International Journal of Research in Engineering, Science and Management
Volume-2, Issue-7, July-2019
www.ijresm.com | ISSN (Online): 2581-5792

A Study on Digital Watermarking Techniques

J. Priscilla Sasi[1], P. Arul[2]
[1]*Research Scholar, Department of Computer Science, Government Arts College, Trichy, India*
[2]*AssistantProfessor, Department of Computer Science, Government Arts College, Trichy, India*

***Abstract*: In the recent days, the internet plays a vital role in the data transfer. During such data transmission, there are numerous possibilities of data getting stolen or breached. To avoid such breaches taking place in the data transmission, the watermarking technique plays a major role in the prevention of data stolen. Digital Watermarking is wide and evolving area in the information technology. In this area, various methods are used for sensitive data are being hidden in digital formats such as images, text, audio or video. The secret information is embedded in such methods where the information, which is hidden secretly, is embedded to the host image, which can be extracted with proper authentication mechanism. The extracted data can be used for various purposes like authentication, copyright protection, owner identification and content protection etc. This paper includes the detailed study regarding the types of digital watermarking and its various techniques employed to secure the confidential data. It also has the definition of each classification, domains, how the application works and the threats followed to the application. The study is mainly focused on image watermarking algorithms, applications and its various attacks.**

***Keywords*: Watermarking Types, Classification, Algorithms, Application, Threats.**

1. Introduction

Digital watermarking is the process of hiding a data related to digital signal [1]. Digital Watermarking is a method for embedding the sensitive data into digital content through multimedia Text, Image, Audio or Video formats. Several methods like Cryptography, Steganography are used in data transfers or processing an image file without the content is not being altered [2]. However, this Watermarking technique is mainly used for verifying the reliability of the digital content. The main purpose of the Watermarking is employed for multiple purposes like, copyright protection, hidden communications, broadcasting the videos for news channels and source tracking systems. The objective of the Watermarking is to prevent the host file and protecting the owner identification even though the unauthorized copy of the data is being changed in the original file however, the owner can still prove the originality of the data files [3].

2. Literature survey

R. G. Schyndel et. al. (1994) suggested that Digital watermarking is that technology which is used in hiding information into a digital media like as video, audio and image. In this technique, secret information watermarked and embedded in digital media using some algorithms and the watermarked media is processed and further the secret information watermarked is extracted using some extraction algorithm [4].

I.J. Cox et al (1997) suggest a model in spread spectrum scheme. In this scheme, noise injects into the watermark images. In order to prevent robustness, the watermark is embedded to the images on the most significant portion, so that the original image embedded in the watermark will not be destroyed [10].

Hsu C-T., et al (1999) suggested that Watermarking is used in such a way that the secret information is being hidden through labeling digital pictures in to the images and the watermark is embedded in the visual patterns into the images by modifying the middle frequency of the image [12].

Christine I. Podilchuk et al (2001) suggested that Digital watermarking is used in owner authentication of data and copyright protection. The focus is on watermark embedding and watermark extraction [5].

L. Y. Wang, et al (2002) suggested that new detection algorithms used to detect the signal and to extract the watermark from it. Robust digital watermarking applications are high; the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. However, in fragile digital watermarking, the extraction algorithm should fail if a change is made to the signal [13].

G. Doerr et al (2003) suggested a digital watermarking recently extended to video contents from still pictures. In this method, a video stream is used instead of still images [6].

V. M. Potdar et al (2005) described that watermarking is a method used in which the identification information is inserted into the digital picture which reveals the owner of the digital image. Watermarks can also be embedded into videos or audios that are referred as signals [7].

Mascher-Kampfer et al (2006) suggested, instead of single watermarking, the usage of multiple watermarking could be possible where the robustness seems to be minimal [8].

A. Adelsbach et al (2007) suggested, in multimedia applications, the cryptography method combined with watermarking is used in preventing the data [11].

R. Halder et al (2010) suggested a digital watermarking for relational databases. It gives an idea on providing protection, intrusion detection, culpable tracing, and maintaining integrity of relational data. The current modern approaches for relational

databases are fingerprinting and watermarking. All the methods are categorized based on, some rules they are if the underlying data is distorted, then if the watermark is embedded and then watermark information type. To preventing the ownership distortion and for maintaining integrity of the database distortion watermarking methods are adopted [9].

