International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Efficient Watermark Embedding and Extracting in Raw Digital Video: Leveraging the Least Significant Bit Technique in the Spatial Domain

[1]Hajar Maseeh Yasin, [2]Amira B. Sallow, [3]Riyadh Zaghlool Mahmood

Submitted: 26/06/2023 **Revised:** 06/08/2023 **Accepted:** 28/08/2023

Abstract: With the emergence of the internet, digital media creators have been able to distribute their works by making them available on web pages or public chatting forums. The person with permission to access these pages or forums can copy these media, modify them, and get an identical original copy. Using digital content has shown various issues, like how authors can ensure the copyright of their works. Additional information has been included with multimedia to protect the media before distribution. This research proposed a new method for embedding watermarks in colored videos in the spatial domain. The embedding and extracting process of the watermark is based on the principle of probability. The embedding process occurs in the Least Significant bit (LSB) of the pixel, determined by the probability of whether the number of "1" in the least Significant Nibble (LSN) of the pixel is even or odd. If it's even, and the watermark bit is "1", the second bit of the pixel will be complemented; otherwise, the pixel remains unchanged. If it's odd, and the watermark bit is 0, the complement will be done on the second bit; otherwise, there is no change. To preserve imperceptibility and quality, this process applies to all video frames, specifically in the blue channel. After undergoing proposed attacks, watermark extraction from the video is also based on the probability principle. It involves collecting even LSNs and comparing them with the total number of pixels in one block. If the sum exceeds the total count of pixels in the block, the extracted bit is 0; otherwise, it's 1. The effectiveness of the proposed algorithm is demonstrated by obtaining optimal values for quality metrics like PSNR, SSIM, and MSE. Regarding robustness, the Normalized Cross-Correlation (NCC) metric is used, yielding highly favorable results that showcase the algorithm's strength and ability to extract watermarks after various attacks, such as distortion and geometric attacks like cropping and resizing. This system is perfect in terms of Imperceptibility, Data Payload, Computational Complexity, Computational Time and Error Probability.

***Keywords**: Watermark, Digital Video Watermarking, Least Significant Bit (LSB), Least Significant Nibble (LSN), Uncompressed Video, Spatial Domain.*

1. Introduction

Digital watermarking is a technique used to hide information in digital multimedia like images, audio, and videos. This hidden information, a watermark, helps identify the content, track its distribution, or verify its authenticity [1]. It's essential in today's digital age because it helps protect intellectual property rights by identifying and securing digital content. Watermarking is widely used for copyright protection, content authentication, and digital forensics [2].

[1]Duhok Polytechnic University, Technical College of Informatics/Akre, Duhok, Kurdistan Region, Iraq, hajar.yaseen@dpu.edu.krd.

[2]Duhok Polytechnic University, Technical College of Administration, Duhok, Kurdistan Region, Iraq, amira.bibo@dpu.edu.krd

[3]University of Mosul, Computer Science, Mosul, Iraq, riyadh.zaghlool@uomosul.edu.iq

Video watermarking is a popular way to protect copyrights and intellectual property in the digital world. Copyright owners can trace unauthorized distribution and prevent piracy by embedding invisible watermarks into videos. These digital markers contain information about the copyright holder or licensing details, deterring infringement and helping with legal action. Video watermarking not only discourages piracy but also ensures the integrity and ownership of video content, promoting a safer environment for creators and their work [3].

In digital forensics, video watermarking plays a crucial role in authenticating and tracing the origin of multimedia content. Watermarks embedded in videos help forensic experts establish ownership, detect tampering, and verify the integrity of digital evidence. They provide essential information like timestamps and digital signatures, aiding in identifying unauthorized modifications. Video

watermarking strengthens the ability to uncover the truth and maintain the accuracy of digital media in a complex digital landscape [4].

Digital video watermarks can be categorized into two types: fragile and robust. Fragile watermarks are highly sensitive and easily detectable, ideal for ensuring the integrity and authenticity of digital content. They're used for sensitive documents or multimedia files that require immediate identification of modifications or tampering [5]. Also, the fragile watermarks are not designed to withstand intentional attacks or alterations [6]. In contrast, robust watermarks are designed to resist various attacks and modifications while remaining detectable and recognizable. They're commonly used for copyright protection and tracking ownership. Robust watermarks use advanced techniques to embed the watermark within the content, making it resilient to familiar image and video processing operations [7].

Video watermarking can be implemented in the spatial domain or frequency domain. Watermarks directly modify the video frames' pixel values in the spatial domain. It's a simple and efficient approach suitable for real-time applications [8]. However, it's more susceptible to video processing operations and can cause noticeable distortions if not done carefully. In the frequency domain [9], watermarking leverages the mathematical properties of video's frequency components. Embedding watermarks in specific frequency bands offers robustness against standard signal processing operations while minimizing visual distortions. Frequency domain watermarking requires more computational resources and complicates the extraction process [10]. The choice between spatial and frequency domain watermarking depends on factors like robustness, perceptual quality, and computational constraints.

