

Secure Digital Image Watermarking using Fibonacci Scrambling and Rotational Embedding

Aditi Sharma¹ and Sateesh Kumar Awasthi²

¹⁻²Dr B R Ambedkar National Institute Of Technology, Jalandhar, India
Email: aditi0201997sharma@gmail.com, awasthisk@nitj.ac.in

Abstract— Present age is the age of technology where we are all flooded with digital data. As the use of data is increasing day by day, the techniques and algorithms for data manipulation are also increasing at a rapid rate. The advancement in technology has brought about a revolution which has led to identification of various ways and techniques for modification and enhancement of images. On the other hand it also brings various challenges with respect to the prevention of tampering, forging or misuse of electronic data in form of image, audio or video. Digital watermarking can prove to be a very useful technique in prevention of any such scenario. Verifying the integrity of delicate images, such as medical photos, is crucial since even the smallest distortion or alteration might lead to a wrong diagnosis. Especially in digital images, watermarking techniques give protection from any such attack to a large extent. This research paper proposes a novel approach to digital image watermarking using a combination of Fibonacci scrambling, rotational embedding, and the Discrete Cosine Transform (DCT). The objective of the proposed algorithm is to bolster the security and resilience of the watermarking process through the incorporation of supplementary encryption and obfuscation mechanisms. We have implemented the code for this algorithm in Python.

Index Terms— Discrete Cosine Transform (DCT), watermark, discrete wavelet Transform, Watermark extracting algorithm, Digital image watermarking, Fibonacci scrambling, Rotational embedding, Security, Robustness.

I. INTRODUCTION

Digital data has become an integral part of the modern world, permeating various aspects of our lives. While technological advancements have brought numerous benefits, they have also led to challenges related to data tampering and unauthorized copying. With the abundance of software applications capable of easily modifying, copying, or replicating digital data, it has become increasingly challenging to identify the original data and trust the authenticity of multimedia content. To address these concerns, methods and techniques are needed to prevent forgery and facilitate the identification of the rightful owner of multimedia. Watermarking is a widely employed technique that serves as a deterrent against data misuse, infringement, and tampering. By embedding information within an image, watermarking makes it difficult for attackers to harm or misuse the image. It simplifies the process of identifying the authentic owner and enables tracing back the image's origin, thus mitigating the risks associated with image misuse. In essence, watermarking plays a crucial role in safeguarding data integrity and protecting against unauthorized use of digital content. The idea of a watermark dates back to ancient times when the people used to hide the messages within the human body. Following that, few years later it arrived on the paper with the thickness of the paper being modified to incorporate the watermark into

it. This process was carried out during the paper's wet state, that is the reason why it is described as a watermark [1]. Watermarking is one of the most widely used processes for copyright protection, content authentication and owner identification. This field of study is growing with a rapid pace, incorporating various new technologies into the already existing technologies. For instance, since the last 50 years, optimization methods that are inspired by evolution and natural genetics, such as Genetic methods, Evolutionary Programming, and Evolutionary Strategies (ES), have dominated the field [10]. Various brands embed their logos on their products which is also a kind of watermarking used by them for promoting their brand. On the other hand some of the watermarks are concealed in the multimedia in order to identify if there is any unauthorized distribution of copyrighted content. The watermarking techniques can be applied to various forms of multimedia contents including images, video, audio and text document files. Depending upon the requirements and objectives it can be used to other forms of multimedia also. The main advantage of using a watermarking is that the content cannot be distinguished from the watermark [5].

The rest of the paper is structured as follows. Section II includes the image watermarking process and its classification on the basis of different parameters. The following section III represents our proposed work; section IV includes the results and discussions of our implementation. Finally, the last section V presents the primary conclusion and references being used in this paper.

