Digital Watermarking: State of The Art and Research Challenges in Health Care & Multimedia Applications

Eelandula Kumaraswamy¹, G Mahesh Kumar², Kommabatla Mahender³, Krishnaveni Bukkapatnam⁴, Ch Rajendra Prasad⁵

¹,²Department of ECE, Sumathi Reddy Institute of Technology for Women, Warangal, Telangana State, India
²,⁵Department of ECE, S R Engineering College, Warangal, Telangana, India
³Bharat Institute of Engineering and Technology, Hyderabad, Telangana, India

¹kumaraswamy441@gmail.com, ²rajendra_prasad_ch@srecwarangal.ac.in, ³kmsharma2@yahoo.co.in

Corresponding Author: Email: kumaraswamy441@gmail.com

Abstract. Nowadays the multimedia data easily available to most people. It is the main cause of illegal access to multimedia content, theft of the intellectual property, easily copying and manipulate the data over the internet, and spreading fake news. With the increase in the availability of the internet to a common man, it is observed that most of the multimedia data misused. Nowadays telemedicine, tele diagnosis, tele consultation, teleradiology, telematic services are necessary. Electronic Patient Record is essential to provide these services. It is necessary to secure the multimedia data by using a suitable watermarking technique. Due to the huge availability of high-speed internet, digital movie piracy was increased rapidly and it causes revenue loss and affects the employment of the people. The high demand for protecting digital videos or movies from unauthorized access. So, it is necessary to protect the intellectual property of the owner, stop unauthorized access of data, also protect and stop the spreading of fake news. In this article, we presented a survey of digital watermarking, bolding its key concepts, embedded and extracted features, state-of-the-art implementation, and research challenges. The primary goal of this article is to provide an improved understanding of the embedding-extracting of watermarking challenges of watermarking and identify important research paths in health care and multimedia applications.
1. Introduction

Digital products piracy and multimedia content copyright dispute is a serious problem nowadays. It is an urgent requirement to find a solution to this problem. Electronic Patient Record (EPR) is used in establishing health care facilities in rural and remote areas. EPR is the important information about the patient, it may attack or distorted or lost may cause loss of important record of the patient. It is necessary to track by using the watermarking technique. Text and image watermarks are embedded in the radiological image for their secure and compact medical image transmission applications. Secure multiple watermarking techniques used for health care applications. The watermarks are used for identity authentication of the medical reports of a patient. The three watermarks are the doctor's signature, patient unique number, and diagnostic information. To reduce the noise effect in the watermark extraction, process a backpropagation neural network technique is used [1].

Security means without proper authentication it is difficult to access the multimedia content and also called protection of the data from unauthorised access. The capability of the technique to oppose the intentional attack of noise is the robustness. Blind watermarking means without the use of the original host image, possible to extract the watermark. Watermarking is the process of embedding secret information in the host (multimedia) like audio, image, or video. The watermark is the secondary data whereas the host is the primary data. Watermark data may be text, image, or video. The host data type may be audio, image, or video file [2]. Hiding the watermark in the host to track and protect the unauthorized access. The watermark is either visible or invisible, where visible watermark best example is TV channel broadcasting, they used a particular TV logo to track the broadcasting and copyright protection. Invisible watermark is not visible by the third party, it is hiding in the host and it can be extracted only authorized persons only.

1.1 Watermark and its strategies

The watermark is embedded in the spatial domain or frequency domain, based on this there are broadly two types of watermarking techniques they are a) Spatial domain watermarking methods b) Transformed or frequency domain methods and all other methods are also listed below.