Time efficiency and reducing computational calculations are crucial aspects of digital video watermarking. By minimizing the processing time and computational load required for embedding or extracting watermarks, the overall efficiency of the watermarking system improves significantly [11]. This is particularly important for real-time applications where quick and seamless watermarking is essential. Reduced computational calculations enhance the speed of watermarking operations and contribute to lower resource consumption, enabling the implementation of watermarking techniques in a broader range of devices with varying processing capabilities. Optimizing time and computational calculations in digital video watermarking ensures efficient and effective protection of intellectual property rights without compromising performance or user experience [12]. Therefore, this research used the LSB technique in the spatial domain to hide the watermark within the video frames. Simultaneously, we developed a novel method to enhance the difficulty of detecting and identifying the watermark by potential intruders. This system also exhibits robustness against various video attacks, including resizing, median filtering, rotation, cropping, and JPEG compression.

The remaining sections are organized as follows: Section 2 reviews digital video watermarking in the spatial domain. Section 3 demonstrates the bit selection for embedding watermark bits in this system. Section 4 explains the proposed algorithm in terms of embedding and extraction. The discussion of experimental results is presented in Section 5, and Section 6 concludes.

2. Related Work

Watermarking techniques can be classified from various angles, and one significant aspect is their resilience to image processing attacks. In the context of withstanding image processing attacks, watermarking can be broadly grouped into three categories: 1. Robust watermarking [13], [14], [15], [16], [17], 2. Fragile watermarking [18], [19], [20], [21], [22] and 3. Semi-fragile watermarking [23], [24], [25], [26]. Furthermore, watermarking methods can be categorized based on the domain in which the watermark is embedded: spatial domain and frequency domain. The spatial part is notable for its low computational complexity and straightforward implementation [27]. To address limitations associated with spatial domain approaches, transform-based techniques have been developed. These methods involve initially transforming the image domain through various frequency transforms, which results in distinct coefficient values, then employed for watermark insertion. This field is continuously advancing and evolving with the types of transformations used [28]. Common changes in frequency domain watermarking encompass the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT), among others [29].

Video watermarking methods exhibit a broad spectrum of diversity, and we will provide a list of studies focused on embedding watermarks within video frames using spatial domain techniques. Video watermarking represents an uncomplicated extension of image watermarking.

Amit Kumar et al. [30] extensively delves into the Least Significant Bit (LSB) technique, thoroughly examining its application across diverse color images. Their exploration extends to employing the LSB method on grayscale images while introducing factors like noise and cropping. The approach involves segmenting the cover image into blocks with watermark bits strategically embedded. This embedding occurs not only in the first bit of each pixel but also across the second, third, and fourth bits, thereby enriching the watermarking process.

Vani and et al. [30] introduce a novel approach to scene-based watermarking, focusing on blind extraction. Their method involves embedding eight bit-plane images derived from a single grayscale watermark image into various scenes within a video sequence. The algorithm selects luminance values from video frames, organizes them into groups, and then embeds watermark bits by manipulating the relative relationships within each group. This process ensures the successful embedding of many watermark bits into the video frames while maintaining minimal distortion. Importantly, their approach enables accurate watermark retrieval during extraction, even when subjected to diverse video manipulations and signal processing attacks.

V. Bánoci and et al. [31] introduced a 2D Spread Spectrum watermarking scheme tailored for video multimedia files. The proposed approach involves embedding the first watermark spreading across frames (time dimension) and subsequently modulating watermark bits within each frame. The utilization of two-dimensional modulation employing PN orthogonal sequences contributes to a robust and adaptive system, effectively combining domain usage and embedding regions to withstand various attacks and ensure copyright protection.

R. Al-Janabi [32] introduced a secure watermarking method involving two stages. In the initial stage, an eight-number secret key, ranging from 0 to 7, designates specific bit positions in individual pixels of the cover image. Based on whether the corresponding bit in the watermark is (0) or not, it is stored in the LSB of the watermarked image. The subsequent stage offers the capability to generate multiple secret keys through shift and rotate operations. Notably, the watermark is redundantly embedded across all extracted image blocks to enhance image protection. This approach ensures heightened security due to its avoidance of direct LSB storage and its utilization of multiple secret keys.

J. Upadhyay and et al. [33] propose a color video watermarking method using DWT and LSB. The approach involves embedding a watermark image into the least significant bit of original video pixels using the LSB technique. They start by dividing the original color video into frames, then converting them into separate R, G, and B components. Applying 2D DWT to each color component follows this step. The R, G, and B approximation coefficients are combined, and the frames are divided into non-overlapping blocks. The watermark is hidden within the 4th to 7^{th}-bit layers of the approximation coefficients of the original video. This LSB watermarking method conceals data within the least significant bit of the actual video pixels. After embedding, an inverse DWT is applied, and the video frames are merged to create the watermarked video.

The method employed by N. F. Hassan and R. Abbas [34] involves a watermarking algorithm designed for secret message embedded within digital videos in a spatial domain. Their approach strategically leverages edge and corner regions in video frames as optimal host locations for concealing secret bits. This choice is motivated by these regions' characteristics of color variation, which ensures minimal impact on color uniformity and transparency. The embedding process is executed through frame decomposition, selecting edges and corners as host locations and utilizing the LSB technique for watermark message embedding. While corner regions accommodate fewer embedded bits compared to edge regions, their inconspicuous nature poses challenges in detection.