II. DIGITAL WATERMARKING

A. Basic Process of Watermarking

The watermarking process involves two primary steps [3]. Initially, a watermark is deliberately selected, which can encompass various forms such as a logo, text, or distinct information. The digital watermark serves as an imperceptible signal that seamlessly integrates into digital data and can subsequently be detected for various purposes, including buyer/seller identification and verification of ownership [5]. Following the selection of the watermark, it is securely embedded into the host image using a confidential key and the chosen watermarking technique. This embedding process often entails modifying pixel values or transform coefficients. Experimental evidence has demonstrated that enhancing the overall security and resilience of the watermarked image is achieved by embedding a modified version of the watermark rather than directly embedding it into the original image [6]. This approach has shown superior results in terms of security and robustness. The secret key, which can be either private or public, is employed to ensure the security of the process [9]. Great care is taken to minimize any visual impact on the original content of the image during the modification. Consequently, the image undergoes this process and acquires the embedded watermark, rendering it resistant to forgery or unauthorized copying. A visual depiction of the fundamental diagram illustrating the sequence of steps involved in the process of embedding the watermark into the image can be observed in Figure 1.

Once the embedding process has been completed, the subsequent step involves extracting the watermark from the original host or cover image where it was embedded. This extraction process involves separating the watermark from the image and can be visualized in Figure 2, which presents the basic block diagram of the watermark extraction process. The specific technique employed determines whether the extraction necessitates the use of the original image or not. To facilitate the extraction process, a range of algorithms is utilized, encompassing correlation-based methods, statistical analysis, and techniques based on the transform domain. Once the extraction process reaches its conclusion, analyzing the watermark yields valuable information regarding the authenticity and ownership of the original host image. When disputes arise regarding the ownership of digital data, the watermark can serve as compelling evidence of ownership and can be removed to support such claims [11].

B. Types Of Watermarking Techniques

The watermarking process described in the previous section is the basic procedure that is followed in every watermarking technique. Although the basic steps remain same, different watermarking techniques vary in the procedure being followed and can be classified based on various factors. Some of the major classifications are described as follows:

a. Classification Based on Visibility

Visible Watermarking: As the name suggests, visible watermarking refers to the one where the watermark is visible to a naked human eye. It is made visible intentionally. The major application of such watermarking technique is found in brand logos printed on their products, stamps being printed on the paper etc. where we want the owner name or identity to be made implicitly known to everyone [2].

Invisible Watermarking: In invisible watermarking, the watermark is incorporated in a way that makes it difficult or impossible to see it with naked eyes [2]. In such watermarking techniques we need a specific technique for

extraction of the watermark. This technique is used for protection of intellectual property rights, tracing back the content and monitoring the digital data.

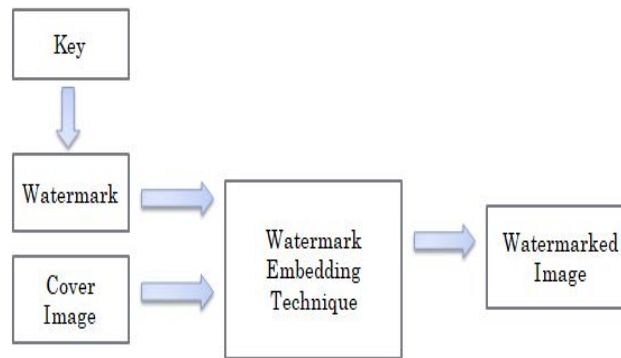


Figure 1. Embedding Watermark into Host image

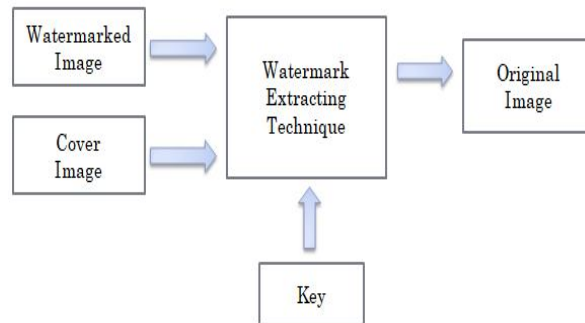


Figure 1. Extracting Watermark from Host image

b. Classification Based on Host

Audio Watermarking: The watermark is placed into the audio data file during audio watermarking [12]. This is done while making sure that the audio quality is not degraded while performing this process.

