Applied Computing Journal https://doi.org/10.52098/acj.202145
ISSN: 2788-9688 Volume 1, Issue 4, pp 152-164, October 2021
Received: 03/12/2021 Revised: 04/01/2022 Accepted: 05/01/2022

Fusion of Watermarking and Steganography for Protecting Image Ownership: A Review

Eimad Abusham[1,*], Mahmood Al-Bahri[2], Maryam G. Aljabri[3] , and Aiysha Ali Majid Al-Marzouqi[4]
[1,2,3,4] Faculty of Computing & Information Technology, University of Sohar, 311, Oman
* Corresponding author: Eimad Abusham[1] , EAbusham@su.edu.om

Abstract

The use of digital images has become very common because of the rapid increase of the internet over time. Moving digital images over the internet is easy, but keeping ownership is complex, and serious issues have emerged. Forgery, fraud, and pirating of this content are rising. Different techniques used to protect images, like watermarking and steganography, but these methods are not enough toprotect. So, providing new techniques is essential for protecting image ownership. We have proposed a fusion method of steganography and watermarking in this work. First, the secret message is encoded within the original image using the LSB technique to obtain the stego image. Secondly, the watermarking process is applied on the stego image using text watermarking or image watermarking to provide stego-watermarked-image. The proposed fusion watermarking and steganography method is very useful for protecting image ownership over insecure communication channels. An attacker cannot get the desired watermarked image from the stego-watermarked-image without knowing the secret message hiding inside it using the LSB technique. The proposed method is efficient, simple and secure; it provides significant protection for image ownership.

Keywords*:* Watermarking; Steganography; Image ownership; Image processing.

1. Introduction

Image processing is a method or way to transfer an image into digital form to perform a certain operation on an image to obtain an improved image or extract some benefit information from the images. Image processing (Abusham & Wong, 2009; Bashier et al., 2013; Abusham, 2014; Abusham, 2021a; Abusham & Zaabi, 2021b) is very important in many fields of science, especially artificial intelligence and application in the military filed. Image enhancement is the process of modifying digital images to make them more suitable for display or further image analysis and processing (Hasoon et al, 2011; Al-hatmi & Yousif, 2017).

The information technology has revolutionized many aspects of our lives (Yousif J, 2011). As the use of internet is increasing day by day and the distribution and modification of data is also increasing that will make the data insecure protection and illegal copyright. So, there is a need some of the techniques which provides security, data authentication and protection from copyright to digital media like watermarking techniques and the steganography. In this paper, we propose method to fusion watermarking and steganography (Baboo & Sasikumar, 2015).

Steganography is a technique that hiding a secret text or message inside the original image to provide stego image. There are two algorithms using in steganography which are encoding algorithm (hide text into image) and decoding algorithm (extract text from image). At encoding algorithm, confidential information is hidden in the image to obtained stego image and in decoding algorithm, extract secret information from stego image (Ajit, & Chouhan, 2015).

Privacy-aware reversible watermarking, interdisciplinary research between watermarking and cryptography, enables a party to entrust the task of embedding watermarks to a cloud service provider without risking information privacy in cloud computing applications (Boussif et al., 2018; Al-Balushi et al., 2017; Yousif & Alattar, 2017; Al-Shezawi et al., 2017).

Watermarking is a technique that imprinting text or image onto original image for identification and authentication purposes. There are different types of watermarking which are text watermarking and image watermarking. The text is embedded into original image to give text watermarking. Also, the image is embedded into original image to give image watermarking (Sharma & Gupta, 2012). Combination of above techniques (Watermarking and Steganography) provides more security rather than using only one technique. Patra (Patra et al., 2006) described the SVD technique (Singular Value Decomposition) which enhance the security and consistency of watermarking images and robustness against attack. Also, researcher had reviewed the two existing watermarking schemes and their shortcomings are highlighted. The authors proposed an improved SVD-based technique that is more resistant to different types of

attacks. Experimental results have shown that the performance of the proposed scheme is much better than the existing schemes.