3. Bit Selection for Watermarking

In this paper, we have embedded the watermark in every video frame. Therefore, before illustrating the applied embedding method, it is necessary to indicate the areas in the frame where the watermark data can be hidden without distortion or manipulation of the video content. This ensures that the watermark remains recognizable and distinguishable by users.

Various data hiding techniques within images demonstrate that hiding information in the least

significant bit (LSB) of each image pixel, or even in the subsequent bit, does not significantly affect the original image's characteristics, regardless of its texture. Each image pixel is represented by a byte with 256 color levels, as shown in Figure 1.

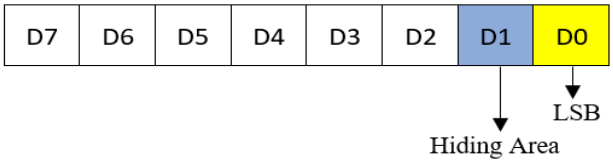


Fig 1. bit Location for Watermark embedding

Modifying the least significant bit (LSB) of the D0 image pixel can alter its value by 0 or 1, resulting in a change of only one number in its representation. Similarly, changing the second bit, D1 would cause the pixel value to increase or decrease by 2. In both cases, the original image's changes are imperceptible after the embedded process, as these specific pixel locations, which are to be concealed, are substituted with the watermark bits. It is essential to emphasize that in this proposed system, the second bit of each pixel in the frame was selected and replaced with a watermark bit to strategically mitigate potential video attacks, such as filtering, cropping, rotation, median filtering, and compression.

4. Proposed System

The technique utilized in this research relies on the method of uniformly distributing watermark bits across all sections of an individual video frame. This is achieved by employing the LSB (Least Significant Bit) technique in the spatial domain. The subsequent section will elaborate on the embedding algorithm proposed for the system and the process for extracting the watermark.

4.1 Watermark Embedding

The embedding process involved utilizing the second bit of each pixel in the video frame. Figure 2 illustrates the proposed method for watermark embedding, where the system extracts the first frame from the video and partitions it into blocks. The number of blocks in each row is determined by the number of bits in the row of the watermark image, and the number of bits in the column of the watermark image determines the number of blocks in each column. The calculation for the number of pixels in each block row is governed by Equation (1), while the number of pixels in each column is determined using Equation (2).

BR=RF/RW …….. (1)

BC=CF/CW ……..…… (2)

Where:

BR: Row size in the block, RF: Row size of the Frame, RW: Row size of the watermark image, BC: Column size in the block, CF: Column size of the Frame, CW: Column size of the watermark image.

The embedding process relies on comparing specific bits in the pixels of extracted blocks within the frame to the corresponding bits in the watermark. Prior to comparison, the system extracts the Least Significant Nibble (LSN) from each pixel and calculates the summation of ones. No action is taken if the summation is even and the watermark bit is 0. Conversely, if the summation is odd and the watermark bit is 0, the system performs a complement operation on the second bit of the pixel. The pixel remains unchanged if the summation is odd and the watermark bit is 1. For illustration, Table 1 presents four example pixels, showcasing the comparison and pixel alteration during the watermark embedding process. In the Parity column, 0's indicate an even summation of ones in the LSN, while 1's indicate an odd summation. The (D1) designation denotes the complement of the second bit.

Table 1. Explain all possibilities for the embedding process.

	Pixel in Blue Channel	LSN	Parity	Watermark bit	Operation	Result
Pixel#1	10110101	0101	0	0	No Change	10110101
Pixel#2	11010100	0100	1	0	$\overline{D1}$	11010110
Pixel#3	01011100	1100	0	1	$\overline{D1}$	01011110
Pixel#4	10101011	1011	1	1	No Change	10101011

International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

In the proposed embedding process, we hide the watermark image's bits within the video frames systematically. We start by concealing the first bit of the watermark in the first block of the initial frame. Then, we proceed to the second bit, hiding it within the second block, and continue this process until all the bits are embedded within the watermark image for the first frame. Afterward, we move on to the second frame and repeat the same process until we complete all frames in the video. The following steps outline the entire embedding process for the system:

1. Read AVI video file.
2. Read Watermark.
3. Pick the first frame of the current video file.
4. Calculate row blocks which is equal to No. of row pixels in watermark.
5. Calculate col blocks which is equal to No. of col pixels in watermark.
6. Calculate block size as:
   Block row size=No. of row in frame/number of row in watermark.
   Block col size=No. of col in frame/number of col in the watermark.
7. Pick the first block of frame of size.
8. Pick the first pixel of the block.
9. Calculate the parity of LSN of the pixel
10. If parity is not equal to D1 of the current pixel, then complement D1.
11. If there is a pixel in the current block, pick the next pixel and go to step 9.
12. If there is a block of the current frame, pick the next one and go to step 8.
13. Append the Watermarked frame to the Video object.
14. If there is a frame in the current video file, pick the next frame and go to step 7.
15. End

