Digital Image Watermarking Techniques

Subjects: Computer Science, Information Systems
Contributor: Mahbuba Begum, Mohammad Shorif Uddin

Image authentication is an extremely significant concern for the digital revolution, as it is easy to alter any image. In the last few decades, it has been an urgent concern for researchers to ensure the authenticity of digital images. Based on the desired applications, several suitable watermarking techniques have been developed to mitigate this concern. However, it is tough to achieve a watermarking system that is simultaneously robust and secure. This paper gives details of standard watermarking system frameworks and lists some standard requirements that are used in designing watermarking techniques for several distinct applications. The current trends of digital image watermarking techniques are also reviewed to find state-of-the-art methods and their limitations. Some conventional attacks are discussed, and future research directions are given.

Keywords: LSB ; DCT ; DFT ; DWT ; SVD

1. Introduction

Image processing and the internet have made it easier to duplicate, modify, reproduce, and distribute digital images at low cost and with approximately immediate delivery without any degradation of quality. Network technology has been developing and progressing so quickly that it threatens the privacy and security of data. Therefore, content authentication, copyright protection, and protection against duplication play an essential role in facing the challenges of the existing and upcoming threats in maintaining digital information. Digital image watermarking is simply the digital watermarking of an image, which provides an alternative solution for ensuring tamper-resistance, the ownership of intellectual property, and reinforcing the security of multimedia documents. Any digital content, such as images, audio, and videos, can hide data. Digital content can easily be illegally possessed, duplicated, and distributed through a physical transmission medium during communications, information processing, and data storage. Digital image watermarking is a technique in which watermark data is embedded into a multimedia product and, later, is extracted from or detected in the watermarked product. These methods ensure tamper-resistance, authentication, content verification, and integration of the image [1]. It is not very easy to eliminate a watermark by displaying or converting the watermarked data into other file formats. Therefore, after an attack, it is possible to obtain information about the transformation from the watermark. To discern the difference between digital watermarking and other technologies such as encryption is essential [2]. Digital-to-analog conversion, compression, file format changes, re-encryption, and decryption can also be survived through digital image watermarking techniques. These tasks make it an alternative (or complementary) to cryptography. The information is embedded in the content and cannot be removed by normal usage [3].

The word “steganography” is derived from the Greek word “steganos.” This technique conceals communication and changes an image such that only the sender and the intended receiver can identify the sent message. This technique makes detection a more difficult task. Instead of encrypting messages, steganography can be used to hide them in other inoffensive-looking objects, so their existence is not discovered and, therefore, can be used as an alternative tool for privacy and security. However, due to the rapid proliferation of internet and computer networks, steganography can be used as a tool for exchanging information and planning terrorist attacks [3]. Steganography hides the existence of a cover image, while a watermarking technique embeds a message into the actual content of the digital signal within the signal itself. Therefore, an eavesdropper cannot remove or replace a message to obtain an output message. To protect content from unauthorized access, embedding information into the original image is essential. Digital image watermarking is imperceptible and hard to remove by unauthorized persons. The technique has been implemented by various algorithms using the spatial and frequency domains, each having their distinct benefits and boundaries.

2. Design Requirements of Image Watermarking System

Digital image watermarking techniques add a watermark into multimedia data to ensure authenticity and to protecting a copyright holder from the unauthorized manipulation of their data [4]. Hence, it is necessary to define the requirements or characteristics of a watermarking system. Figure 1 illustrates the requirements of watermarking techniques. Based on applications, these requirements evaluate the performance of watermarking systems.

Figure 1: Design requirements for an image watermarking system.

3. Summary of the State-of-the-Art Watermarking Techniques

Used Techniques	Factors	Advantages	Limitations	Applications
DCT and Fractal Encoding [5]	Robustness	Better robustness, -Good PSNR, -Improves security	Higher computational complexity	Copyright ownership
SCDFT and QFT [6]	Robustness, imperceptibility	Robust against geometric transformations, Gaussian noise, and image enhancement, -Maximizes imperceptibility	Not robust against JPEG compression and color conversion, -Higher computational complexity	Copy control and transaction tracking
DWT and QR Decomposition [7]	Robustness, imperceptibility	Robust against compression, cropping, filtering, and noise adding, -Better imperceptibility,	Less robust against salt-and-pepper noise and cropping	Copyright protection
SVD and Redistributed image normalization [8]	Robustness and security	Solves false positive detection problem, -Better robustness and imperceptibility	Does not work for color images	Ownership identification, medical image watermarking, and fingerprinting

4. Digital Image Watermarking Applications

Digital image watermarking is a highly focused research area, due to its potential use in media applications such as copyright protection, annotation, privacy control, data authentication, device control, media forensics, and medical reports (e.g., X-rays). Some associated applications of digital image watermarking are shown in Figure 2.

