

A Review of Digital Image Watermarking Technology

Yangkai Zhou

College of Computer and Communication, Lanzhou University of Technology, Lanzhou, China

Abstract. In recent times, the concern surrounding multimedia security has grown more prominent. With the development of network technology and multimedia technology, a large number of enterprises in China have emerged with streaming media technology as their core business. These enterprises have a good development trend and broad prospects, which has attracted more and more freelancers and organizations to participate in multimedia creation. Various media forms, including images, videos, audio files, and text files, are progressively losing their reliability due to their susceptibility to distortion or alteration through tampering tools. Therefore, maintaining the authenticity and integrity of digital media has become the primary goal. Multimedia data also presents various challenges, including unauthorized distribution, information overload, and alteration of the content it represents. In this paper, watermarking methods are categorized according to their distinct operational mechanisms. The discussion also covered attacks, applications and requirements related to watermarking technology. Watermarks don't just keep the content from being changed. They can also offer data integrity and content verification. By adding information about the original signal to the image, watermarking technology improves the security of the original image.

1 Introduction

Nowadays, it is hard to imagine a world without images. With the advancement of technology, the forms of digital data include various types such as text, video, and more. However, some editing tools have been maliciously exploited by certain individuals, which has led to a copyright controversy. Meanwhile, as a relatively intuitive form of information in communication and exchange, images are widely used in daily life, such as medical images and military maps. If the content of an image is maliciously modified or damaged, not only will its original value be lost, but it may also trigger copyright disputes. Throughout the day, people come into contact with various images, which exist in different places such as television, magazines, websites, newspapers, and books [1]. Digital image processing has a variety of applications beyond analogue image processing. Operations such as enhancing image quality, filtering noise, segmentation, and restoration can be performed on digital images. A digital image can be defined as a two-dimensional image with finite numerical values and is also known as pixels or image elements. Digital data is

zhouyangkai@lsu.edu.gn

confronted with numerous issues related to data privacy and security. Efficient security technologies are needed to prevent the illegal use of data. Due to the rapid development of technology, various multi-functional software has emerged. The digital media has been properly modified. People's attitude towards multimedia is deteriorating. Therefore, in accordance with the demands of the majority, the developers have taken corresponding measures to protect the relevant data. In order to prevent the modification of various indicators of digital data, developers have successively developed a variety of technologies. For example, password encryption, digital watermarking technology The ability to collect information is the key to an organization's success. Whether it can effectively prevent other users from accessing and modifying the information generated by its operation and processes is also a matter of concern. The convenient access to digital storage devices and the wide use of the Internet have made the generation and dissemination of digital materials extremely easy. Therefore, it has become imperative to formulate strategies to combat copyright infringement [2]. The implementation of digital watermarking technology is an essential part of digital image processing and a widely used technique, which is suitable for situations where organizations want to prevent data from being released into the public domain. When a business has a direct trust relationship with its clients and needs to protect their information, it is absolutely necessary to adopt digital image watermarking technology [2]. There are many ways to hide and control data, but among them, the most practical method is to use digital image watermarking. Several watermarking techniques are available to conceal secret information in digital data like text, audio, and video. In order to protect the ownership of digital content, researchers from all over the world are constantly innovating and reforming, hoping to greatly enhance their control over digital data. Through this series of developments, the probability of illegal possession, malicious tampering and dissemination of various literature resources and media data has been significantly reduced [3]. Thanks to digital image watermarking technology, it's easy to attach secret data to cover images, which can later be used for different purposes like identifying the owner, copyright protection, authentication, and content protection.

This article mainly introduces the basic model of digital watermarking technology, its core characteristics and classification, as well as the attack types of digital image watermarking algorithms, and the current application directions and contents of digital image watermarking.

2 The Basic Model of Digital Image Watermarking Technology

The basic model (as its name suggests) aims to represent the fundamental scenarios of image watermarking applications. We first determine the basic components of the watermarking scheme and their possible inputs and outputs. Regardless of the system and security requirements, as shown in Figure 1, a watermarking scheme can consist of three basic components. To systematically define them, three functions are considered in this paper: watermark generation, denoted as *a*; embedding, denoted as *b*; and detection, denoted as *c*. To represent different data (such as inputs and outputs) in this context, in the following sections, we will use capital letters to denote these data.

