International Journal of Innovation Sciences and Research
Vol.5, No, 08, pp. 851-854, August 2016

Available online at
http://www.ijisr.com

REVIEW ARTICLE

WATERMARKING TECHNIQUES USED AS A SECURITY FOR DIGITAL IMAGES AND TEXT

***Manpreet Kaur and Vinod Kumar Sharma**

Computer Science and Engineering, Guru Kashi University, Talwandi Sabo, Punjab, India

Accepted 13th July, 2016; Published Online 31st August, 2016

ABSTRACT

Water marking is the art of hiding the fact that communication is taking place, by hiding information in other information. Watermarking is still a challenging research field with many interesting problems such as Robustness to both geometric and nongeometric attacks with blind detection, Other attacks such as protocol attacks and cryptographic attacks , Correct recovery of multiple-bit message, Public-key detection. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exist a large variety of invisible water marking techniques some are more complex than others and all of them have respective strong and weak points. Different applications may require absolute invisibility of the secret information, while others require a large secret message to be hidden. Here in this review of various techniques is discussed. DWT, DCT and LSB used for watermarking to provide protection against unauthorized persons who can make misuse of data or images. LSB method show more clarity on the secret images. DWT-Based watermarking methods are fast /robust and protect against most forms of manipulation. Schemes based on pixel dependency are robust in most forms of image manipulation, but fail when significant pixels are moved from their original location.

Key words: Digital images, invisible, water marking, Robustness, protocol attacks.

INTRODUCTION

Digital watermarking is a technology for embedding various types of information in digital content. In general, information for protecting copyrights and proving the validity of data is embedded as a watermark. A digital watermark is a digital signal or pattern inserted into digital content. The digital content could be a still image, an audio clip, a video clip, a text document, or some form of digital data that the creator or owner would like to protect. The main purpose of the watermark is to identify who the owner of the digital data is, but it can also identify the intended recipient. Why do we need to embed such information in digital content using digital watermark technology? The Internet boom is one of the reasons. It has become easy to connect to the Internet from home computers and obtain or provide various information using the World Wide Web (WWW). All the information handled on the Internet is provided as digital content. Such digital content can be easily copied in a way that makes the new file indistinguishable from the original. Then the content can be reproduced in large quantities. For example, if paper bank notes or stock certificates could be easily copied and used, trust in their authenticity would greatly be reduced, resulting in a big loss. To prevent this, currencies and stock certificates contain watermarks. These watermarks are one of the methods for preventing counterfeit and illegal use. Digital watermarks apply a similar method to digital content. Watermarked content can prove its origin, thereby protecting copyright. A watermark also discourages piracy by silently and psychologically deterring criminals from making illegal copies.

Principle of digital watermarks

A watermark on a bank note has a different transparency than the rest of the note when a light is shined on it. However, this method is useless in the digital world. Currently there are various techniques for embedding digital watermarks. Basically, they all digitally write desired information directly onto images or audio data in such a manner that the images or audio data are not damaged. Embedding a watermark should not result in a significant increase or reduction in the original data. Digital watermarks are added to images or audio data in such a way that they are invisible or inaudible and unidentifiable by human eye or ear. Furthermore, they can be embedded in content with a variety of file formats. Digital watermarking is the content protection method for the multimedia era.

Structure of a digital watermark

The structure of a digital watermark is shown in the following figure 1.1.

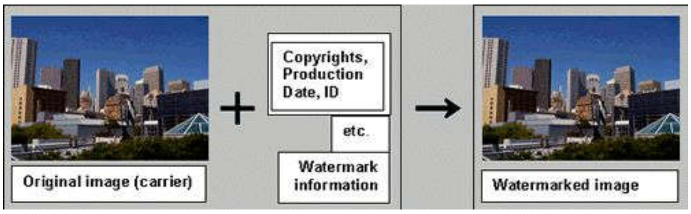


Figure 1. Digital watermark Structure

The material that contains a digital watermark is called a carrier. A digital watermark is not provided as a separate file or

****Corresponding author: Manpreet Kaur***
Computer Science and Engineering, Guru Kashi University,
Talwandi Sabo, Punjab, India.

a link. It is information that is directly embedded in the carrier file. Therefore, simply viewing the carrier image containing it cannot identify the digital watermark. Special software is needed to embed and detect such digital watermarks. Kowa 's Stegano Sign is one of these software packages. Both images and audio data can carry watermarks. A digital watermark can be detected as shown in the following figure 1.2.