Zhao and dang discussed a new approach for increase image security and robustness by mixing the two simpler and efficient methods which are DWT (Discreate Wavelet Transform) and DCT (Discrete Cosine Transform). This paper improved a blind DCT watermarking algorithm to get a new color image digital watermarking schema based on DWT and DCT. According to simulation results, this watermarking schema is robust under common attacks especially the compression attacks (Zhao, & Dang, 2008; Zhao et al., 2014). Lai and Yah suggested a hybrid watermarking techniques that combines between two algorithms. The DCT (Discrete Cosine Transform) and SVD (Singular Value Decomposition) work together to increase security and make the digital content more authentication (Lai, &Yah, 2010). Sharma had presented a comparative study of steganography and watermarking based on goals, different methods and the result that used in each technique. According to the comparing, steganography is used for very specific amount of people, usually between two. While watermarked images are distributed between large amount of people (Sharma & Gupta, 2012). Rao had planned about watermarking system based on SVD (Singular Value Decomposition) and PSO (Particle Swarm Optimization) to provide trademark safety and reliability and to provide effective robustness with better security. Researchers had modified the singular values of the host image with the principal components of the watermark in the DWT domain for providing copyright protection. Experimental results have provided that the proposed scheme is providing copyright protection (Rao et al., 2012).

Harish had planned about a hybrid technique which combines DWT, DCT and SVD to make the more robust watermarking. They had embedded the principal components of the watermark in the DCT domain of DWT sub band of host image for providing copyright protection. Experimental results provided to illustrate that the proposed scheme can withstand a variety of image processing attacks. (Harish et al., 2013). Al-Haj described algorithm that combination of the Discrete Wavelet Transform (DWT) and the Discrete Cosine Transform (DCT) for given the watermark to the digital image. This combination improved the performance of the watermarking algorithms. Watermarking was done by embedding the watermark in the first and second level DWT sub-bands of the host image, then applying the DCT. (Al-haj, 2014). Gonge and Ghatol proposed a hybrid algorithm which combines DWT (Discrete Wavelet Transforms) and SVD (Singular Value Decomposition) method to make the watermark more security. Proposed method is used to provide ownership and copyright protection for check image and private key encryption and decryption technique used for security of bank watermark (Gonge & Ghatol, 2015).

Razzaq and Shaikh had presented a fusion of encryption, steganography and watermarking for enhance digital image security. first step in the method is encryption by using XOR operation. Then, steganography is applied using LSB technique and at the end watermarking is performed to provide significant security from attacks (Razzaq & Shaikh, 2017). Awad, Mursi, and Alsammak proposed DCT-M3 algorithm for embed the message that minimizing before embedding. The algorithm, named DCT-M3, uses modulus 3 of the difference between two DCT coefficients to embed two bits of the compressed form of the secret message. This algorithm provides better results compared to the LSB technique (Awad et al., 2018). Abraham and Paul suggested new algorithm for color image watermarking. LSB techniques are used for embedding the watermark to generate high quality watermarked image. Spatial domain methods are developed for copyright protection. This algorithm is resolve using different quality metrics and watermark removal attacks (Abraham & Paul, 2019).

Table 1 summarizes the related work and compare between different techniques that using in watermarking and steganography.

Table 1: Various Techniques of Watermarking and Steganography.

Year	Author Name	Techniques	Features
2006	Patra, Soha and Ang	SVD	More security from attack and Consistency
2008	Zhao and Dang	DWT – DCT	Increase robustness and the security
2010	Lai and Yah	DCT- SVD	Robustness, imperceptibility
2012	Rao, Shekhawat and Srivastava	SVD – PSO	Reliability of watermarking image, Robustness, optimal scaling factor
2013	Harish, Kumar and Kusagur	DWT, DCT & SVD	more robust watermarking
2014	Al-Haj	DWT-DCT	Improved the performance of the watermarking algorithms
2015	Gonge and Ghatol	DWT- SVD	Robustness, the better watermarking identification, better security
2017	Razzaq and Shaikh	XOR operation & LSB	Enhance digital image security
2018	Awad, Mursi, and Alsammak	DCT-M3	Enhance quality and capacity of the stego image
2019	Abraham and Paul	LSB	High quality watermarked image

2. Research Methodology

In the present study we explored and reviewed the main concepts and tools of Fusion of Watermarking and Steganography techniques. Multi phases are needed to perform the combining of Watermarking and Steganography processes. First, take the original image to hiding the secret text inside it using LSB method to provide stego image. Then, stego image is watermarked to provide copyright. When stego-watermarked-image is move to destination, then we could apply the de-steganography to retrieve secret text for confirm ownership.