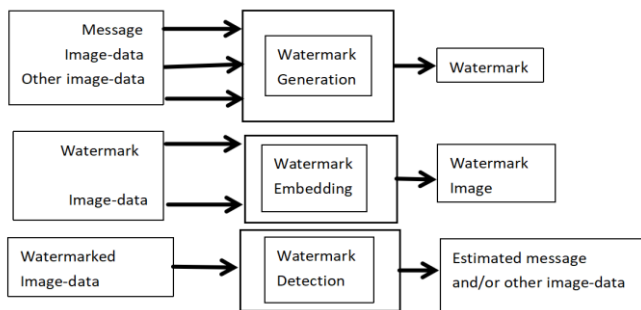


Figure 1. Fundamental components of image watermarking (Picture credit: Original)

Figure 2 shows digital watermark embedding process:

- 1)Watermark information generation: Generate a digital watermark containing specific information as required.
- 2)Watermark embedding: Embed digital watermarks into the digital signals that need protection, such as audio, video and images, etc.

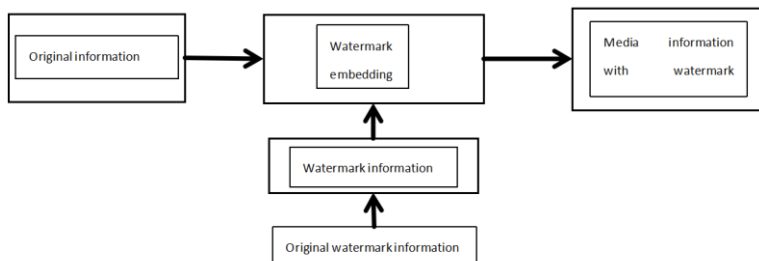


Figure 2. Digital Watermark Embedding Process (Picture credit: Original)

3)Watermark detection: Input of watermark, watermark image data, and original image data leads to the output of estimated information or other image data. Estimation of information or restoration of related image data is possible through the detection of the watermark embedded in the image during the watermark detection process.

3 The Basic Model of Digital Image Watermarking Technology

3.1 Transparency

The transparency of watermarks mainly refers to the fact that there is no obvious visual change to the human eye in a digital image after watermark information is embedded compared to before the embedding. Additionally, transparency is also demonstrated in that the original watermark cannot be recovered even by statistical methods. Here it should be pointed out that, to achieve transparency, a protected digital image needs to be used. The watermark should not detract from the image's visual appeal, but it should not be completely hidden either.

3.2 Robustness

The ability to extract a clear copyright image from the carrier image, regardless of network noise or slight tampering, is often referred to as robustness. Digital watermarking has always been a challenge in terms of robustness. Most watermarking algorithms can only demonstrate strong robustness against one type of attack. However, for other attacks, the effect is not good. In the existing literature, the main methods used to improve the robustness of the algorithm mainly include the discrete wavelet transform, discrete wavelet transformation (DWT) [4], Curvelet transform [5] and singular value decomposition singular value decomposition (SVD) [6].

3.3 Safety

The security issue arises because the carrier image embedded with watermark information needs to be transmitted over the network, and the embedding algorithm is usually public. When the carrier image is intercepted by lawbreakers, the copyright information might be extracted, which would cause the algorithm to lose its purpose of copyright protection. Therefore, the security of copyright information is usually also one of the essential characteristics that digital image watermarking algorithms must possess. According to the current watermarking algorithm, the security of the data is enhanced through encryption processing. The commonly used scrambling methods mainly include Arnold Shuffle [5], Chaotic mapping [6], Visual password [7], etc. As for the literature [8], before embedding the copyright information, perform a scrambling operation on the copyright information. Due to the unpredictability of the chaotic mapping with random periodization can improve the security of copyright information to a certain extent.

3.4 False Alarm Rate

The false alarm rate is mainly used to evaluate the reliability of detection algorithms. After information hiding is completed, by using other similar algorithms or carriers to extract similar copyright information, the extracted results are similar in form to the original information, they may actually contain a large amount of inaccurate or misleading data, thereby increasing the risk of false alarms. otherwise, it is the opposite. Especially in zero watermarking technology, in order to reduce the false alarm rate, it is necessary to construct carrier features with strong uniqueness. Therefore, this indicator is commonly used to measure the false alarm rate of zero watermarking.