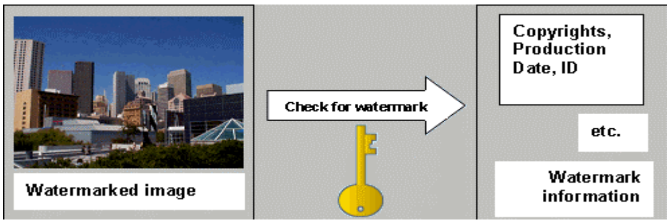


Figure 2. Detection of digital watermark in image

The importance of digital watermarks

The Internet has provided worldwide publishing opportunities to creators of various works, including writers, photographers, musicians and artists. However, these same opportunities provide ease of access to these works, which has resulted in pirating. It is easy to duplicate audio and visual files, and is therefore probable that duplication on the Internet occurs without the rightful owners' permission. An example of an area where copyright protection needs to be enforced is in the on-line music industry.

The Recording Industry Association of America (RIAA) says that the value of illegal copies of music that are distributed over the Internet could reach $2 billion a year. Digital watermarking is being recognized as a way for improving this situation. RIAA reports that "record labels see watermarking as a crucial piece of the copy protection system, whether their music is released over the Internet or on DVD-Audio". They are of the opinion that any encryption system can be broken, sooner or later, and that digital watermarking is needed to indicate who the culprit is. Another scenario in which the enforcement of copyright is needed is in newsgathering. When digital cameras are used to snap-shot an event, the images must be watermarked as they are captured. This is so that later, image's origin and content can be verified. This suggests that there are many applications that could require image watermarking, including Internet imaging, digital libraries, digital cameras, medical imaging, image and video databases, surveillance imaging, video-on-demand systems, and satellite-delivered video.

Types of watermarking

Visible watermarks

A visible watermark is a visible translucent image which is overlaid on the primary image. Perhaps consisting of the logo or seal of the organization which holds the rights to the primary image, it allows the primary image to be viewed, but still marks it clearly as the property of the owning organization.
It is important to overlay the watermark in a way which makes it difficult to remove, if the goal of indicating property rights is to be achieved.

Invisible watermarks

An invisible watermark is an overlaid image which cannot be seen, but which can be detected algorithmically. Different applications of this technology call for two very different types of invisible watermarks:

- A watermark which is destroyed when the image is manipulated digitally in any way may be useful in proving authenticity of an image. If the watermark is still intact, then the image has not been "doctored." If the watermark has been destroyed, then the image has been tampered with. Such a technology might be important, for example, in admitting digital images as evidence in court.
- An invisible watermark which is very resistant to destruction under any image manipulation might be useful in verifying ownership of an image suspected of misappropriation. Digital detection of the watermark would indicate the source of the image.

Information security through watermarking

Essentially, computer and network security have some requirements that should be addressed in order to get secure systems. Thus, in order to determine the performance of a security technology, three key concepts should be analyzed: confidentiality, integrity, and availability. Cole (2003) identifies these concepts as follows:

1. **"Confidentiality deals with protecting, detecting, and deterring the unauthorized disclosure of information".** The main goal of cryptography is to garble a plaintext message in such a way that only the intended recipient can read it. This is precisely the goal of confidentiality.
2. "**Integrity deals with preventing, detecting, and deterring the unauthorized modification of information".** An integrity attack is potentially more dangerous than an confidentiality attack. Cryptography addresses integrity by performing a digital signature check across information.
3. **"Availability relates to preventing, detecting, or deterring the denial of access to critical information".** Cryptography can prevent confidentiality and integrity attacks, but it cannot prevent availability attacks. Cryptography, like any other network security technology, is not a silver bullet. Therefore, it must be combined with other techniques to achieve robust security solution.

In addition to the three key concepts of security, two other security goals are critical relative to cryptography: authentication and non-repudiation (Cole, 2003).

1. **Authentication:** "In most transactions you need to be able to authenticator validate that the people you're dealing with are who they say they are".
2. **Non-repudiation** deals with the ability to prove in a court of law that someone sent something or signed something digitally". Without non repudiation, digital signatures and contracts would be useless.

Attacks

- Removal attacks
- Geometric attacks
- Cryptographic attacks
- Protocol attacks

Lıterature survey

Radhika v. Totla, (2013) author studied about Digital Watermarking as to prevent illegal copying and duplication by methods such as DCT & DWT based algorithms. In this, digital watermarking of images as a technique such as invisible is designed to exploit some aspects of the human visual system. Many of these techniques rely either on transparency (low-amplitude) or frequency sensitivity to ensure the mark's invisibility. The watermark's imperceptibility obtained is more in DWT by using more robust against attacks such as cropping and resizing as compare to DCT.