Kaur G., et al (2013) developed a watermarking technique using Least Significant Bits (LSB). LSB is positioned on watermark for security of the image. However, it is one of the easiest identifier of secret data in the LSB based image watermarking though it is not a reliable technique of image watermarking as it works on spatial domain [14].

Zargar A. J et al (2014) also suggested that watermarking is working with the help of Least Significant Bits (LSB). In this new technique, the double ampersand '&&" operation is being added to the existing LSB of the original watermarked image. It is a simple and helpful in reducing the number of attacks [15].

Kaur S et al (2016) developed a new hybrid technique using SVD-DWT-DCT watermarking. In this concept, the Diagonal components of SVD are embedded in the watermark. Wherein the middle frequency level of DCT technique is used after LH filter applied in the DWT. The robustness is measured using the filter of noise ratio to increase the peak signal at a great rate and reduce the mean square ratio [16].

3. General model of digital watermarking

The sensitive information is hidden in the digital data such as images, text, audios, and videos as signals or messages using specific algorithms related to watermarking. The hidden information is extracted later without being exploited by the cyber criminals using similar algorithm. This technique is mainly used for protecting the authorized data and copyright protection. The process of embedding and extraction process is shown in Fig. 1.

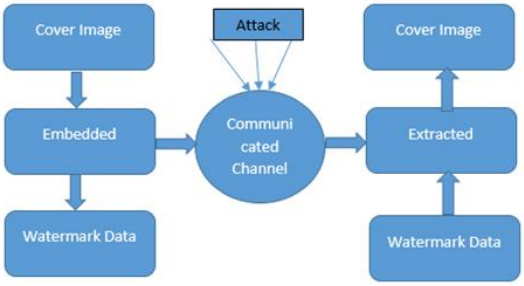

Fig. 1. The working of watermarking

4. Types of digital watermarking

Generally, the Digital Watermarking is mainly divided into major types namely Visible Watermarking and Invisible Watermarking, Robust Watermarking, Fragile Watermarking and Invisible Fragile & Robust Watermarking which can be discussed below.

- *Visible digital watermarking* – where the sensitive data embedded within the watermark is visible as semi-transparent images or textual verbiage that overlaid on the actual image [17].
- *Invisible digital watermarking* – where the sensitive data embedded within the watermark is not visible on the images or textual verbiage that shrouded on the actual image without being affecting the image quality and its properties [18].
- *Robust watermark* - Robustness watermarking scheme is specifically used for copyright information on the digital media in which the watermark is embedded to resists the edit processing and attacks [18].
- *Fragile watermark* - Fragile watermarking is mainly focused on integrity protection where the signal changes are sensitive in nature. The watermark is been identified by the data being tampered according to the state of fragile watermarking [18].
- *Semi fragile watermark* - Semi fragile watermarking is capable of tolerating some degree of the change to a watermarked image, such as the addition of quantization noise compression attacks [18].
- *Invisible-robust watermark* - The invisible-robust watermark is embedding in at pixel level; which are not determined the recovery of this watermark can be done using the decoding algorithm process [18].
- *Invisible-fragile watermark* – In invisible-fragile watermark, the data is embedded with image in such a way that any attacks of the image would alter or destroy the watermark [18].

5. Categories of Watermarking

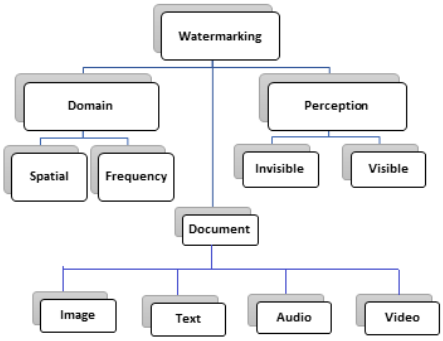

Fig. 2. Classification of digital watermarking

The categories of Watermarking are defined according to document, domain and perception, which are explained in Fig [2].

- *Categories of watermarking* - The Digital Watermarking classification are categorized broadly in the Document types namely Text Watermarking, Image Watermarking, Audio Watermarking, Video Watermarking
- *Text watermarking* - Text Watermarking is one of the useful tool, which helps in the digital security that has the unauthorized alterations in the text contents,

repetitions of texts, and unapproved access to edit the text that cause security breaches.