Video Watermarking: The watermark is in the form of an overlay on a video which includes some information about the owner of the content which might include text, some kind of copyright disclaimer or text [1].

Image Watermarking: In this method, an image is placed into the carrier data (host image) during digital image watermarking [13].

Text Watermarking: To prevent text alterations, text watermarking refers to addition of a watermark to documents such as PDFs and Word documents [4]. With the aid of text watermarking techniques, copyright infringement can be identified when a text document contains a hidden message about the material [1].

c. Classification Based on Domain

Spatial Domain Watermarking: When we make use of spatial domain watermarking, selected pixel's intensity is changed [1][2]. The most widely used algorithms in this field are LSB (Least Significant Bit) and SSM (Spread Spectrum Modulation) modulation. Although spatial domain watermarking algorithms are easy to implement but are quite vulnerable to attacks [9].

Transform Domain Watermarking: In this procedure, the watermark is not directly inserted. Prior to inserting the watermark into the modified signal, the carrier image must first be transformed [1]. The frequency domain algorithms, are employed to modify specific frequency components of the image [2][16]. Through various experiments it is observed that to ensure transparency or imperceptibility, the watermarking image should be placed into the high frequency regions of the original image. The transform domain method outperforms the spatial domain method in terms of overall performance [6]. It is observed that frequency domain watermarking is more difficult yet more resilient to attacks [3][9].

d. Classification Based on Robustness

Fragile Watermarking: A watermark is called as fragile if it cannot withstand any kind of change [2]. In case of any tampering the watermark will be degraded and cannot be retrieved. Such watermarking techniques prove to

be useful when we have highly sensitive data as the fragility of the watermarking allows us to tell whether the data has been altered [4].

Robust Watermarking: A watermark can be defined as a robust watermark if it does not allow any changes or modification [2]. This means that even if the image is compressed, cropped or any other basic image processing is done; the watermark can still be retrieved without much distortion and hence can be checked or examined for identification of ownership. This kind of watermarking is frequently used for copyright protection [4].

e. Classification Based on Extraction Process

Blind Watermarking: This technique is referred to as blind because there is no need for the original image for extraction. The watermark can be extracted from the watermarked data itself. Blind watermarking approaches often make use of algorithms created to accurately detect and extract the embedded watermark without knowing the original data beforehand [17]. When the original data might not be available or when the watermark needs to be retrieved separately from the original data, this method is helpful.

Non-Blind Watermarking: For implementing this technique we have a dependency on the original image as it requires the original image to be available while the extraction process takes place. The original data is referenced or used as a template by the extraction algorithm to help with the extraction and verification of the embedded watermark. When the original data is easily accessible and can serve as the basis for the extraction process, this method is advantageous.

III. PROPOSED WORK

The increasing prevalence of digital media and the ease of digital content manipulation have raised concerns regarding copyright infringement and unauthorized use of digital images. Digital image watermarking techniques provide a means to embed an imperceptible mark into the image, enabling its authentication and identification. This paper introduces a novel algorithm for digital image watermarking that combines Fibonacci scrambling, rotational embedding, and the DCT to improve security and robustness

Below subsections provide the detailed step by step process that is being followed in the proposed watermarking technique.