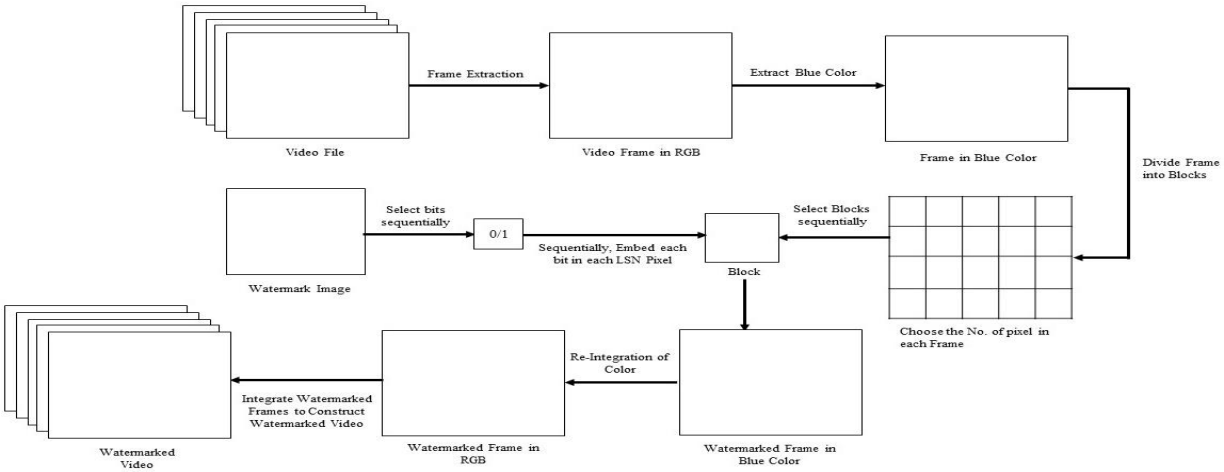


Fig 2. Block Diagram for Proposed Watermark Embedding

4.2 Watermark Extract

Figure 3 demonstrates the watermark extraction process. The extraction of the hidden watermark is as crucial as the embedding process. The successful recovery of the watermark is essential for establishing ownership of the resources. The extraction procedure involves using the watermarked video as input, and as a result, the system retrieves the hidden watermark image.

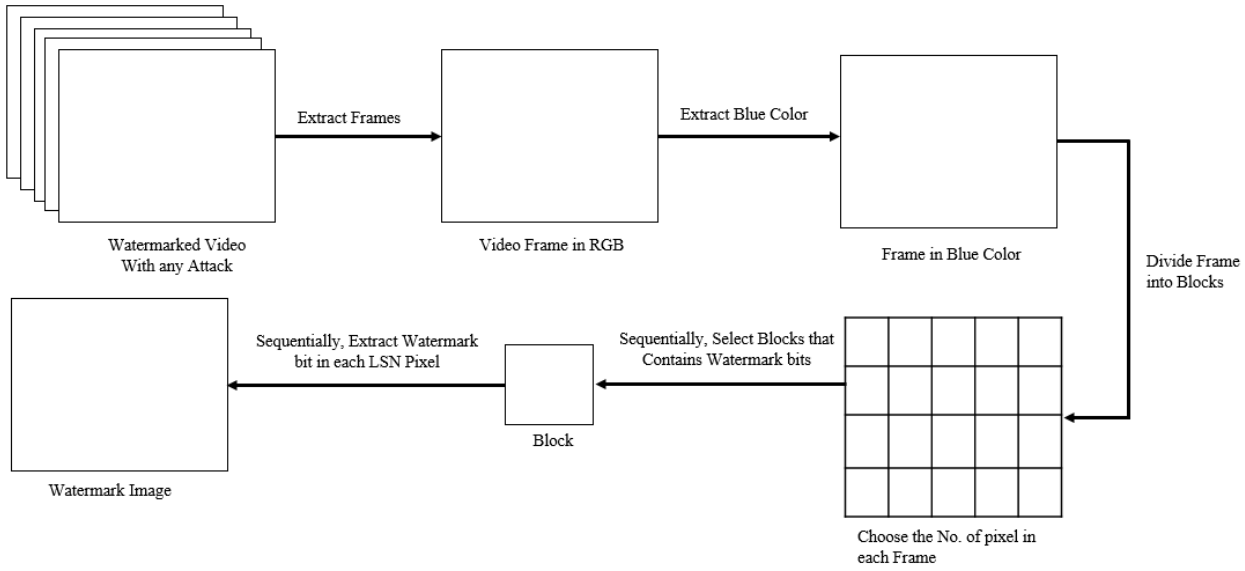


Fig 3. Block Diagram for Proposed Watermark Extraction.