3. Watermarking & Steganography Review

In this section, the important information of watermarking and steganography will be display. In addition, it explains the basic idea of watermark embedding and extracting techniques and the different types of watermarking. Also, it will review a basic steganography embedding and extracting. Moreover, it will present a literature review that related to the subject of watermarking and steganography and summarizes the related work.

3.1. Digital Watermarking

Watermarking is a technique of inserting the information to the different digital media for example image, video or audio that provides the data authentication and copyright protection (Singh, & Chadha,2013). By using digital watermarking technique, the owner of digital media can protect the copyright of the file. Figure 1 shows the different watermarking classification which are text watermarking, image watermarking, audio watermarking and video watermarking.

Text watermarking is used to operate as a watermark text in the image. It can have applied in the layout and background of appearance of the image. Image watermarking is used to hide any secure any image into image. Audio watermarking is a single which are inserted as watermarking into audio singles. Video watermarking is used to security the videos which is divided into different video shots and after that, each shot selected one video frame. This video frame in image processing is called identical frame.

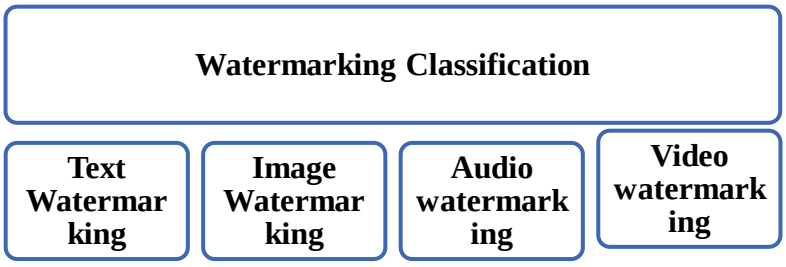


Figure 1: Classification of Watermarking

The digital watermarking technique includes two different algorithms or process which are watermarking embedding algorithm and watermarking extraction algorithm. All types of digital watermarking techniques have the same two algorithms (Hussein, 2012).

Figure 2 presents the algorithm of embedding watermarking. In the embedding process, watermark which is text or image can embed into original image to obtain watermarked image.

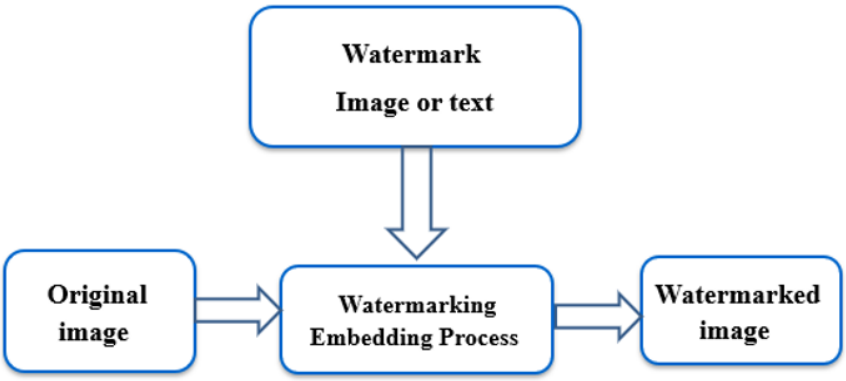


Figure 2. Algorithm of Watermarking Embedding

3.2. Applications of Digital Watermarking

There are several applications using the digital watermarking and enable to use in it for example copyright protection, fingerprinting, data authentication, copy protection and broadcast monitoring as shown in Figure 4.