A. Fibonacci Scrambling

The initial step of the proposed algorithm involves the scrambling of the watermark using the Fibonacci sequence. The Fibonacci sequence is a widely recognized mathematical sequence renowned for its ability to generate numbers that exhibit properties similar to random numbers. The sequence, which starts with the numbers 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, is commonly referred to as the Fibonacci numbers and holds great significance in both historical and mathematical contexts. These numbers were named by Edouard Lucas, a French mathematician of the nineteenth century, in honor of Leonard Fibonacci of Pisa, a renowned mathematician from the Middle Ages. Fibonacci originally mentioned these numbers in his book *Liber Abaci* (1202) while discussing a problem involving rabbits [14]. By applying Fibonacci scrambling, we introduce an additional layer of randomness and unpredictability to the watermark, making it resistant to statistical attacks. By applying the Fibonacci sequence to the pixels of an image, the positions of the pixels are rearranged, resulting in a visually scrambled version of the original image. The original image is converted into a matrix of pixel values. Each pixel represents a discrete element of the image. The Fibonacci sequence is generated with a length equal to the total number of pixels in the image in form of a Fibonacci matrix. The pixels in the image matrix are rearranged based on the Fibonacci sequence. Each pixel is assigned a new position determined by the Fibonacci sequence. The rearranged pixel positions are used to create a new image matrix, resulting in a scrambled version of the original image. The Fibonacci sequence provides a complex pattern for pixel rearrangement, making it difficult to reverse-engineer the scrambling process and retrieve the original image.

B. Rotational Embedding

Rotational embedding, also known as clockwise shifting of pixels, is a technique used to embed information into digital images by rearranging the positions of pixels in a clockwise direction. This method alters the spatial arrangement of pixels, making it difficult for unauthorized individuals to discover the embedded information without the proper decryption process. Once the scrambling process is completed, the original image is converted into a smaller blocks of pixels, representing discrete elements of the image. In the proposed algorithm, the smaller blocks are 16 x 16 blocks. The key, which is the rotation parameter, is then determined which is passed along with the image blocks to the rotating function. This parameter defines the degree around which the blocks will be rotated. We have made use of the key value so as to keep this technique more temper resistant. The rotation adds another level of security by altering the spatial arrangement of the image pixels [14]. This spatial transformation

makes it difficult for unauthorized users to identify and remove the watermark without the correct rotation key. Once we have the key value, each block is individually rotated in a clockwise direction based on the rotation parameter, and during this process, the embedded data is integrated into the shifted pixels.

C. Discrete Cosine Transform

Following the application of rotational scrambling on each block of the image, the blocks are then rearranged to form a single image.

After that when we finally have the encrypted watermark image, the watermark is embedded into the host image using the DCT domain processing. The DCT is a transformation technique that converts a spatial domain signal, such as an image, into the frequency domain. It decomposes the image into a set of orthogonal frequency components called DCT coefficients [11]. These coefficients represent the different frequencies present in the image, with the lower-frequency components typically containing the majority of the image's energy. The DCT allows for efficient and robust embedding by transforming the image into its frequency components. By utilizing the watermark data, the DCT coefficients are altered in a manner that ensures the imperceptible embedding of the watermark within the image. The use of the DCT domain minimizes the visual impact on the image while maintaining the watermark's integrity and robustness.

D. Watermark Extraction

To extract the watermark from the watermarked host image, the reverse process is applied. Firstly we perform inverse DCT. Inverse discrete cosine transform (IDCT) is an essential operation in watermarking that is used to reconstruct the watermarked image. It is the reverse process of the discrete cosine transform (DCT) and is applied in the spatial domain to convert the frequency components back into the image domain. Once we have the embedded image, the IDCT is performed on a block-by-block basis, as the DCT is applied to image blocks to achieve better frequency localization. Each block of modified DCT coefficients is independently transformed using the IDCT, and the resulting pixel values are combined to reconstruct the entire watermarked image. Once we have that image, then we convert the image back into small blocks of 16×16 . After obtaining these smaller blocks using the secret key value we reverse the rotation. The extracted watermark is then descrambled using the Fibonacci sequence, resulting in the retrieval of the original watermark. This extraction process ensures the integrity and fidelity of the embedded watermark, even in the presence of potential attacks. We have discussed the effect of potential attacks on the image in next section of this paper.