4 Classification of Digital Image Watermarking Algorithms

4.1 Based on Spatial Domain

4.1.1 Least Significant Bit

Least Significant Bit (LSB) Digital Watermarking, it is also known as the least significant bit, referring to the lowest bit when the pixel values of a digital image are represented in binary form. To replace watermark information with watermark pixels at the lower-left corner of digital images is the objective of digital watermarking [9]. The watermark information and pixel values are both binary bit sequences. If each pixel value of a grayscale image is represented by 8-bit binary numbers, changing the value of the lowest

bit will not have a significant impact on the visual effect. The embedding process is shown in Figure 3. Taking a 3×3-sized block image as an example, the watermark information {0,1,1,0,0,0,1,0,0} is embedded into it using the LSB watermarking algorithm.

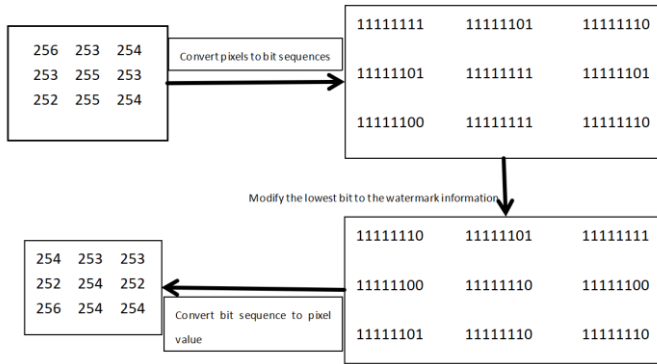


Figure 3. The embedding process (Picture credit: Original)

The extraction of watermark information merely requires converting the corresponding pixel values into binary bit sequences, and then extracting the lowest bit of each bit sequence. This method of extracting watermarks belongs to blind detection, meaning that all watermark information can be extracted without the need for the data of the original carrier image. Precisely because the extraction algorithm is simple, this kind of watermark can be easily extracted by malicious parties and modified into other information. Encrypting or scrambling the watermark information before embedding can help improve the security of the watermark. In this way, without the key, obtaining accurate watermark information is impossible. From the perspective of the embedding process of LSB watermarking algorithm, since the embedding position is the lowest significant bit, it has poor resistance to noise and the embedding position is fixed, thus it is vulnerable to attacks. In response to the above shortcomings, the researchers have proposed some improved LSB algorithms. In terms of pixel selection, they have implemented encryption for embedding watermarks. Watermarks can be embedded in odd-numbered rows or even-numbered rows, and they can also be embedded by randomly selecting pixel values according to the key. The improved LSB algorithm has been enhanced in terms of security and robustness.

4.1.2 Digital watermarking in binary images

A binary image refers to an image that has been processed from an input image with multiple grey levels to one with only two grey levels [10]. The pixel values of a binary image are only two numbers, 0 and 1.0 represent black and 1 represents white. As a result, a binary image is also called a black-and-white image. Embedding watermark information is possible by changing the parity of the number of black and white pixels. When the embedded watermark bit is 0, adjust the chosen pixels to ensure an even count of black pixels. In cases where the embedded watermark is 1, the system enforces an odd distribution of black pixels in the selected region. Decoding the watermark involves assessing whether black pixels appear an odd or even number of times.

4.1.3 Digital watermarking based on image features

Digital watermarking algorithms based on image features include watermarking algorithms that analyze image luminance values. There are also watermarking algorithms based on

image statistical features. Utilizing statistical features, they are a kind of important embedding techniques in spatial domain embedding algorithms. The main idea is to modify the original image data so that certain statistical features of the original image change. During detection, only the statistical features of the watermarked image need to be examined. This is to achieve the purpose of blind detection [11]. The acquisition of these statistical features requires key control to ensure their security. Commonly used statistical features include the average value, standard deviation and histogram.

4.2 Based on the Frequency Domain

4.2.1 Digital Watermarking Based on DCT Domain

Digital watermarking based on DCT domain is a common digital image watermarking technology. It takes advantage of the properties of DCT (Discrete Cosine Transform) transformation and embeds watermark information into the frequency domain of digital media. DCT is a transformation method that can convert time-domain signals or images to the frequency domain. It decomposes signals or images into a series of frequency components, and these components are arranged in ascending order of frequency from low to high.