The method used in the merging process is the same as the one used in the retrieval method in terms of extracting the frame, dividing it into blocks, and determining the block size. Once the block size for extracting the watermark image is selected, the process begins with the first block. In the first block, the system set a counter to calculate the sum of 1s from the LSN in each pixel. If the sum is even, the counter increments by one; otherwise, it remains unchanged. Afterward, the system checks if the counter is greater or smaller than half the number of pixels in the block. If the counter is greater than half, the system takes the bit 0 and sets it as the first bit to form the watermark image. On the other hand, if the counter is smaller than half, bit 1 is appended to the watermark image. This process continues until all pixels in the first block are processed. The system continues to follow the same approach for all blocks in the first frame until all bits forming the watermark image are extracted. It is recommended to extract the watermark from all frames to ensure a clearer watermark image, especially when the video might be subject to attacks or alterations. To achieve this, the system applies the same process to extract the watermark image from the first frame and repeats it for all remaining frames in the video. The following steps provide a detailed explanation of the entire process of extracting the watermark image from all frames in the watermarked video:

1. Read Watermarked AVI video file.
2. Pick the first frame of the current video file.
3. Calculate row blocks that are equal to no. of row pixels in the watermark.
4. Calculate col blocks that are equal to no. of col pixels in the watermark.
5. Calculate block size as:
   Block row size=No. of the row in the frame/number of rows in the watermark.
   Block col size=No. of col in frame/number of col in the watermark.
6. Pick the first block from the frame of size.
7. Set sum = 0.
8. Pick the first pixel of the block.
9. Calculate P, which is the parity of LSN of the pixel.
10. Sum = sum + P.
11. If there is a pixel in the current block, pick the next pixel, and go to 9.
12. If sum> 0.5*(row pixels in Block* col pixels in Block), then append ‘1’ to the watermark; otherwise append ‘0’.
13. If there is a block of the current frame, pick the next block of frame size (12x16), and go to 7.
14. If there is a frame in the current video file, pick the next frame, go to 6.
15. End.

5. Results and Discussion

In this section, we will delve into the experiments conducted to evaluate the performance of the watermarking algorithm and architecture proposed in the preceding sections.

5.1 Experimental setup

The proposed algorithm is implemented using MATLAB R2018a. The experiment is conducted on the system equipped with an Intel(R) Core i7-10750H CPU @ 2.60GHz and 16 GB of RAM operating on Windows 10. To evaluate the algorithm's performance, four standard color videos, "Akiyo", “Football”, "Johnny", and

"PedestrianArea" are used with different sizes and characteristics, as shown in Table 2. The binary watermark size is set to (64 x 40), and 100 frames are utilized from each video for the simulation. Figure 4 displays snapshots from all four test videos and watermark.

Specifically, the blue channel of the video frames is chosen for the embedding and extraction process; this can be attributed to several reasons. Firstly, the human visual system is generally less sensitive to changes in the blue channel than the red and green channels, making the watermark less visually noticeable and reducing the likelihood of detection and tampering. Secondly, video compression techniques often employ chrominance subsampling, which reduces the resolution and precision of the color channels, with the blue channel typically having a lower resolution. This characteristic can be leveraged to make the watermark less susceptible to compression artifacts. Lastly, the blue color channel may exhibit specific statistical properties that make it suitable for watermark embedding. For instance, if the video content displays more dominant or consistent patterns in the red and green channels, embedding the watermark in the blue channel can enhance its robustness against intentional or unintentional modifications.

Fig 4. Snapshots of the six test videos. (a) Akiyo. (b) Football. (c) Watermark. (d) Johnny. (e) PedestrianArea.

Table 2. Details of the videos used

Video Name	Akiyo	Football	Johnny	Pedestrian Area
Video Width	768	768	1280	1920
Video Height	640	640	720	1080
Frame Rate	30	30	60	25
Video Format	RGB24	RGB24	RGB24	RGB24

5.2 Execution efficiency

Within this subsection, a series of simulation experiments are conducted employing various strategies to demonstrate the algorithm's efficacy. The average time taken for embedding and extraction per frame is computed for each strategy. The process of embedding the watermark occurs within the spatial domain, encompassing the video frames' blue segments through utilizing the LSN technique. Similarly, the extraction of the watermark is executed following a parallel procedure. The outcomes obtained from assessing

all tested videos are meticulously presented in Table 3.

Table 3. Time efficiency for tested videos in second

Video Name	Embedding Time	Extracting Time
Akiyo	10.2307	10.1246
Football	10.3723	10.1432
Johnny	20.9148	18.9025
PedestrianArea	44.2567	42.3088

5.3 Quality Check

Comprehensive simulation operations are conducted to verify the proposed algorithm using diverse video clips, as mentioned in section 5.1. The embedding process is implemented on the blue part of the tested video. Therefore, to assess the quality of video frames after the embedding process, several metrics were employed between the original blue color and watermarked blue, which can be elaborated as follows, along with the statement of the average values obtained from each metric:

A. Mean Squared Error (MSE): is a fundamental metric that quantifies the dissimilarity between the original and watermarked video frames. Mathematically, it is expressed by Equation (3) [35].