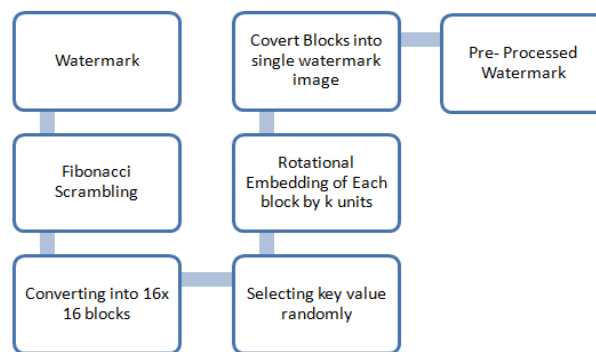


Figure 3. Watermark Pre-processing

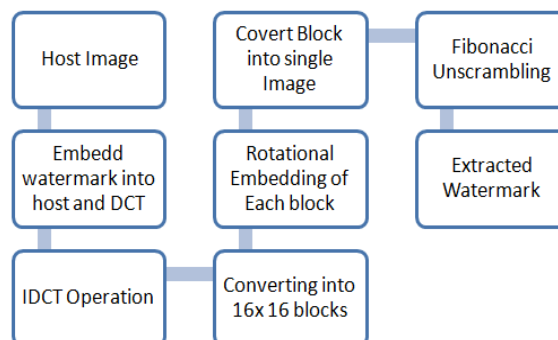


Figure 4. Watermark Extraction Using Proposed Algorithm

IV. RESULTS

The proposed watermarking algorithm has been employed to embed and extract the watermark from the host image. After that we have obtained the structural similarity index parameter for the various images and tested it's robustness against various attacks like compression, cropping, introduction of noise, averaging and sharpening. When we applied this watermarking technique to various images we found that this technique is robust and watermark is easily extracted even after various attacks.

A. Parameter Used for Performance Analysis

In this paper we are making use of a python specific parameter called as Structural Similarity Index for the analysis of quality of the extracted watermark.

Structural Similarity Index Parameter (SSIP): The Structural Similarity Index (SSIM) is a commonly utilized metric for quantifying the similarity between two images. It aims to capture both the structural information and the perceived quality of the images. Unlike other similarity metrics such as Mean Squared Error (MSE), SSIM takes into account the human visual system's characteristics and provides a more accurate measure of image similarity. In Python, you can calculate the SSIM using the compare_ssim function from the skimage.measure module of the scikit-image library. The compare_ssim function calculates the SSIM between the two images and returns a score between -1 and 1, where a higher score indicates greater similarity. SSIM is based on three main components: luminance comparison, contrast comparison, and structural comparison.

B. Results For Various Attacks

We have performed various attacks on a sample dataset of the images. Once we have the embedded image, we then tried to extract the watermark using our proposed algorithm. One of the sample image under attack is shown in figure 4 to Figure 9 and the extracted watermarks along with their SSI are depicted in table 1. It is quite evident from the results that proposed algorithm is resistant to common attacks on the embedded image.



Figure 5. Original watermarked Image

Figure 6. Gaussian Noise

Figure 7. Averaging image by 3*3 filter



Figure 8. Salt and Pepper Noise



Figure 9. Cropping Of Image



Figure 10. Median Filtering

As we can infer from the figure- 6 shown, we have applied Gaussian Noise with mean = 0 and Standard Deviation =49 to our image and Gaussian noise is a type of statistical noise that affects the pixel values of an image. It is characterized by having a mean (average) value of zero and a standard deviation that determines the spread or intensity of the noise. The process of adding Gaussian noise to an image involves generating random values from a Gaussian distribution and adding these values to the pixel intensities of the image. The amount of noise added is controlled by the standard deviation of the distribution. Higher standard deviation values result in stronger noise, while lower values produce milder noise. We observed that the obtained watermark quality is still not degraded much.

