized by their file names; however this is a very fragile technique as file name can be easily changed. So by embedding the object identifier within the object itself, we can reduce the possibility of tampering and hence can be effectively used in archiving systems.

Image and content authentication

With the help of image authentication applications, we can solve the purpose of detecting modification to the data. The characteristic of an image such as its edges are embedded and compared with the current images for differences. This problem can be solved by cryptography, where digital signature has been studied as a message authentication method. One of such technology being used for image authentication is the trustworthy digital camera.

Medical application

We can use digital watermarking for printing name of patient on X-ray reports and MRI scans. This plays an important role in treatment offered to the patient because if there is a mix up in the reports of two patients, this could lead to a disaster.

Tamper detection

By embedding fragile watermarking, digital data can be detected for tampering. If the fragile watermarking got degraded, it indicates the presence of tampering and hence the digital content cannot be trusted. Such type of watermarking can be used to authenticate the content. It is also useful in court of law where digital images could be used as a forensic tool to prove whether the image is tampered or not.

Digital finger printing

Fingerprints are unique to the owner of digital content. It is the characteristic of an object that tend to distinguish it from other small objects. Hence a single digital object can have different fingerprints because they belong to different users. As in the applications of copyright protection, the watermark for finger printing is used to trace authorized users who violate the license agreement and distribute the copyrighted material illegally.

7. CONCLUSION

In this paper, we tend to surveyed the varied aspects for digital watermarking techniques and its applications. A quick and comparative analysis of watermarking technique is additionally given which may facilitate within the new researches in connected areas. We tend to also classified the watermarking algorithms based on spatial and transform domain. Because of area limitation we tend to could not cover enough technical details however we have tried to be as possible.

REFERENCES

[1] Jiang Xuehua,-Digital Watermarking and Its Application in Image Copyright Protection, 2010 International Conference on Intelligent Computation Technology and Automation.

[2] S. S. Gonge and J. W. Bakal, “Robust Digital Watermarking Techniques by Using DCT and Spread Spectrum”, International Journal of Electrical, Electronics and Data Communication, ISSN: 2320-2084, vol. 1, no. 2, (2013).

[3] N. Chandrakar and J. Baggaa,"Performance Comparison of Digital Image Watermarking Techniques: A Survey", International Journal of computer Application Technology and Research, vol. 2, no. 2, (2013), pp. 126-130.

[4] Singh, Surya Pratap, Paresh Rawat, and Sudhir Agrawal "A robust watermarking approach using DCT-DWT." *International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 2, Issue 8* (2012).

[5] Anil Lamba, "Uses Of Cluster Computing Techniques To Perform Big Data Analytics For Smart Grid Automation System", International Journal for Technological Research in Engineering, Volume 1 Issue 7, pp.5804-5808, 2014.

[6] Anil Lamba, “Uses Of Different Cyber Security Service To Prevent Attack On Smart Home Infrastructure", International Journal for Technological Research in Engineering, Volume 1, Issue 11, pp.5809-5813, 2014.

[7] Anil Lamba, "A Role Of Data Mining Analysis To Identify Suspicious Activity Alert System”, International Journal for Technological Research in Engineering, Volume 2 Issue 3, pp.5814-5825, 2014.

[8] Anil Lamba, "To Classify Cyber-Security Threats In Automotive Doming Using Different Assessment Methodologies”, International Journal for Technological Research in Engineering, Volume 3, Issue 3, pp.5831-5836, 2015.

[9] Anil Lamba, “A Study Paper On Security Related Issue Before Adopting Cloud Computing Service Model”, International Journal for Technological Research in Engineering, Volume 3, Issue 4, pp.5837-5840, 2015.

[10] Anil Lamba, "Uses Of Artificial Intelligent Techniques To Build Accurate Models For Intrusion Detection System”, International Journal for Technological Research in Engineering, Volume 2, Issue 12, pp.5826-5830, 2015.

[11] Reddy, R., M. V. N. Prasad, and D. S. Rao. "Robust Digital Watermarking of Images using Wavelets." International Journal of Computer and Electrical Engineering, vol.1, no.2, pp.1793-8163, 2009.

[12] Mei Jiansheng, Li Sukang, “A Digital Watermarking Algorithm Based On DCT and DWT”, Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA’09) Nanchang, P. R. China, May 22-24, 2009, pp. 104-107.

[13] Sang, Jun, and Mohammad S. Alam. "Fragility and robustness of binary-phase-only-filter-based fragile/semifragile digital image watermarking." Instrumentation and Measurement, IEEE Transactions , vol. 57, no.3, pp. 595-606, 2008.

[14] Li, Q., and Cox, I.J, “Using perceptual models to improve fidelity and provide resistance to valumetric scaling for quantization index modulation watermarking”, IEEE Transaction on Information Forensics and Security, Vol.2, no.2,2007, pp.127–139.

[15] Anil Lamba, "Mitigating Zero-Day Attacks In IOT Using A Strategic Framework", International Journal for Technological Research in Engineering, Volume 4, Issue 1, pp.5711-5714, 2016.

[16] Anil Lamba, "Identifying & Mitigating Cyber Security Threats In Vehicular Technologies", International Journal for Technological Research in Engineering, Volume 3, Issue 7, pp.5703-5706, 2016.

[17] Anil Lamba, "S4: A Novel & Secure Method For Enforcing Privacy In Cloud Data Warehouses", International Journal for Technological Research in Engineering, Volume 3, Issue 8, pp.5707-5710, 2016.

[18] Anil Lamba, “Cyber Attack Prevention Using VAPT Tools (Vulnerability Assessment & Penetration Testing)”, Cikitusi Journal for Multidisciplinary Research, Volume 1, Issue 2, July - December, pp.64-71, 2014.

[19] Anil Lamba, “A Through Analysis on Protecting Cyber Threats and Attacks on CPS Embedded Subsystems”, International Journal of Current Engineering and Scientific Research (IJCESR), Volume-1, Issue-3, pp.48-55, 2014.

[20] Anil Lamba, “Analysing Sanitization Technique of Reverse Proxy Framework for Enhancing Database-Security”, International Journal of Information and Computing Science, Volume 1, Issue 1, pp.30-44, 2014.

[21] Anil Lamba, “Enhancing Awareness of Cyber-Security and Cloud Computing using Principles of Game Theory”, International Journal of Advanced in Management, Technology and Engineering Sciences, Volume III, Issue I, pp.71-82, 2013.

[22] Anil Lamba, “Resolve Security Policies Conflicts Through Semantics Matching Alignment”, International Journal of Scientific Research and Review, Volume 2, Issue 2, pp.43-58, 2013.

[23] Anil Lamba, “A Detailed Analysis of Data Security in a cloud Environment”, SURAJ PUNJ Journal for Multidisciplinary Research, Volume 3, Issue 2, pp.43-51, 2013.

[24] Ganic, E and Eskicioglu, AM, “Robust DWT-SVD domain image watermarking: embedding data in all frequencies”, In Proceedings of the ACM Multimedia and Security Workshop, 2004, pp. 166-174.

[25] Suhail, M.A.,and Obaidat, M. S., “Digital watermarking-based DCT and JPEG model”, IEEE Transaction on Instrumentation and Measurement, Vol.52, no.5, 2003, pp.1640–1647.