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(I_{Original}(i) - I_{Watermarked}(i))^2 \quad \ldots\ldots. (3)$$

Here, (*N)* represents the total number of pixels in a frame, and ($I_{Original}$) and ($I_{Watermarked}$) denotes the intensity values of the (*i*)-th pixel in the original and watermarked frames, respectively. The resulting average MSE between $3.0035x10^{-5}$ and $3.131x10^{-5}$ signifies that, on average, the squared differences between corresponding pixels are exceedingly small. This suggests that the watermarking process introduced minimal distortion to the video frames.

B. Peak Signal-to-Noise Ratio (PSNR): is a standard quality measurement that quantifies the ratio of the maximum possible signal value to the noise introduced during watermarking. It is computed by Equation (4) [36].

$$PSNR = 10\,.\,log_{10}(\frac{MAX^2}{MSE}) \quad \ldots\ldots\ldots (4)$$

Here, (*MAX*) represents the maximum possible pixel value, and (*MSE*) is the previously calculated Mean Squared Error. The average values of PSNR 45.2238, 45.0601, 45.1048, and 45.0434 obtained from "Akiyo", "Football, "Johnny" and "PedestrianArea", respectively, are notably high, indicating that the watermarking process has preserved the perceptual quality of the video frames remarkably well. Higher PSNR values indicate better fidelity between the original and watermarked frames.

C. Structural Similarity Index (SSIM) is a perceptual metric that assesses the structural similarity between two images. It is defined by the Equation (5) [37]:

$$SSIM_{(x,y)} = \frac{(2\mu_x\mu_y+C_1).(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_y^2+C_1).(\sigma_x^2+\sigma_y^2+C_2)} \quad \ldots\ldots\ldots (5)$$

Here, (x) and (y) denote the original and watermarked frame, respectively. μ_x, μ_y, σ_x and $\sigma_y$represent mean and standard deviation values of the pixel intensities, while (σ_{xy}) signifies the covariance between (x) and (y). The constants (C_1) and (C_2) are used for stability. The SSIM (0.9868, 0.9745, 0.9831 and 0.9820) indicates a high degree of structural similarity, underscoring the minimal perceptual differences between the two frames.

D. Normalized Absolute Error (NAE) measures the normalized average absolute difference between the original and watermarked frames. It is computed by Equation (6) [38]:

$$MSE = \frac{1}{N}\sum_{i=1}^{N}\frac{|I_{Original}(i) - I_{Watermarked}(i)|}{MAX} \quad \ldots\ldots\ldots (6)$$

Like MSE, (*N*) denotes the total number of pixels, and (*MAX*) represents the maximum pixel value. The NAE value of (0.0093, 0.0170, 0.0072 and 0.0131) indicates that, on average, the pixel-wise differences between the frames are minimal and normalized, signifying a high level of similarity.

E. Average Difference (AD) provides insight into the average pixel-wise difference between the original and watermarked frames without normalization. Mathematically, it is calculated by Equation (7) [39]:

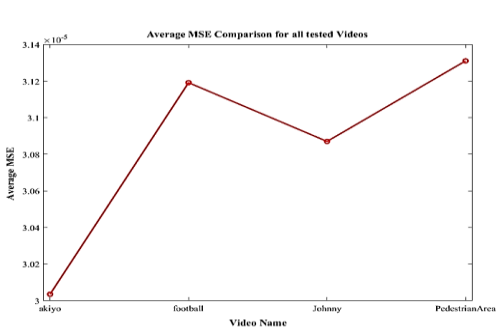
$$AD = \frac{1}{N}\sum_{i=1}^{N}|I_{Original}(i) - I_{Watermarked}(i)| \quad \ldots\ldots\ldots (7)$$

Once again, (*N*) represents the total number of pixels. The AD value of (0.0038, 0.004 and 0.0039) indicates a low average pixel-wise difference between the frames, further corroborating the minimal differences introduced by the watermarking process.

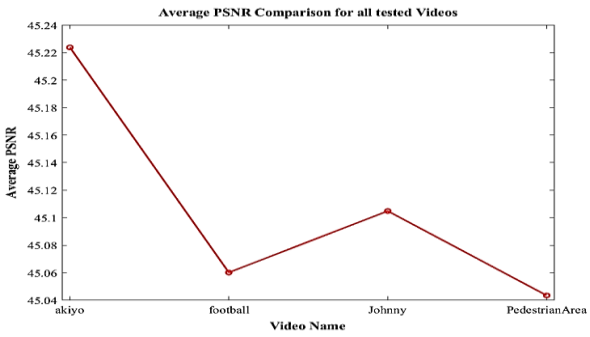
Table 4 display the results values for all measurement used. As shown in this table, the obtained results collectively underscore the fidelity of the video watermarking technique. The consistently low values of MSE, NAE, and AD, coupled with the high values of PSNR and SSIM, collectively suggest that the watermarking process effectively embeds the watermark while preserving the visual quality of the video frames. Furthermore, there are no significant values when the measurements are applied to videos of different sizes. This indicates that the embedding process is more effective when applied to SD, HD, and FHD videos. The distortion rate could be negligible for the human visual system. These metrics demonstrate the technique's potential to withstand distortions and maintain the original content's integrity. Figure 5 plot the values obtains from each quality measurement.