The forward transform of DCT:

$$C(n, m) = a(u)a(v) \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} f(x, y) \cos\left(\pi n \frac{2x+1}{2N}\right) \quad (1)$$

Inverse Transform of DCT:

$$f(n, m) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} a(u)a(v)C(x, y) \cos\left(\pi n \frac{2x+1}{2N}\right) \cos\left(\pi m \frac{2y+1}{2N}\right) \quad (2)$$

Among them,

$$a(u) = \begin{cases} \sqrt{\frac{1}{N}}, u = 0 \\ \sqrt{\frac{2}{N}}, u = 1, 2, \dots, N-1 \end{cases} \quad (3)$$

4.2.2 Digital Watermarking Based on DWT Domain

Digital watermarking based on DWT domain is a common digital image watermarking technique. It takes advantage of the properties of DWT (Discrete Wavelet Transform) transformation and embeds watermark information into the frequency domain of digital media. DWT is a transformation method, similar to DCT, which performs spectral transformation of temporal signals or two-dimensional images. The difference is that DWT uses wavelet functions as basis functions instead of cosine functions. It can simultaneously provide a lot of useful information in both time domain and frequency domain.

5 Analysis of Watermarking Techniques in Different Domains

Following an extensive analysis of multiple spatial-domain processing methods, it is concluded that spatial domain processing techniques are simple and have low complexity,

and are only applicable to identity verification. They have lower costs and can embed more bits of information, thus having a powerful capacity. If LSB technology is combined with other technologies, only when both are combined can good performance be demonstrated. However, these methods have relatively weak resistance to different types of attacks.

Building upon the evaluation of multiple frequency-domain manipulation techniques, it is concluded that the technology in this field is more complex, involves a large amount of overhead, and has higher costs. In frequency domain technology, since it will reduce image quality, it is impossible to embed more information bits in the coefficients. The primary objective of digital watermarking technology in this domain is to ensure copyright protection while maintaining resilience against multiple attack vectors. The application of distortion techniques typically generates problematic visual artifacts. Findings indicate that combining large-capacity approaches with strongly robust techniques represents the optimal solution for balancing distortion reduction and capacity improvement.

The purpose of using image watermarking technology imposes several requirements on the algorithm. Multiple criteria are adopted to measure the robustness and quality of the embedded watermarks. Primary assessment parameters involve unnoticeable embedding, resistance to various attacks, information capacity, operational speed, and security. An assessment must provide a certain degree of guarantee for all the selected requirements. Therefore, in order to evaluate these functions separately, each requirement has several guarantee levels. Moreover, for each level of each specific function, some standards have been assigned. However, the number of guarantee levels cannot be accurately selected. A large number of guarantee levels will make the assessment extremely complicated and unusable for some purposes.

6 Attacks on Digital Image Watermarking Algorithms

According to relevant data, it is still possible for most people to extract and tamper with watermarked data. Therefore, there will be some obstacles. Therefore, the watermarking system should have high resistance to attacks. In a watermarking system [12]. Any process that could lead to the detection of a watermark as harmful or the communication conveyed by the watermark being compromised is known as an attack in a watermarking system.

The watermark detection function is exploited by hackers to delete or destroy it, which is the cause of the active attack. Merely by accessing the watermark embedding function, attackers can easily cause the watermark image to become distorted. Active attacks that target image watermarks are most often eliminated, masking, forgery, copying, and obfuscation attacks. Detecting the watermarked image during attack elimination is impossible, but the attacker attempts to create an output image that is similar, while the copy attack creates a copy without the watermark. When dealing with forgery attacks, the detector may incorrectly validate invalid watermark images, which can be used by attackers to conduct illegal embedding operations. An attack that is out-of-order may come from the mistake of labeling an effective watermarked image as fake [13]. Active attacks, such as those related to fingerprint recognition, copyright protection, and copy control, necessitate protection measures.

6.1 Active attack:

The main title of the paper should be 18pt, Full Capital letters and centred.