1. Copyright Protection: To protect copyright ownership, the information about the owner like name or image of owner is embedded as a watermark to the digital file. This prevents from illegal copying of the digital file.
2. Fingerprinting: The finger printing watermark embedded in the content is used to trace authorized users.
3. Data Authentication: In data authentication, the intent is to uncover the alterations to the data by embedding a watermark into the digital file.
4. Copy Protection: Copy protection application prevents unauthorized replication of the content by watermarked it.
5. Broadcast Monitoring: The content of television and radio channels is growth over the last years, so the reality of broadcast is become very important for different employed in this channel like owners, distributors and broadcasters (Singh, & Chadha,2013).

3.3. Kinds of Digital Watermarking

The digital watermarking divides into different types based on different criteria such as perceptivity, domains, robustness and detection process.

3.3.1. Based on Perceptivity

Figure 5 shows watermarking has two types based on perceptivity which are visible watermarking and invisible watermarking. In visible watermarking, the watermark which is text or image can be seen in the digital content. For example, the logo of all television channel is visible to the viewer. However, Invisible watermark is inserted into the digital content that is the watermark cannot be visible to the viewer for some advantages such as authentication and protection image ownership (Honsinger, 2002; Jain & Ghanekar, 2018).

By perceptivity, the watermark embedded is either invisible or visible, as illustrated in Figure 6. Embedding method of visible watermarking is easier than invisible watermarking while invisible watermarking is better to protecting from an attack.

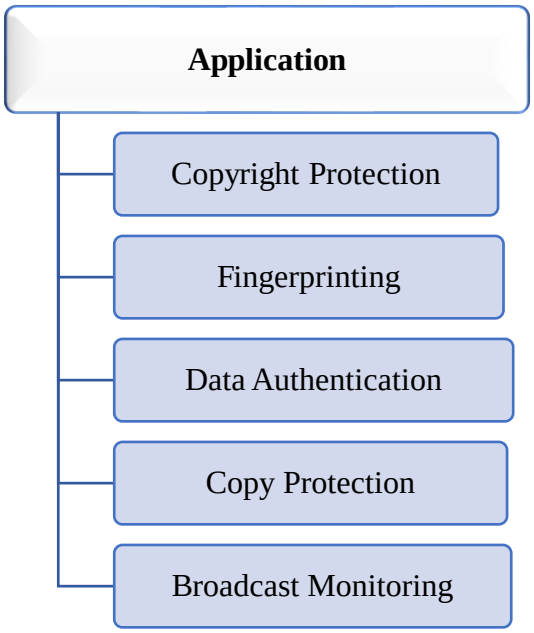


Figure 1: Applications of Digital Watermarking

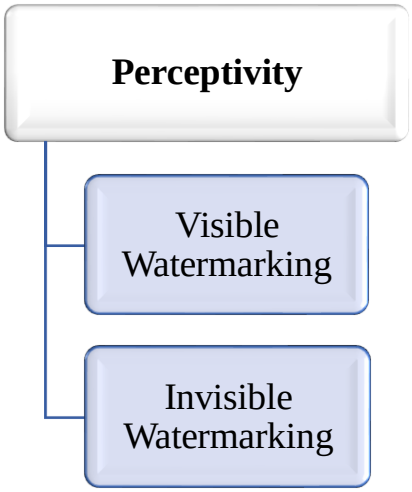
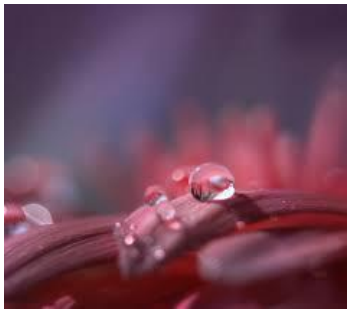
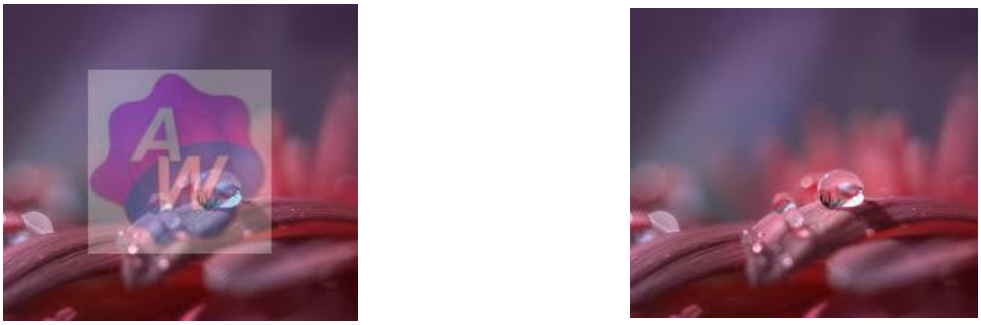