Figure 2. Related applications of digital image watermarking.

5. Challenges of Image Watermarking Methods

At present, information is an asset. With the advent of computers, the usage of multimedia technology is increasing daily. This makes the tasks of protecting information from being accessed by unauthorized parties (confidentiality), ensuring the authenticity of information and protecting against unauthorized changes (integrity), and confirming that information is accessible by authorized users (availability) more challenging. These are the three key security requirements of a system, which are very difficult and challenging to implement. Moreover, robustness, imperceptibility, and capacity are the essential requirements in designing a good watermarking system. However, an important trait is that the watermarking system should be robust enough against various intentional attacks such as: elimination attack, collusion attack, remodulation attack, interference attacks, noise attacks, geometric attack, ambiguity attack, or a copy attack, etc.

However, keeping a balance among these three conflicting requirements is a difficult task. Imperceptibility can be achieved by embedding a watermark in the high-frequency components; however, this task produces weaker robustness, as robustness occurs in the low-frequency components. Still, security is a big challenge in digital image watermarking. More recently, internet of things (IoT)-based authentication schemes have provided supreme security without human interaction [9], where more encryption can be done outside the image contents. Furthermore, blockchain-based authentication schemes also provide high levels of security. Blockchain technology stores data in a decentralized manner and completely protects data against any tampering [10]. It also detects forgery and differentiates the original image from the tampered image. Therefore, these two schemes can be accommodated in the watermark domain.

6. Conclusions

At present, information can be duplicated easily due to the interactive and digital communication of multimedia data. This issue makes digital image watermarking a significant field of research. Digital image watermarking using various techniques for image authentication, integrity verification, tamper detection, copyright protection, and the digital security of an image. In this study, we reviewed the most dominant state-of-the-art watermarking techniques. Through this study, it can be concluded that DWT is a high-quality and robust technique for image watermarking due to its multi-resolution characteristics. Though robustness, imperceptibility, and capacity are the essential requirements in designing an efficient watermarking system, however, it is almost impossible to achieve all of these requirements simultaneously. Therefore, a good trade-off between these three requirements must be maintained. Still security remains a big challenge in digital image watermarking technologies, and the accommodation of IoT and blockchain-based authentication schemes provides a challenge for researchers. Therefore, future work can be focused on developing new and advanced techniques as well as by combining various techniques in different domains to fulfill the above three important requirements.

References

1. Tao, H.; Chongmin, L.; Zain, J.M.; Abdalla; Robust Image Watermarking Theories and Techniques: A Review. *J. Appl. Res. Technol* **2014**, *12*, 122-138, .
2. Zhang, Y. Digital Watermarking Technology: A Review. In Proceedings of the ETP International Conference on Future Computer and Communication, Wuhan, China, 6–7 June 2009; pp. 250–252.
3. Cox, I.; Miller, M.; Bloom, J.; Fridrich, J.; Kalker, T. Digital Watermarking and Steganography; The Morgan Kaufmann Series in Multimedia Information and Systems: Burlington, Massachusetts , 2008; pp. 1-13.
4. Pun, C.M. High Capacity and Robust Digital Image Watermarking. In Proceedings of the 5th International Joint Conference on INC, IMS and IDC, Seoul, South Korea, 25–27 August 2009; pp. 1457–1461.
5. Liu, S.; Pan, Z.; Song, H; Digital ImageWatermarking Method Based on DCT and Fractal Encoding. *IET Image Process* **2017**, *11*, 815-821, .
6. Tsui, T.K.; Zhang, X.; Androutsos, D; Color ImageWatermarking Using Multidimensional Fourier Transforms. *IEEE Trans. Inf. Forensics Secur.* **2008**, *3*, 16-28, .
7. Jia, S.; Zhou, Q.; Zhou, H; A Novel Color Image Watermarking Scheme Based on DWT and QR Decomposition. *A Novel Color Image Watermarking Scheme Based on DWT and QR Decomposition.* **2017**, *20*, 193-200, .
8. Ali, M.; Ahn, C.W.; Pant, M.; Siarry, P; A Reliable Image Watermarking Scheme Based on Redistributed Image Normalization and SVD.. *Discret. Dyn. Nat. Soc.* **2016**, *2016*, 1-15, .
9. El-hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni; A Survey of Internet of Things (IoT) Authentication Schemes. *Sensors* **2019**, *19*, 1141, .
10. Dobre, R.A.; Preda, R.O.; Oprea, C.C.; Pirnog, I. Authentication of JPEG Images on the Blockchain. In Proceedings of the International Conference on Control, Artificial Intelligence, Robotics & Optimization (ICCAIRO), Prague, Czech Republic, 19–21 May 2018; pp. 211–215.