Vinita Gupta (2014), here author describes that Digital watermarking is the act of hiding a message related to a digital signals in different forms like an image, song, video within the signal itself. In this, a review on Image Watermarking for good Robustness is presented with properties and application area where water making technique need to be used. Here watermarking algorithms based on the transform domain in which the watermark is embedded. Here they shows the different techniques and discusses the important technology called QR code which can be used in future work.

Preeti Parashar (2014), here author said that the digital watermarking is a field of information hiding which hide the crucial information in the original data for protection illegal duplication and distribution of multimedia data. In this, a survey on the existing digital image watermarking techniques is done. The results of various digital image watermarking techniques have been compared on the basis of outputs. The image watermarking techniques may divide on the basis of domain like spatial domain, transform domain or on the basis of wavelets. The spatial domain techniques directly work on the pixels and the frequency domain works on the transform coefficients of the image. In this, survey of different techniques based on spatial domain (LSB) and the transform domain (DCT, DWT, DFT). Digital watermarking is still a challenging research field with many interesting problems, like it does not prevent copying or distribution and also cannot survive in every possible attack. One future research pointer is the development of truly robust, transparent and secure watermarking technique for different digital media including images, video and audio.

Abdullah Bamatraf (2011), here new digital watermarking algorithm using least significant bit (LSB) by inversing the binary values of the watermark text and shifting the watermark according to the odd or even number of pixel coordinates of image before embedding the watermark which is flexible depending on the length of the watermark text. If the length of the watermark text is more than ((MxN)/8)-2 then embedding of the extra watermark text in the second LSB is used. Comparison of an algorithm with the 1-LSB algorithm and Lee's algorithm using Peak signal-to-noise ratio (PSNR). Results in quality of the watermarked image and also attack the watermarked image by using cropping and adding noise and we got good results as well.

Vinayak S. Dhole (2015), Fragile watermarking is worked for authentication and content integrity verification. Here, a modified fragile watermarking technique for image recovery in which detection and recovering of the tampered image with its tampered region as to produce resistance on various attacks like birthday attack, college attack and quantization attacks. Using a non-sequential block chaining and randomized block chaining, created as secrete key which produces tampered regions recovery in great amount worked on color as well as on gray scale images.

Zhou Fu-an (2015), here watermarking technique such as Least Significant Bit and discrete cosine transform are discussed. The DCT is performed on the original host image, and the secret watermark image is embedded into the coefficient of DCT, that replace the least significant bit. The embedded secret watermark bit will cause minimal distortion of the original host image, but we cannot find the difference of the original host image and the watermarked image. The experiment based on this algorithm demonstrates that the watermarking is robust to the common signal processing techniques, including noise attack, JPEG Compression attack and so on.

Madhuri Rajawat (2015), Digital watermarking is a method of combining data into a digital signal with two images such as watermark image, which is cover on the original image (secondary image) that gives security to the image which acts as a digital mark, providing the image a good decision of ownership or authenticity. Author proposed here, a new algorithm for RGB components such as red, green and blue for enhancing security and robustness is worked on 2-DWT. As an experimental results PSNR value which is reached up to 55% have been marked.

MATERIALS AND METHODS

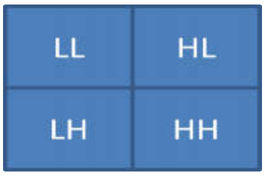
DCT: Used in today's standard JPEG compression. Relation to DFT, Compression explained by previous groups, Image divided into non-overlapping blocks, Each block is DC transformed, Block coefficients are quantized through a special algorithm, Not ideal for human visual system. Formally, the discrete cosine transform (DCT) is a linear, invertible function, F : R^N -> R^N (where R denotes the set of real numbers), or equivalently an invertible N × N square matrix

$$X_k = \sum_{n=0}^{N-1} x_n \cos\left[\frac{\pi}{N}\left(n - \frac{1}{2}\right)k\right] \qquad k = 0, \ldots, N-1.$$

An image is first divided into blocks and DCT is performed on each block. The watermark is then embedded by selectively modifying the middle-frequency DCT coefficients.