1.1.1 Spatial domain methods

In this domain there are various methods are available, some of those are as follows

i. Singular Value Decomposition (SVD),
ii. In this proposed method the data is embedded in to the 2D prediction error histogram computed for the rhombus predictor after the image splitting and sorting. The embedding process as follows- the pixels are pairing with one of their neighbours based on the minimum error and for this adaptive pairing is used. At the extraction process- to get the watermark prediction error is added to get the original pixels [3].
iii. A binary watermark is embedded in the blue component of RGB image in the spatial domain [4].
iv. Principal Component Analysis (PCA)
v. Wavelet shrinking and bicubic interpolation with help of spatial correlation. Most of the self-embedding fragile watermarking schemes content recovery and tamper detection are of non-overlapping type only [5].
vi. Single Pixel Imaging (SPI) is an extension of computational ghost imaging (CGI). A time varying (TV) signal hidden in the light source of SPI system to achieve high qualitative image watermarking.

1.1.2 Transformed domain methods

In this domain, there are various techniques are available, some those are as shown below

i. Arnold transform
ii. Discrete Cosine Transform (DCT), DCT has a good property that most of the energy is compacted in few frequency components only.

iii. Discrete Wavelet Transform (DWT)

iv. Wavelet based spread spectrum multiple watermarking technique

v. Coevolution genetic watermarking technique proposed based on wavelet packet transformation. It is very much suitable for distributed computing networks and it has greater applications in the real world [6].

a) DWT-SVD, DCT-DWT-SVD, combine used methods
b) Encrypted domain
c) Multiple watermark methods (more than one watermark that is text and image are used in the host image)
d) Audio watermarking technique- Quantization Index Modulation (QIM) and Singular Value Decomposition (SVD), Visual Attention Model (VAM) based watermarking algorithm has great robustness and imperceptibility. Data embedded in the host according to the visual attentiveness of the regions, modulating the vectors in DCT domain subject to the auditory masking constraint, audio watermarking technique based on Fibonacci numbers. Initially, the FFT spectrum is divided into different short frames and changes the magnitude of selected sample frames using Fibonacci numbers [7].

Spatial domain methods are simpler and efficient than the frequency or transformed domain and compressed methods. In most practical applications the video content is generally compressed form, so the compressed domain watermarking techniques are performed in the transformed domain. Some machine learning techniques are used, and it improves the watermark detection rate.

1.2 Performance measuring parameters
To evaluate the performance of the particular method, various evaluation parameters are used. They are Peak Signal to Noise Ratio (PSNR), Normalizes cross correlation (NCC), Tamper detection rate, Bit accuracy.

1.3 Various types of attacks
The robustness of the proposed method is tested against various attacks, they are Tampering, Text removal attack, text insertion attack, copy and paste attack, vector quantization (VQ) attack, JPEG compression, cropping and adding noise, gaussian noise, low pass filtering, additive noise attack, cropping attack, scaling attack, rotation attack, random bending attack, resizing.

2. Research Challenges
The various research challenges in the field of digital watermarking are listed below

i. Theatrical content protection and online copy control is a serious issue nowadays. Imperceptibility and robust watermarking techniques are challenging tasks. Illegal distribution of video content from theatres is protected or monitored by issuing a special key or watermark to each theatre. The copying of the movie’s contents unauthorized way by the poorly supervised movie theatres only. That caused illegal copies distributed over the internet by mass production of duplicate copies.

a. A Human Vision System has less sensitive to Chrominance distortion than the luminance distortion so the watermark is embedded in the chrominance channel adds enough enhance the robustness of the watermarking technique

b. Protecting 3D videos from illegal distribution is also important in the present day because there is a demand for 3D videos also. Designing the multi view videos and their watermarking techniques are the future interest in the watermarking domain [8].
ii. Robustness, imperceptibility and watermark embedding capacity are the major factor in any watermarking technique. The literature survey concludes that attaining all at the same time is difficult. Design an algorithm to attain robustness, imperceptibility, and security. (or improve the performance with respect to these).

iii. Wireless Sensor Networks need new techniques for the security, piracy, digital right management and usage measurement improvement. Both static and functional watermarking techniques can be used to collect data from network depending on types sensors and actuators deployed (audio, video, and measured data).

iv. The study regarding switching from one set of sensors to another where one set of sensors has high accuracy but vulnerable to attacks and the second set of sensors has low accuracy but cannot be attacked [9-12].