The watermark detection function is exploited by hackers to delete or destroy it, which is the cause of the active attack. Merely by accessing the watermark embedding function, attackers can easily cause the watermark image to become distorted. Active attacks that target image watermarks are most often eliminated, masking, forgery, copying, and

obfuscation attacks. Detecting the watermarked image during attack elimination is impossible, but the attacker attempts to create an output image that is similar, while the copy attack creates a copy without the watermark. When dealing with forgery attacks, the detector may incorrectly validate invalid watermark images, which can be used by attackers to conduct illegal embedding operations. An attack that is out-of-order may come from the mistake of labeling an effective watermarked image as fake [13]. Active attacks, such as those related to fingerprint recognition, copyright protection, and copy Passive attacks: Passive attacks occur when the attacker attempts to determine whether a given watermark exists. The watermark isn't modified by the attacker, but rather obtained information about it. In order to attain various important goals in hidden communication, it is important to consider various levels of passive attacks at this point.

6.2 Passive attacks

Passive attacks occur when the attacker attempts to determine whether a given watermark exists. The watermark isn't modified by the attacker, but rather obtained information about it. In order to attain various important goals in hidden communication, it is important to consider various levels of passive attacks at this point.

6.3 Removal attacks

The objective of removal attacks is to remove watermarks from host images without utilizing the keys that were used when embedding the watermark. Such attacks are of critical importance. Collusion attack, remanufacturing attack, interference attack, noise attack, and lossy compression are all categorised in these categories. These attacks cannot completely remove the watermark, but will greatly damage the watermark information. The original owner attempts to make the detection of the watermark difficult by removing the attack, as this reduces the robustness level of the watermark signal. The remastered image attack modifies the watermarked image by using modulation techniques. This kind of attack demodulates the same watermark image by means of the opposite modulation technique. Hackers commit a collusion attack by removing the watermark from original data and creating a new copy without the watermark using multiple copies of the same original data. This kind of attack adds noise signals to the watermarked image, causing confusion for the data sender. Due to the addition of extra noise in the watermarked image, interference attacks may occur [14]. The intention of these attacks is to harm the watermarks that are embedded in the documents without compromising their quality [15].

6.4 Encryption attacks

Extending the security of watermarking schemes by removing the embedded watermark information is being attempted. By conducting a brute-force search, confidential information can be embedded that can mislead the user. Another type of attack involves using available public watermark detection equipment to generate a signal without a watermark. This kind of attack is called an "oracle" attack [16]. Due to the extremely high computational complexity of these types of attacks, they must be restricted in applications.

7 Application of Digital Image Watermarking

The research field of digital image watermarking is highly concentrated due to the potential use in media such as copyright protection, annotation, privacy control, data authentication,

device control, media forensics, and medical reports. Figure 4 shows digital image watermarking application.

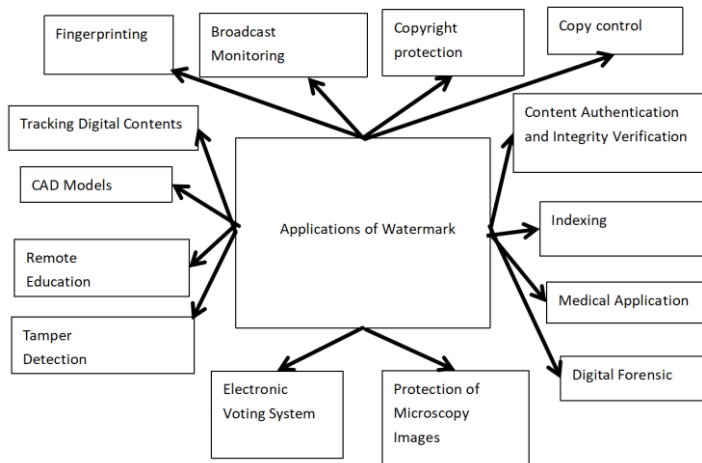


Figure 4. Digital image watermarking application (Picture credit: Original)