Table 4. Results of the used quality metrics after the hiding process.

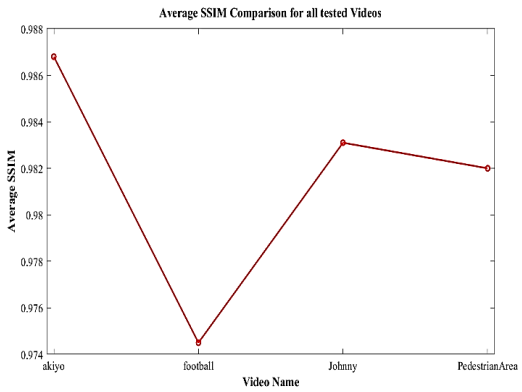
Video	MSE	PSNR	SSIM	NAE	AD
akiyo	3.0035e-05	45.2238	0.9868	0.0093	0.0038
football	3.1191e-05	45.0601	0.9745	0.0170	0.0040
Johnny	3.087e-05	45.1048	0.9831	0.0072	0.0039
PedestrianArea	3.131e-05	45.0434	0.9820	0.0131	0.0040



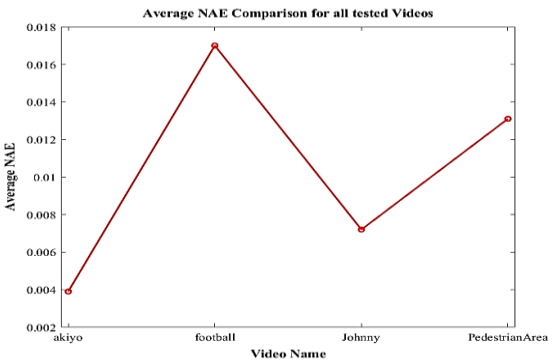
(a)



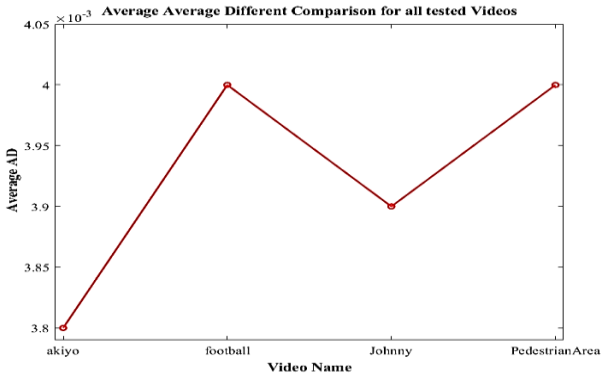
(b)



(c)



(d)



(e)

Fig 5: Plot of Quality Metric Values: (a) MSE. (b) PSNR. (c) SSIM. (d) AD. (e) NAE.

5.4 Robustness Against Attacks

The robustness of the proposed algorithm is validated by using various attacks, such as noise, geometric and JPEG compression attacks. To test the algorithm's robustness against noise attacks, we add salt & pepper noise to the watermarked videos; the density of salt & pepper noise is 0.05, which means about 5% of the pixels in a frame are affected. Geometric transformations are the most challenging attacks for watermarking algorithms. Here we rotate the watermarked videos by various degrees (5°, 10°, 15° and 20°) and extract the watermark from the rotated videos without performing synchronization. The robustness of the algorithm against scaling attacks is also tested. We downscale each watermarked video to 20% of its original size and extract the watermark from the downscaled videos. In addition, we implement cropping attacks by cropping 20% of the pixels from each side of the watermarked video. Finally, the JPEG compression process is done on each frame in the watermarked video with value 85 as quality, then we extract the watermarked from the compressed frame. The algorithm's robustness is evaluated by quantifying the Normalized Cross Correlation (NCC) value between the original and extracted watermarks, as defined in Equation (8). The variables ($W_{Original}$) and ($W_{Extracted}$) represent the original and extracted watermark image, respectively, whereas ($\overline{W_{Original}}$) and ($\overline{W_{Extracted}}$) correspond to the mean pixel values of the original and extracted watermark. The variable (N) pertains to the total pixel count within the frame.

$$NCC(A,B) = \frac{\sum_{i=1}^{N}\left(W_{Original_i}-\overline{W_{Original}}\right)-\left(W_{Extracted_i}-\overline{W_{Extracted}}\right)}{\sqrt{\sum_{i=1}^{N}\left(W_{Original_i}-\overline{W_{Original}}\right)^2-\sum_{i=1}^{N}\left(W_{Extracted_i}-\overline{W_{Extracted}}\right)^2}} \quad \ldots\ldots\ldots (8)$$

Evaluating the watermarked videos under various attack scenarios provides valuable insights into the robustness and effectiveness of the watermarking technique. Table 5 shows the best NCC values for each watermarked video obtained during apply mentioned attacks.