DWT: Wavelet Transform: Based on Short Time Fourier Transform (STFT). Becoming more common in compression techniques. Better model of Human Visual System than DCT. The 2D-DWT Transform divides the image into 4 sub-bands:

LL – Lower resolution version of image
LH – Horizontal edge data
HL – Vertical edge data
HH – Diagonal edge data
Most DWT watermarking algorithms embed only in the HL, LH and HH sub-bands



Perform 2D-DWT to divide image into LL, HL, LH and HH sub-bands. Select coefficients from the LL, HL, LH and HH sub-bands that surpass a particular threshold T1, Embed watermarking data via additive modification by **$t'i = ti + \alpha|ti|xi$** where xi = watermark & α = weighting constant, Perform 2D-IDWT to create "watermarked image". DWT Watermarking schemes work well against most forms of image modification, Jpeg Compression, Down-sampling & Up-sampling, Gaussian Noise, and Median Filtering. Technique does not work well in cases of image rotation. Dependent on pixel location.

LSB: The LSB technique is the simplest technique of watermark insertion. Consider a still image: each pixel of the color image has three components — red, green and blue. Allocate 3 bytes for each pixel. Then, each colour has 1 byte, or 8 bits. A pixel that is bright purple in colour can be show N as X0 = {R=255, G=0, B=255}, Look at another pixel: X1 = {R=255, G=0, B=254}, Detecting a difference of 1 on a color scale of 256 is almost impossible for human eye. Replace the color intensity information in the LSB with watermarking information; the image will still look the same to the naked eye. Use a secret key to choose a random set of bits. The more bits used in the host image, the more it deteriorates. Increasing the number of bits used though obviously has a beneficial reaction on the secret image increasing its clarity.

Conclusıon and Future work

The proposed scheme used in this paper encrypts the secret information before embedding it in the image. Steganography and watermarking bring a variety of very important techniques how to hide important information in an undetectable and/or irremovable way in audio and video data. Certainly the time complexity of the overall process increases but at the same time the security achieved at this cost is well worth it. In this invisible watermarking is used with Steganographic techniques. It is not pure Steganographic technique but the effect is same with some additional advantage. First advantage is the data file and reference image is going through the open channel separately. Purpose of Watermarking is to provide Copyright Protection, Fingerprinting, Copy Protection, Broadcasting Monitoring and data Authentication. All these features can be provided with different techniques such as DCT, DWT or LSB using as Steganography. Steganography methods usually do not need to provide strong security against removing or modification of the hidden message. Watermarking methods need to be very robust to attempts to remove or modify a hidden message. LSB method show more clarity on the secret images. DWT-Based watermarking methods are fast /robust and protect against most forms of manipulation. Schemes based on pixel dependency are robust in most forms of image manipulation, but fail when significant pixels are moved from their original location.

REFERENCES

Abdullah Bamatraf, Rosziati Ibrahim and Mohd. Najib Mohd. Salleh, 2011. "A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit", *Journal of Computing*, Volume 3, Issue 4, ISSN 2151-9617.

Madhuri Rajawat, D. S. Tomar, 2015. "A Secure Watermarking and Tampering detection technique on RGB Image using 2 Level DWT", *2015 Fifth International Conference on Communication Systems and Network Technologies*, 978-1-4799-1797-6/15 $31.00 © IEEE.

Preeti Parashar and Rajeev Kumar Singh, 2014. "A Survey: Digital Image Watermarking Techniques", *International Journal of Signal Processing, Image Processing and Pattern Recognition*, Vol. 7, No. 6, pp. 111 -124.

Radhika V. Totla, K.S. Bapat, 2013. "Comparative Analysis of Watermarking in Digital Images Using DCT & DWT", *International Journal of Scientific and Research Publications*, Volume 3, Issue 2, ISSN: 2250-3153.

Vinayak S. Dhole, Nitin N. Patil, 2015. "Self Embedding Fragile Watermarking for Image Tampering Detection and Image Recovery using Self Recovery Blocks", 2015 *International Conference on Computing Communication Control and Automation*, 978-1-4799-6892-3/15 $31.00 © IEEE.

Vinita Gupta and Mr. Atul Barve, 2014. "A Review on Image Watermarking and Its Techniques", *International Journal of Advanced Research in Computer Science and Software Engineering,* Volume 4, Issue 1, ISSN: 2277 128X pp. 92-97.

Zhou Fu-an, 2015. "A Robust Watermarking Scheme Based on Least Significant Bit and Discrete Cosine Transform", *International Journal of Security and Its Applications* Vol. 9, No. 4, pp. 175-184.

****