Figure 5: Kinds of watermarking depending on perceptivity



(a)

(b)



(c) (d)

Figure 6: Comparison between visible and invisible watermarked image. (a) Cover image, (b) watermark image, (c) visible watermarking, (d) invisible watermarking.

3.3.2. Based on Domains

Watermark can be inserted into the original image in spatial domain and in frequency domain. Figure 7 presents the types of watermarking based on domains. There are various techniques used in spatial and frequency domains. In spatial domain, the techniques worked directly on single pixel of an image for example, LSB and spread spectrum. While in frequency domain, the techniques worked on frequency of an image such as DCT, DWT and FFT (Sarkar & Sanyal, 2014).

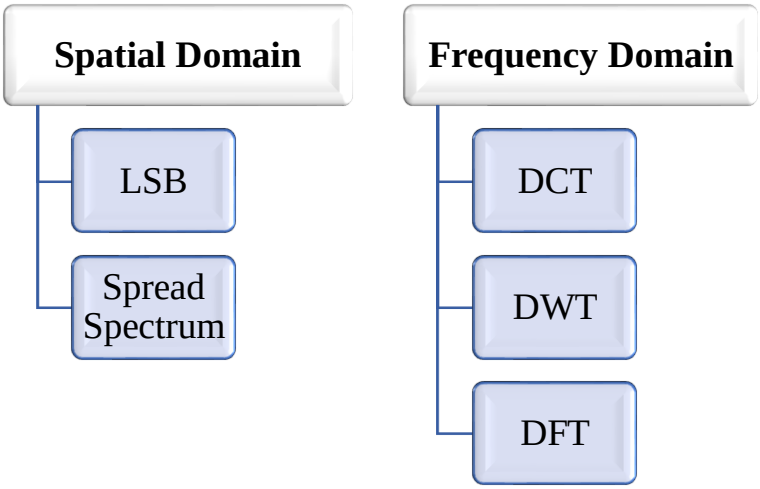


Figure 7: Kinds of watermarking depending on

1. **Discrete cosine transforms (DCT):** it represents data in terms of frequency space rather than an amplitude space. They are difficult to implement and are computationally more expensive. At the same time, they are weak against geometric attacks like rotation, scaling, cropping etc. Embedding in the perceptually significant portion of the image has its own advantages because most compression schemes remove the perceptually insignificant portion of the image (Singh, & Chadha,2013).

Figure 8 present the steps of DCT Block Based Watermarking Algorithm.

Step 1: Read the original image.
Step 2: Segment the image into non-overlapping blocks of 8x8.
Step 3: Apply forward DCT to each of these blocks.
Step 4: Apply some block selection criteria (e.g., HVS).
Step 5: Apply coefficient selection criteria (e.g., highest).
Step 6: Embed watermark by modifying the selected coefficients.
Step 7: Apply inverse DCT transform on each block.

Figure 8: DCT Block Based Watermarking Algorithm steps.