After testing with Gaussian Noise we also tested the proposed technique with salt and pepper noise with strength of 0.2 as shown in figure-8 Adding salt and pepper noise to an image involves randomly selecting a set of pixels and changing their intensity values to either the maximum value (salt) or the minimum value (pepper). This introduces sudden and sporadic high and low intensity values in the image, disrupting its visual appearance. We found that the proposed watermarking technique is resistant to this attack as well

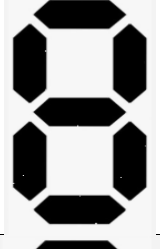
After testing with noise attacks we tried to test the technique with other image operations like sharpening (Sharpening an image is a technique used to enhance the edges and details within the image, making it appear sharper and more defined. It involves increasing the contrast of the edges, which makes them stand out more prominently), averaging filter (The averaging filter, which is alternatively referred to as a box filter, serves as a straightforward low-pass filter. It aids in the smoothing of an image by replacing the value of each pixel with the average value obtained from its neighboring pixels) and median filters (The median filter is a non-linear filter that helps in reducing noise in an image while preserving edges. The algorithm substitutes the value of each pixel with the median value derived from its neighboring pixels.) and the technique turned out to be resistant to those attacks as well.

Once all testing with filters is completed we also tested the proposed technique by cropping some portion of the image and applying image compression. While trying to retrieve the watermark we found that the watermark was retrieved without much degradation.

Thus, our proposed technique is resistant to noise attacks, filter attacks, image compression, application of sharpening, averaging and cropping. These experiments were carried out for checking the method's robustness. The table 1 shows the Structural Similarity Index Parameter for the watermarks obtained after various attacks on the image.

TABLE I. SSIM FOR VARIOUS ATTACKS

<i>Attack Type</i>	<i>Extracted Watermark</i>	<i>Structural Similarity Index (SSI)</i>
Original Watermark		0.992217246 8027256
Gaussian Noise (mean = 0, standard Deviation = 49)		0.991154353 2354701
Salt and Pepper Noise (with strength = 0.2)		0.990426729 5044367

<i>Attack Type</i>	<i>Extracted Watermark</i>	<i>Structural Similarity Index (SSI)</i>
Sharpening the image by 3*3 filter		0.993067955 3452366
Averaging the image by 3*3 filter		0.996919923 2092615
Image compression		0.993674040 9945721
Image Cropping		0.997925650 9344983
Median Filtering using 3*3 mask		0.993442656 7792107

V. CONCLUSION

In this paper, our proposed digital image watermarking technique combines Fibonacci scrambling, image rotation, and DCT embedding to achieve a robust, secure, and imperceptible watermarking scheme. The integration of these techniques enhances the security and integrity of the watermark, making it resistant to attacks and unauthorized manipulations. The objective of our proposed method is to enhance the security and robustness of watermarking while maintaining a high level of imperceptibility which is successively achieved. Fibonacci scrambling process adds an extra layer of security to the watermark, ensuring its integrity and authenticity.

Furthermore, we have incorporated image rotation as an additional step in the watermarking process. By rotating the image clockwise by a specified number of units, we introduce a spatial transformation that further enhances the security of the watermark. This rotation makes it challenging for unauthorized users to detect the watermark or manipulate the image without distorting the embedded watermark.

As we have used two level scrambling, our technique proves to be more secure against any kind of attacks which has been tested successfully. The DCT provides a frequency-based representation of the image, and by modifying specific DCT coefficients, we embed the watermark in a manner that is imperceptible to the human eye. This ensures that the watermarked image retains its visual quality while carrying the embedded information. Through extensive experimentation and analysis, we have demonstrated the effectiveness and reliability of our proposed method.