Future scope: Develop a generalized attack model to detect the various possible attacks and design a robust controller in the regime of when attack is detected.

v. IOT applications has been used in secure and sensitive sectors like military and health. In these areas sensory data is more important while decision-making process. It is necessary to provide security to the sensory data. Sensors has limited computational and power resources. These limitations create a challenging task to create a secure mechanism. A false data injections attacks are very crucial in sensory networks where small alteration lead to a severe consequence. So, it is important to provide a filtering to detect the false data injection attack.

Future scope: The proposed method provides solution for the stated problem with certain extension and it is need to solve the energy related issues in future.

vi. Geometric attacks and various other types of distortion are overcome by designing a watermarking technique using deep convolutional neural network. A deep neural network had made tremendous progress in multimedia. Training a neural network requires a large amount of data and time. It is good to use trained models by fine tuning the step helps to reduce the computational cost and improves the performance. Therefore, sharing the trained models enhances the growth in research and development. At the same time the trained model is the research asset of the owner. In this process, it is necessary to authenticate ownership of the trained neural network based on watermarking. It is observed that fine tuning caused less alteration when the watermark is embedded near the input layer compared to near the output layer. Limitations while inserting a watermark in the deep neural network is 1. Distillation is a theoretically serious problem but practically seems to be less risky. 2. Overwriting is destroying the original watermark, overwriting still a service attack. 3.Block box type situation: a client-server system where a watermark model is used on the server by unauthorized persons. 4. Embedding is a sequential task: First training the original task and the second task is embedding the watermark in the model. After embedding there is an increase in the error rate is called catastrophic forgetting. 5. Compressing deep neural network is an important and active research topic. 6. Network morphism is a severe attack on the embedded watermark. 7. Steganalysis is the method to detect the watermark in the file (audio, video, data in this case it is the deep neural network model). The proposed model is robust to the steganalysis. In future scope, design an effective steganalysis to detect the embedded watermark in the deep neural network [13].

vii. Investigate and develop a new watermark technique to resist – stealing a model and robust for all other types of attacks.

viii. Need to implement secure digital watermarking techniques for e-governance applications and tele medical applications. Two different watermarks are embedded in the cover page to enhance the robustness and security also it reduces the storage space, transmission bandwidth and transmission time for tele medical services.

However, computational complexity of the proposed method needs to reduce in future research.

Future scope- develop lossless data hiding techniques for medical applications. The application areas of the proposed methods are secure digital multimedia data over social networks, e-health, e-voting system, digital cinema, education and insurance companies etc [14-16].
enhancement of the robustness is possible by using back propagation neural network (BPNN) it also addresses the channel noise distortion.

Future work- Minimize the computational complexity for color image watermarking, also extend the work for video watermarking.

ix. Need to develop an adaptive watermarking method, which focus to improve the robustness of the watermark, it resists for geometric attacks and all other attacks with low computational cost.

x. Develop a readily available watermark extractable and embeddable methods for all real time applications. Improve the performance of the method in robustness, imperceptible, embedding capacity, and computational complexities and security requirements [17,18].

3. Conclusion
Digital watermarking has recently emerged as an entrancing criterion for protecting multimedia and delivering health care services over the Internet. A huge rise in the availability of the internet to people. It turns to protect and improve the security of the multimedia data by using enhanced watermarking techniques. However, despite the techniques provides the necessary protection to the multimedia data and health care services, the current technological facilities are not maturing enough to realize its full potential. Many key challenges in the digital watermarking domain, including robust to various attacks to the watermarking techniques, copyright protection, health care and multimedia applications, online movie protection, are some of the research areas to start research and a lot of scope for improving the watermarking techniques.

Therefore, we believe there is still tremendous opportunity for researchers to make ground breaking contributions in this field, and bring significant impact to their development in the health care and multimedia applications. In this paper, we have surveyed the state-of-the-art of digital watermarking, covering its essential concepts, various domain-based embedding and extracting techniques, prominent characteristics, key attacks, performance parameters as well as research directions. As the development of watermarking techniques is still at an early stage, we hope our work will provide a better understanding of the research challenges of digital watermarking, and pave the way for further research in this area.