2. **Discrete Fourier transform (DFT):** Transforms a continuous function into its frequency components. It has robustness against geometric attacks like rotation, scaling, cropping and translation. Spatial shifts in the image affects the phase representation of the image but not the magnitude representation (Singh, & Chadha,2013).
3. **Discrete wavelet transforms (DWT):** Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The transforms are depending on small waves, called wavelet. The wavelet transform decomposes the image into three spatial directions, i.e. horizontal, vertical and diagonal. The Discrete Wavelet Transform is currently applied in a broad variety of signal processing applications, such as in audio and video compression (Al-haj, 2014).
4. **Least Significant Bit (LSB):** The embedding of the watermark is performed choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with watermark bits. The watermark may be spread throughout the image or may be in the select locations of the image. This method is easy to implement and does not generate serious distortion to the image (Gupta et al., 2012).
5. **Spread-spectrum:** Spread spectrum techniques are methods in which energy generated at one or more discrete frequencies is distributed in time. SSM based watermarking algorithms embed information by linearly combining the host image with a small pseudo noise signal that is modulated by the embedded watermark (Singh, & Chadha,2013).

Table 2 summarized the main differences spatial domain and frequency domain based on some standards.

Table 2: Difference between spatial domain and frequency domain

Standards	Spatial Domain	Frequency domain
Computation Cost	Low	High
Robustness	Fragile	More Robust
Perceptual quality	High control	Low control
Computational complexity	Low	High
Computational Time	Less	More
Amplitude	High	Low
Example of Application	Mainly Authentication	Copy rights

In spatial domain, the watermark is embedded directly into pixels of the image, which involves less complex computation and less cost computation. While frequency domain watermarks are more robust to signal processing attacks, involve more complex computation and more cost computation (Singh, & Chadha, 2013).

3.3.3. Based on the Use of Keys

Depending on the use of keys, watermarking is distributed into asymmetric watermarking and symmetric watermarking. Asymmetric watermarking used different keys for embedding and extracting the watermark while symmetric watermarking used same key.

3.3.4. Based on Robustness

Depending on the robustness watermark are distributed into robust, fragile and semi-fragile watermarks. Watermark want robustness for maintain ownership from different attacks (Singh & Chadha,2013).

3.3.5. Based on Detection Process

There are different techniques used to extract the information from watermarked files which are non-blind, semi-blind and blind techniques.

3.4. Steganography

Steganography is an art of secret communication that hidden information through content medium such as images. Image steganography is used to embed the information message from unlawful communication. There are two algorithms used in the steganography techniques which are insertion algorithm and extraction algorithm. At the insertion method, secret information or message is hidden in the original image to provide stego image which is transmitted through unsecured channel as it is the original image. While secret information is extracted from stego image in the extraction method as shown in Figure 9 (Douglas et al., 2018; Diskin).

Steganography is can be implemented in many applications, such as secret communications, feature tagging elements and copyright protection (Ajit, & Chouhan,2015).

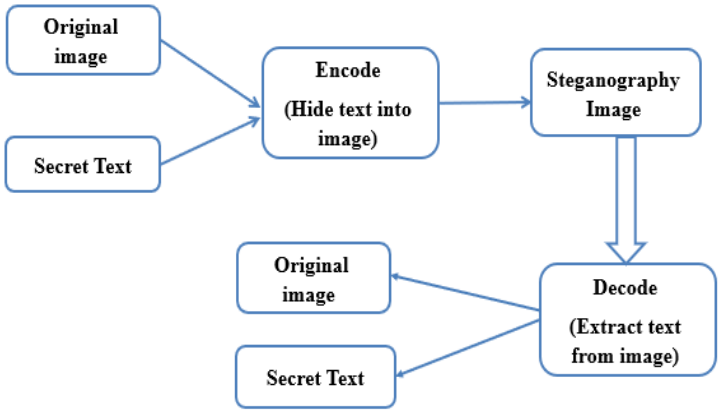


Figure 9: Flowchart for Insertion and Extraction of Steganography

3.5. Comparative Study of Watermarking & Steganography

There are some differences between steganography and watermarking techniques based on some criteria which show in Table 3 below (Sharma & Gupta, 2012).