7.1 Copyright Protection, Claims of Ownership or Confirmation of Ownership

Copyright protection seems to be one of the initial application fields of digital watermarking technology. If the watermark exists on the Internet, the owner can protect multimedia data by making the ownership mark visible during commercial use. Compared with easily removable text marks, this application proves ownership by extracting embedded information from watermarked documents. Without strong robustness, it's impossible to remove the watermarked image without causing data distortion [17]. According to the data [18], The host image is protected and tampered with by embedding a fragile yet robust watermark image. A three-dimensional (3D) mesh by Hamidi et al. describes a scheme for protecting copyright information [19]. Grid saliency was used to obtain wavelet coefficients using grid saliency after conducting wavelet analysis on the original 3D mesh. By using Quantization Index Modulation (QIM) technology and a secret key, the watermark was added to the original 3D mesh, which was then extracted in the opposite direction. The aforementioned method is both practical and effective. Digital image watermarking technology has a important effect on the storage and transportation of satellite images. To guarantee copyright protection, a study [20]. A novel reversible invisible watermarking scheme based on SHA-3 is proposed, which utilizes hash functions and adaptive prediction algorithms.

7.2 Content Authentication and Integrity Verification

Digital images can be modified using various high-performance processing tools. Integrity is achieved when information is protected against unauthorized access in order to achieve secure communication. The authenticity of the image can be confirmed through the watermark. When the watermark is altered [21], it can be known that the image has undergone some changes.

7.3 Radio Monitoring

The owner can use the program to confirm the time and location. Satellite TV can be used to check the exact broadcast time of the content. It will add a special watermark to each audio and video data segment [22]. Multiple organizations and individuals who advertise can benefit from this method to ensure that the content is shown at the exact time agreed upon by both the client and the advertising agency [23]. Such programs ensure the smooth operation of audio-visual media [24]. The watermark data is detected in real time and then transmitted to the media room. When the watermark data is embedded into the original medium, relevant personnel will utilize the data and then transmit it to audio media, etc [25].

7.4 Copy control and fingerprint recognition

People usually steal unauthorized data, so copyright control is adopted. Watermarking technology can act as a restriction on copying behavior by informing hardware devices or software. Pirates are aware of the hidden information that poses a major threat to copyright protection. In cases involving fingerprint recognition and the use of transaction tracking [26] innocent users will not be falsely accused due to the collusion of pirates, and at least one pirate can be traced by the detector [27]. Just like fingerprint recognition, it can identify individuals, while transaction tracking can uniquely identify each copy of a work. Watermarks record the information of the recipients of each work's legal distribution, and it has been proven that invisible watermarks are more effective than visible ones [28].

8 Conclusion

This article introduces the basic model, characteristics and algorithms of digital image watermarking, as well as the advantages and disadvantages of different technologies in various fields. It also studies the types of attacks that watermarking technology may suffer and summarizes the practical application scenarios of image watermarking technology. Image watermarking technology is a challenging new field that shows significant potential for improvement and can greatly enhance the security and reliability of digital assets. It integrates the principles and technologies of numerous different disciplines such as communication, signal processing, encryption and steganography. Although people have been striving to design an efficient watermarking scheme in the past few years, most of the techniques proposed so far seem unable to resist all possible attacks and image processing operations.

In conclusion, digital image watermarking has demonstrated tremendous potential and opened the door to further research and development. With continuous efforts, it is possible to provide a secure and effective way to protect digital assets in an increasingly digital environment. This endeavor is of great significance as the digital world continues to grow and expand.

References

1. Wu, D. Y., Zhang, J. Y., Rong, W. Y.: 'A Review of Digital Image Watermarking Technology.' *High Technology Communications*, 2021, 31(02):148-162
2. Pavan, A. C., Somashekark, M. T.: 'An overview on research trends, challenges, applications and future direction in digital image watermarking.' *International Research Journal on Advanced Science Hub*, 2023, 5.1: 8-14