REFERENCES

- [1] Verma, Lalita, and Sanjay Pratap Singh Chauhan. "A review on Digital Image Watermarking using transformation and optimization techniques." In 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), pp. 1008-1012. IEEE, 2020.
- [2] Pal, Purnima, Harsh Vikram Singh, and Sarvesh Kumar Verma. "Study on watermarking techniques in digital images." In 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), pp. 372-376. IEEE, 2018.
- [3] Sridhar, B., and C. Arun. "A wavelet based image watermarking technique using image sharing method." In 2013 International Conference on Information Communication and Embedded Systems (ICICES), pp. 629-633. IEEE, 2013.
- [4] Xuehua, Jiang. "Digital watermarking and its application in image copyright protection." In 2010 International Conference on Intelligent Computation Technology and Automation, vol. 2, pp. 114-117. IEEE, 2010.
- [5] Salama, Ahmed, Randa Atta, Rawya Rizk, and Fayez Wanes. "A robust digital image watermarking technique based on wavelet transform." In 2011 IEEE International Conference on System Engineering and Technology, pp. 100-105. IEEE, 2011.
- [6] Xuehua, Jiang. "Digital watermarking and its application in image copyright protection." In 2010 International Conference on Intelligent Computation Technology and Automation, vol. 2, pp. 114-117. IEEE, 2010.
- [7] Duang, Yifang, Yi Wang, Congjun Cao, and Xiaolin Zhang. "Research on Digital Watermarking Algorithm Based on Discrete Cosine Transform." In 2022 15th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI), pp. 1-6. IEEE, 2022.
- [8] Yong, Xie, Wu-yang Shan, Xiao-long Cao, and Qi-qin Feng. "Analysis and comparison of holographic and traditional digital image watermarking in DWT domain." In 2012 7th International Conference on Computer Science & Education (ICCSE), pp. 790-793. IEEE, 2012.
- [9] Charu Jain, "Watermarking Algorithm using Bacterial Foraging Optimization," in International Journal of Recent Research Aspects ISSN: 2349-7688, vol. 2, Issue 1, March 2015.
- [10] Heena, Dr Himanshu Aggarwal. "Color Image Quantization Based on Euclidean Distance Using Bacteria Foraging Optimization." IJECSE Volume 1 4 (2012): 2285-2290.
- [11] Abdullatif, Mohammad, Akram M. Zeki, Jalel Chebil, and Teddy Surya Gunawan. "Properties of digital image watermarking." In 2013 IEEE 9th international colloquium on signal processing and its applications, pp. 235-240. IEEE, 2013.
- [12] Shelke, R. D., and Milind U. Nemade. "Audio watermarking techniques for copyright protection: A review." In 2016 International Conference on Global Trends in Signal Processing, Information Computing and Communication (ICGTSPICC), pp. 634-640. IEEE, 2016.
- [13] Yamuna, G., T. Shankar, and U. Vanitha. "Protection of Digital Image Based on Wavelet Transform." CiiT International Journal of Digital Image Processing 3, no. 13 (2011): 864-867..
- [14] Mondal, Bhaskar. "Cryptographic image scrambling techniques." Cryptographic and Information Security Approaches for Images and Videos; Ramakrishnan, S., Ed (2018): 37-65.
- [15] Abdullah, Mohammed AM, Satnam S. Dlay, Wai L. Woo, and Jonathon A. Chambers. "A framework for iris biometrics protection: a marriage between watermarking and visual cryptography." IEEE Access 4 (2016): 10180-10193.
- [16] Abdullah, Mohammed AM, Satnam S. Dlay, Wai L. Woo, and Jonathon A. Chambers. "A framework for iris biometrics protection: a marriage between watermarking and visual cryptography." IEEE Access 4 (2016): 10180-10193.
- [17] Dai, Congying. "Analysis on Digital Watermarking Technology and Its Applications." In 2022 International Conference on Data Analytics, Computing and Artificial Intelligence (ICDAI), pp. 200-204. IEEE, 2022.
- [18] Anand, Ashima, and Amit Kumar Singh. "Dual watermarking for security of COVID-19 patient record." IEEE Transactions on Dependable and Secure Computing 20, no. 1 (2022): 859-866.
- [19] Agarwal, Charu, Anurag Mishra, and Arpita Sharma. "Digital image watermarking in DCT domain using fuzzy inference system." In 2011 24th Canadian Conference on Electrical and Computer Engineering (CCECE), pp. 000822-000825. IEEE, 2011.