- *Image watermarking* - Image watermarking is to obscure the copyright information in to the image format and extract the particular information for the author's ownership. The process of Image Watermarking includes embedding the watermark into the original image and extraction of the watermark from the image where the copyright information is hide.
- *Audio watermarking* - Audio watermarking is an electronic signal that is embedded in an audio signal to identify the ownership of the copyright information. In this kind of watermarking, the data inserted in the audio signals through music or any audio formats to embed and used to identify the copyright information.
- *Video watermarking* - Group of digital images or sequence of images that hide the data into the frames of the videos. Here the watermark is clear on the video that consists of the text, image or any copyright information embedded in the video.

6. Domain involved in digital watermarking

Generally, the digital watermarking techniques across all the areas can be categorized under two major domains namely frequency domain and spatial domain. The techniques used in the watermarking are effective and strong where the watermark, which is embedded, cannot be extracted easily. Separate algorithm to extract the secret information is being used in the extraction. There are vital algorithms used which can be classified into two main domains namely frequency domain and spatial domain.

A. *Frequency domain*

Table 1
Advantages of Algorithms in Frequency domain

Algorithm	Advantages	Disadvantages
DCT [Discrete Cosine Transform] *Data transformed in frequency space.*	Robust. Not able to remove by attacks. Used in Image compression	Cannot suppress higher frequency. Susceptible to cropping and scaling
DWT [Discrete Wavelet Transform] *Data transformed as small waves with frequency variation.*	Splits signal in to high and low frequency part High compression ratio Used for two dimensional decomposition Susceptible to cropping and scaling	High cost Takes longer duration Noise present at the edge of the image.
DFT [Discrete Fourier Transform] *Data transforms in frequency components on continuous functions.*	Used to recover from optical distortion	High cost. Gain factor decrease in images. Complex in implementing.

The watermark is embedded in the spectral coefficient of the image. There are number of algorithms describing the Frequency domain, and the advantages, disadvantages of each algorithm are highlighted below. The commonly used algorithms are DCT, DWT, and DFT [19].

B. *Spatial Domain*

The watermarking algorithm used to load the new data into original form of image. It is widely applied in color separation of images, and influences the image based on the direct embedding of watermark in to the pixels of the image. The advantages and disadvantages of the various algorithm used are prescribed below [20].

Table 2
Advantages of Algorithms in Spatial domain

Algorithm	Advantages	Disadvantages
LSB [Least Significant Bit]	Easy to implement. Highly transparent. Low deterioration of image quality.	Not very robust. Sensitive to noise. Cannot be used in practical application.
Correlation	Robust Increase gain factor in images	Image quality decrease due to gain factor increase.
Patchwork	High robust	Can hide smaller information.

7. Applications of digital watermarking

In today's world, various applications may be used in Digital watermarking. They are as follows

- *Copyright* – used to identify the copyright and ownership protection.
- *Source tracking* - Source tracking is the process of identifying and tracking the source of information of every content in the document.
- *Image authentication* – Data embedding and data extraction uses only frequency domain technique
- *Content Management* – This provides a unique identity in all forms of the digital media content.
- *Fraud and Tamper detection* – the data embedded can be detected using fragile watermarking.
- *Broadcast Monitoring* – This is used in major advertisement and commercial broadcasting.

8. Properties and approaches of watermarking

Digital watermarking has some desirable properties and some of these properties might be conflicts to another depending on the application used in the system. The properties consists of three main properties namely,

- *Effectiveness* - This is measured when the probability of the watermark images in the messages are correctly identified.
- *Image fidelity* - The original image is altered and adjusted to an added message and therefore it certainly affects the quality of the image.
- *Payload size* - The size of the message content

embedded in the watermark requires a huge payload to cover up the work.

- *Robustness* - This is an important property in the watermarking concepts like the images, texts after watermarking applied is altered or changed during the transmission or the malicious attacks that try to remove the watermark to have them undetectable. The robust watermark helps to withstand the compression, scanning, printing, rotation, scaling, cropping and in Gaussian noise.

9. Various watermarking attacks

There are various threats intentional or unintentional available in the watermarking system. The main objective of these attacks is to prevent the watermarking from performing the intended purpose. Some of the attacks are as follows.

- *Removal attack* – attacks can be possible when unauthorized user tries to remove the watermark.
- *Low pass filtering attack* – attacks can be possible when the data is passed from low pass filter.
- *Interference attack* – attacks can be possible when the noise is being inserted in the watermark image.
- *Geometric attack* – attacks can be possible when changing the geometric information of the image.
- *Image attack* – attacks can be possible when parts of the images are removed.