References:
[1] Agarwal, N., Singh, A. K., & Singh, P. K. (2019). Survey of robust and imperceptible watermarking. Multimedia Tools and Applications, 78(7), 8603-8633.
[2] Bhowmik, D., Oakes, M., & Abhayaratne, C. (2016). Visual attention-based image watermarking. IEEE Access, 4, 8002-8018.
[3] Chen, Y. H., & Huang, H. C. (2015). Co-evolutionary genetic watermarking for owner identification. Neural Computing and Applications, 26(2), 291-8.
[4] Dragoi, I. C., & Coltuc, D. (2016). Adaptive pairing reversible watermarking. IEEE Transactions on Image Processing, 25(5), 2420-22.
[5] Ernawan, F., & Kabir, M. N. (2018). A robust image watermarking technique with an optimal DCT-psychovisual threshold. IEEE Access, 6, 20464-80.
[6] Fallahpour, M., & Megías, D. Audio watermarking based on Fibonacci numbers. IEEE/ACM Transactions on Audio, Speech, and Language Processing, 23(8), 1273-82.
[7] Guo, J., Zheng, P., & Huang, J. Secure watermarking scheme against watermark attacks in the encrypted domain. Journal of Visual Communication and Image Representation, 30, 125-35.
[8] Hu, H. T., & Hsu, L. Y. (2015). Robust, transparent and high-capacity audio watermarking in DCT domain. Signal Processing, 109, 226-235.
[9] Hwang, M. J., Lee, J., Lee, M., & Kang, H. G. (2017). SVD-based adaptive QIM watermarking on stereo audio signals. IEEE Transactions on Multimedia, 20(1), 45-54.
[10] Jiao, S., Zhou, C., Shi, Y., Zou, W., & Li, X. (2019). Review on optical image hiding and watermarking techniques. *Optics & Laser Technology, 109*, 370-380.

[11] Kumar, C., Singh, A. K., & Kumar, P. (2018). A recent survey on image watermarking techniques and its application in e-governance. *Multimedia Tools and Applications, 77*(3), 3597-3622.

[12] Nagai, Y., Uchida, Y., Sakazawa, S., & Satoh, S. I. (2018). Digital watermarking for deep neural networks. *International Journal of Multimedia Information Retrieval, 7*(1), 3-16.

[13] Merugu S, Juluru TK and Srinivas S 2019 Adaptive compressive sensing of images using adaptive block compressive sensing algorithm and improvement *International Journal of Innovative Technology and Exploring Engineering* 8(5) 1055-1060.

[14] Jhansi Rani G, Raghava Kumari D, Anitha M and Sarita B 2020 Analysis of raspberry pi based ATM theft monitoring and security system *International Journal of Psychosocial Rehabilitation* 24(8) 15376-15383 10.37200/IJPR/V24I8/PR281514.

[15] Anitha M., Jhansi Rani G., Raghava Kumara D and Anuradha P. 2020 Implementation of arithmetic logic unit using quaternary signed digit number system *International Journal of Psychosocial Rehabilitation* 24(8) 15363-15375 10.37200/IJPR/V24I8/PR281513.

[16] Raghava Kumari D, Anitha M, Jhansi Rani G and Ramesh Babu D 2020 Road traffic control by using Li-Fi technology between vehicle to vehicle communications *International Journal of Psychosocial Rehabilitation* 24(8) 15393-15397 10.37200/IJPR/V24I8/PR281516.

[17] Swathi N, Padmaja Ch and Navya Jyothi G 2020 Audio assistive for blind people to identify the cloth patterns and colors *Journal of Critical Reviews* 7(17) 154-158 10.31838/jcr.07.17.23.

[18] Mahender K, Ramesh KS and Kumar TA 2017 An efficient ofdm system with reduced paper for combating multipath fading *Journal of Advanced Research in Dynamical and Control Systems* 9(Special issue 14) 1939-1948.