Table 3: Comparative study of Watermarking and Steganography

Standard	Steganography	Watermarking
Purpose	Encode an information in one-to-one connection	Embed an information in one-to-many connection
Transporter	Whichever media for example text, audio and video.	Generally, paper, image and audio.
Secrete message	Encoded with transporter without knowing about existence	Inserted with transporter with or without knowing about existence
Aims	Steer connection	Copyright, authentication etc.
Attack method	Steganalysis	Data Transformation
Clarity	Not visible	Generally visible
Drop case	Discovery	Extraction
Target meeting	Steganography is usually inserted between very small group of people.	Watermarked output can be sending clearly between great sets of people
Result	Stego file	Watermarked file

4. Conclusion

This manuscript discussed the Literature review of watermarking and steganography. It showed background information on digital watermarking, types, and watermarking applications. Also, it described the steganography technique and explained how it works. Moreover, it presented the summarization of related work based on the method.

Acknowledgment

The research leading to these results has received no Research Project Grant Funding.

References

[1]. Abraham, J., & Paul, V. (2019). An imperceptible spatial domain color image watermarking scheme. Journal of King Saud University-Computer and Information Sciences, 31(1), 125-133.
[2]. Abusham, E. A. (2014). Face verification using Local Graph Structure (LGS). In 2014 International Symposium on Biometrics and Security Technologies (ISBAST) (pp. 79-83). IEEE.
[3]. Abusham, E. E., & Wong, E. K. (2009). Locally linear discriminate embedding for face recognition. Discrete Dynamics in Nature and Society, 2009.
[4]. Abusham, E. A. (2021a). Image Processing Technique for the Detection of Alberseem Leaves Diseases Based on Soft Computing. Artificial Intelligence & Robotics Development Journal, 103-115.
[5]. Abusham, E. A., & Zaabi, A. M. A. (2021b). Smartphone application for Self-Management Diabetes: A review. Applied computing Journal, 25-37.
[6]. AL-Balushi, A. I., Yousif, J., & Al-Shezawi, M. (2017). Car accident notification based on Mobile cloud computing. International Journal of Computation and Applied Sciences IJOCAAS, Volume2, (2).
[7]. Al-Hatmi, M. O., & Yousif, J. H. (2017). A review of Image Enhancement Systems and a case study of Salt &pepper noise removing. International Journal of Computation and Applied Sciences (IJOCAAS), 2(3), 171-176.
[8]. Ajit, P., & Chouhan, K. (2015). A Study and literature Review on Image Steganography. International Journal of Computer Science and Information Technologies (IJCSIT), 6(1), 685–688.
[9]. Al-haj, A. (2014). Combined DWT-DCT digital image watermarking Combined DWT-DCT Digital Image Watermarking. Journal of Computer Science 3 (9), 740-746. https://doi.org/10.3844/jcssp.2007.740.746
[10]. Al-Shezawi, M. O., Yousif, J. H., & AL-Balushi, I. A. (2017). Automatic attendance registration system based mobile cloud computing. International Journal of Computation and Applied Sciences, 2(3), 116-122.
[11]. Awad, A., Mursi, M. F. M., & Alsammak, A. K. (2018). Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3. Ain Shams Engineering Journal, 9(4), 1965–1974. https://doi.org/10.1016/j.asej.2017.02.003
[12]. Baboo, S. S., & Sasikumar, V. R. (2015). Fusion of Steganography Digital Watermarking Data Hidden in Patient Medical Image using PPC Approach. Global Journal of Computer Science and Technology (H) Information & Technology, 15(4), 0975-4350.
[13]. Bashier, H. K., Abusham, E. E., Abdullah, M. F. A., Liew, T. H., Yusof, I., & Lau, S. H. (2013b). Real time face tracker based on local graph structure threshold (LGS-TH). Australian Journal of Basic and Applied Sciences, 7(2), 632-638.
[14]. Boussif, M., Aloui, N., & Cherif, A. (2018). Secured cloud computing for medical data based on watermarking and encryption. IET Networks, 7(5), 294-298.
[15]. Douglas, M., Bailey, K., Leeney, M., Curran, K., & Douglas, M. (2018). An overview of steganography techniques applied to the protection of biometric data. Multimed Tools Appl (2018), 17333–17373 https://doi.org/10.1007/s11042-017-5308-3
[16]. Gonge, S. S., & Ghatol, A. (2015). A robust and secure dwt-svd digital image watermarking using encrypted watermark for copyright protection of cheque image. In International Symposium on Security in Computing and Communication, Springer, 290-303.
[17]. Gupta, S., Goyal, A., & Bhushan, B. (2012). Information Hiding Using Least Significant Bit Steganography and Cryptography. Modern Education and Computer Science, 6, 27-34. https://doi.org/10.5815/ijmecs.2012.06.04
[18]. Hasoon, F. N., Yousif, J. H., Hasson, N. N., & Ramli, A. R. (2011). Image enhancement using nonlinear filtering based neural network. Journal of Computing, 3(5), 171-176.
[19]. Harish, N. J., Kumar, B. B. S., & Kusagur, A. (2013). Hybrid Robust Watermarking Technique Based on DWT, DCT and SVD. International Journal of Advanced Electrical and Electronics Engineering (IJAEEE), (5), 137–143.
[20]. Hussein, E., & Belal, M. A. (2012). Digital watermarking techniques, applications and attacks applied to digital media: a survey. International Journal of Engineering Research & Technology, 1(7), 1-8.