10. Conclusion

The digital watermarking is very much helpful in the data authorization and authentication. This paper gives an idea on the analytical study on various types of digital watermarking techniques. Here we have discussed about various types, categories of watermarking techniques and discussed about some of the vital algorithms in frequency and spatial domain. We have studied several pros and cons in frequency domain algorithms however further work will be more focused on extending the algorithms used in frequency and spatial domain.

References

[1] Melinos Averkiou, “Digital watermarking.”
[2] Jian Liu, Xiangjian “A Review Study on Digital Watermarking," Information and Communication Technologies, 2005. ICICT 2005. First International Conference, Page 337 – 341, 27-28 Aug. 2005.
[3] Cox I.J., M.L. Miller, and J.A. Bloom, “Digital Watermarking." 1st edition 2001, San Francisco: Morgan Kaufmann Publisher.
[4] R. G. Schyndel, A. Tirkel, and C. F Osborne, “A Digital Watermark”, Proceedings of IEEE International conference on Image Processing, ICIP-1994, pp. 86-90, 1994.
[5] “Christine I. Podilchuk, Edward J. Delp, Digital watermarking: Algorithms and applications, IEEE Signal Processing Magazine, July 2001.”
[6] G. Doerr and J. L. Dugelay, A guide tour of video watermarking, Signal Process.: Image Commun., vol. 18, no. 4, pp. 263 282, 2003.”
[7] V. M. Potdar, S. Han, and E. Chang, A survey of digital image watermarking techniques, in Proc. 3rd IEEE Int. Conf. Ind. Informat., pp. 709716, 2005.
[8] A. Mascher Kampfer, H. Stogner, and A. Uhl, Multiple re-watermarking scenarios, in Proc. 13th Int. Conf. Syst., Signals, Image Process., pp. 5356, 2006”
[9] R. Halder, S. Pal, and A. Cortesi, Watermarking techniques for relational databases: Survey, classification and comparison, J. Universal Comput. Sci., vol. 16, no. 21, pp. 3164-3190, 2010.”
[10] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Trans. Image Process., vol. 6, no. 12, pp. 1673-1687, Dec. 1997.”
[11] A. Adelsbach, S. Katzenbeisser, and A.-R. Sadeghi, A computational model for watermark robustness, in Proc. 8th Int. Conf. Inf. Hiding, pp. 145-160, 2007.”
[12] C. T. Hsu and J. L. Wu, “Hidden digital watermarks in images,” IEEE Transaction on Image Processing, vol. 8, no. 1, pp. 58-68, 1999.”
[13] L. Y. Wang and P. C. Chen, “On the protection and authentication of digital image based on wavelet transformation,” in Proc. IEEE Region, 10 Conference on Computers, Communications, Control and Power Engineering, 2002, pp. 148-151.”
[14] G. Kaur and K. Kaur, “Image watermarking using LSB (Least Significant Bit),” International Journal of Advance Research in Computer Science and Software Engineering, vol. 3, no. 4, April 2013.
[15] A. J. Zargar, “Digital image watermarking using LSB technique,” International Journal of Scientific & Engineering Research, vol. 5, no. 7, pp. 202-205, July 2014.
[16] S. Kaur and R. K. Sidhu, “Robust digital image watermarking for copyright protection with SVD-DWT-DCT and Kalman filtering,” International Journal Emerging Technologies in Engineering Research, vol. 4, no. 1, pp. 59-63, 2016.
[17] S. C. Shie and S. D. Lin, “Improving robustness of visible image watermarks,” Imaging Science Journal, Vol. 56, no. 1, pp. 23–28, 2008.”
[18] H. B Basanth Kumar,” Digital Image Watermarking: An Overview” Orient. J. Comp. Sci. & Technol., Vol. 9(1), 07-11, 2016.
[19] G. Bouridane. A, M. K. Ibrahim, Digital Image Watermarking Using Balanced Multi wavelets, IEEE Transaction on Signal Processing, vol. 54, no. 4, pp. 1519-1536, 2006.
[20] G. Coatrieux, L. Lecornu, B. Sankur and C. Roux, "A Review of Image Watermarking Applications in Healthcare," *2006 International Conference of the IEEE Engineering in Medicine and Biology Society*, New York, NY, 2006, pp. 4691-4694.