3. Liang, H. Y., et al.: 'A blind data hiding technique with error correction abilities and a high embedding payload.' *Journal of applied research and technology*, 2013, 11.2: 259-271
4. Yang, Y. B., Zhou, Y. M., Lu, H. M., et al.: 'Are slice-based cohesion metrics actually useful in effort-aware post-re-lease fault-proneness prediction?: an empirical study.' *IEEE Transactions on Software Engineering*, 2014,41(4): 331-357
5. Chen, L., Sun, X. Y., Lu. M., et al.: 'Contourlet watermarking algorithm based on Arnold scrambling and singular valuede composition.' *Journal of Southeast University*, 2012, 28(4): 386-391
6. Tu, S. F., Hsu, C. S.: 'A joint ownership protection scheme for digital images based on visual cryptography.' *International Arab Journal Information Technology*, 2012, 9(3):276-283
7. Su, Q. T., Yuan, Z. H., Liu, D. C.: 'An approximate schur de-composition-based spatial domain color image watermark-ing method.' *IEEE Access*, 2018, 7:4358-4370
8. Khalili, M., Asatryan, D.: 'Colour spaces effects on improved discrete wavelet transform-based digital image watermarking using Arnold transform map.' *IET Signal Processing*, 2013, 7(3):177-187
9. Wang, S. M.: 'Adaptive Detection Algorithm for Small Targets in Digital Images.' *Computer Engineering and Applications*, 2016, 52(1): 210-213
10. Wang, S. M.: 'A Review of Digital Image Watermarking Technology.' *Journal of Hunan Institute of Science and Technology (Natural Science Edition)*, 2022, 35 (01): 31-36+68
11. Kaur, E. J., Kaur, E. K.: 'Digital Watermark: A Study.' *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* 2012, 2, 159–163
12. Huang, C. H., Wu, J. L.: 'Attacking visible watermarking schemes.' *IEEE transactions on multimedia*, 2004, 6.1: 16-30
13. Nyeem, H., Boles, W. B. C.: 'Digital image watermarking: its formal model, fundamental properties and possible attacks.' *EURASIP Journal on Advances in Signal Processing*, 2014: 1-22
14. Chitra, K., Venkatesan, V. P.: 'Spatial Domain Watermarking Technique: An Introspective Study.' In *Proceedings of the International Conference on Informatics and Analytics*, Pondicherry, India, 25–26 August 2016; pp. 1–6
15. Varshney, Y.: 'Attacks on Digital Watermarks: Classification, Implications, Benchmarks.' *Int. J. Emerg. Technol.* 2017, 8, 229–235
16. Soman, K. P.: 'Insight into wavelets: from theory to practice.' PHI Learning Pvt. Ltd., 2010
17. Ramasamy, R., Arumugam, V.: 'Digital watermarking—A tutorial.' *IEEE Potentials*, 2022, 41.4: 43-48
18. Hsu, C. S., Tu, S. F.: 'Digital Watermarking Scheme for Copyright Protection and Tampering Detection.' *Int. J. Inf. Technol. Secur.* 2019, 11, 107–119
19. Hamidi, M, et al.: 'Blind robust 3D mesh watermarking based on mesh saliency and wavelet transform for copyright protection. *Information*, 2019, 10.2: 67
20. Kunhu, A., Al, M. S., Al-Ahmad. H.: 'A Novel Reversible Watermarking Scheme Based on SHA3 for Copyright Protection and Integrity of Satellite Imagery.' *Int. J. Comput. Sci. Netw. Secur.* 2019, 19, 92–102

21. Adnan, W. W., et al.: 'A review of image watermarking. In: Proceedings.' Student Conference on Research and Development, 2003. SCORED 2003. IEEE, 2003. p. 381-384
22. Kumar, V. A., Rao, C. H. S., Dharmaraj, C.: 'Image Digital Watermarking: A Survey.' *Int. J. Adv. Manag. Technol. Eng. Sci.* 2018, 8, 127–143
23. Yusof, Y., Khalfa, O. O.: 'Digital watermarking for digital images using wavelet transform.' In: 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications. IEEE, 2007. p. 665-669
24. Singh, V.: 'Digital watermarking: a tutorial.' *JSAT*, January Edition, 2011
25. Agbaje, M., Olugbenga Awodele, O., Idowu, S. A.: 'Broadcast Monitoring and Applications.' *J. Telecommun.* 2012, 7, 11–16
26. Begum, M., Uddin, M. S.: 'Digital image watermarking techniques: a review.' *Information*, 2020, 11.2: 110
27. Furon, T.: 'A Survey of Watermarking Security; International Workshop on Digital Watermarking: Siena,' Italy, 2005, pp. 201–215
28. Rashid, A.: 'Digital Watermarking Applications and Techniques: A Brief Review.' *Int. J. Comput. Appl. Technol. Res.* 2016, 5, 147–150