[21]. Honsinger, C. (2002). Digital watermarking. Journal of Electronic Imaging, 11(3), 414.
[22]. Lai, C. C., & Yeh, C. H. (2010). A hybrid image watermarking scheme based on SVD and DCT. In Machine Learning and Cybernetics (ICMLC), 6, 2887-2891.
[23]. Jain, P., & Ghanekar, U. (2018). Robust watermarking technique for textured images. Procedia Computer Science, 125(2009), 179–186. https://doi.org/10.1016/j.procs.2017.12.025
[24]. Patra, J. C., Soh, W., Ang, E. L., & Meher, P. K. (2006). An improved SVD-based watermarking technique for image and document authentication. In Asia Pacific Conference on Circuits and Systems (APCCAS), 2006, 1984-1987.
[25]. Rao, V. S. V., Shekhawat, R. S., & Srivastava, V. K. (2012, March). A reliable digital image watermarking scheme based on SVD and particle swarm optimization. In Engineering and Systems (SCES), 2012 Students Conference, 1-6.
[26]. Razzaq, M. A., & Shaikh, R. A. (2017). Digital Image Security: Fusion of Encryption, Steganography and Watermarking. International Journal of Advanced Computer Science and Applications, 8(5), 224–228.
[27]. Roy, R., Sarkar, A., & Changder, S. (2013). Chaos based Edge Adaptive Image Steganography. Procedia Technology, 10(2013), 138–146. https://doi.org/10.1016/j.protcy.2013.12.346
[28]. Sarkar, T., & Sanyal, S. (2014). Digital watermarking techniques in spatial and frequency domain. International Journal, 2(2), 2–6.
[29]. Sharma, M. K. & Gupta, P. C. (2012). A comparative study of steganography and watermarking. International Journal of Research in IT and Management (IJRIM), 2(2), 1–12.
[30]. Singh, P., & Chadha, R. S. (2013). A survey of digital watermarking techniques, applications and attacks. International Journal of Engineering and Innovative Technology (IJEIT), 2(9), 165-175.
[31]. Yousif, J. H. (2011). Information Technology Development. LAP LAMBERT Academic Publishing, Germany ISBN 9783844316704.
[32]. Yousif, J. H., & Alattar, N. N. (2017). Cloud management system based air quality. International Journal of Computation and Applied Sciences (IJOCAAS), 2(2).
[33]. Zhao, H., Chongmin, L., Zain, J. M., & Abdalla, A. N. (2014). Robust Image Watermarking Theories and Techniques: A Review. Journal of Applied Research and Technology, 12(1), 122–138. https://doi.org/10.1016/S1665-6423(14)71612-8
[34]. Zhao, M., & Dang, Y. (2008). Color image copyright protection digital watermarking algorithm based on DWT & DCT. In International Conference on Wireless Communications, Networking and Mobile Computing, 2008, 1-4.