Table 5. NCC Values with Different Attacks

Video Name	akiyo	football	Johnny	PedestrianArea
No Attack	1	1	1	1
Median Filter	1	1	1	1
Cropping 10%	0.6665	0.6665	0.6665	0.6665
Rescaling 20%	0.9875	0.9958	0.9402	0.9859
Rotation 45^0	0.7311	0.7311	0.7311	0.7311
JPEG Compression	0.7458	0.7941	0.7640	0.6802

As shown in Table 5, the results demonstrate the robustness of the watermark extraction technique in the face of various attacks. We observe that all videos are unaltered and subjected to noise; the extracted watermarks maintain a strong correlation with the original. However, when subjected to cropping, the NCC values drop to approximately 0.6665 for all videos, indicating a significant reduction in accuracy. Rescaling results in reasonably high NCC values, reflecting a moderate

impact on extraction accuracy. On the other hand, rotating the frames and applying JPEG compression lead to consistent NCC values of approximately 0.7311 and a range of 0.6802 to 0.7941, respectively, highlighting the technique's vulnerability to these transformations and compression. The findings underscore the technique's robustness against noise and modest rescaling but also emphasize its sensitivity to cropping, rotation, and compression attacks.

We conclude from the above the NCC values for watermark extraction are generally close to 1 for most cases, indicating a high level of correlation between the extracted watermark and the original watermark image. Moreover, this system demonstrates the watermarking technique's strength against noise and moderate rescaling but highlights areas of concern, particularly in cropping, rotation, and JPEG compression cases. These results inform practical applications of the proposed technique, emphasizing its suitability for specific scenarios and suggesting avenues for further enhancement. Figure 6-9 shows the watermark image extracted from the video after it was subjected to the previously mentioned attacks with NCC values.

NCC = 1 (a) NCC = 0.6665 (b) NCC = 0.9875 (c) NCC = 0.7311 (d) NCC = 0.7458 (e)

Fig 6. Watermark image extracted from "**akyio**" video with NCC value after attacks: (a) Median Filter. (b) Cropping. (c) Rescaling. (d) Rotation. (e) JPEG compression.

NCC = 1 (a) NCC = 0.6665 (b) NCC = 0.9958 (c) NCC = 0.7311 (d) NCC = 0.7941 (e)

Fig 7. Watermark image extracted from "**football**" video with NCC value after attacks: (a) Median Filter. (b) Cropping. (c) Rescaling. (d) Rotation. (e) JPEG compression.

NCC = 1 (a) NCC = 0.6665 (b) NCC = 0.9402 (c) NCC = 0.7311 (d) NCC = 0.7640 (e)

Fig 8. Watermark image extracted from "**Johnny**" video with NCC value after attacks: (a) Median Filter. (b) Cropping. (c) Rescaling. (d) Rotation. (e) JPEG compression.

NCC = 1 (a) NCC = 0.6665 (b) NCC = 0.9859 (c) NCC = 0.7311 (d) NCC = 0.6802 (e)

Fig 9. Watermark image extracted from "**PedestrianArea**" video with NCC value after attacks: (a) Median Filter. (b) Cropping. (c) Rescaling. (d) Rotation. (e) JPEG compression.

After obtaining the quality and robustness results, we would like to mention here that when we decided to select different videos types in terms of size and content, the objective was to observe whether some notable results and values could be distinguished from one type to another during the embedding process and when subjected to various attacks. In the embedding process, we observed that the quality metrics were consistent, and there was no significant difference when using videos of different types SD, HD, or FHD, all of them yielded good and valuable results. The same applies to the exposure of videos to the proposed attacks, as we did not notice any distinction between video types. From this, we conclude that the proposed algorithm applies to any video, whether it is SD, HD, or FHD, as all of them yield excellent results.

6. Conclusion

The proposed algorithm provides high-quality and blind watermarked videos. The system relies on embedding the watermark bit in the spatial domain using the LSB. The embedding process takes place in the second bit of each pixel in the video frames, specifically in the blue channel of the color video. This operation is executed based on a pre-defined condition to protect the video from watermark detection. This system stands out for its strength and robustness against various attacks to alter or remove the watermark. The embedded watermark in the video file is imperceptible within the embedded frame, and its inclusion does not cause any change or distortion in the carrier cover, i.e., the video file itself.

To evaluate the proposed system in terms of perception and robustness, four different videos were chosen in terms of size and content. Excellent values were obtained for the embedded frame quality metrics such as PSNR, SSIM, and others. Similarly, the value of the NCC demonstrated the robustness and efficiency of the research method. The diversity in video selection aimed to observe whether there were significant results and distinguishable values between different types during the hiding process and exposure to various attacks. Notably, the accuracy metrics in the embedding process remained consistent, showing no significant difference when using SD, HD, or FHD videos; all yielded very close, valuable, and almost equal results. Likewise, no distinction was observed between video types in terms of exposing the videos to the attacks used. The NCC coefficients also exhibited good and consistent values. From this, it can be inferred that the proposed algorithm applies to any type of video, whether it is SD, HD, or FHD, as all yield very good results.

Each technique comes with its own set of advantages and drawbacks, but the LSB method strikes a good balance between performance, robustness, computational cost, and embedding quality. The drawbacks of the suggested approach involve relatively higher execution time during the embedding and extraction process and the necessity of using uncompressed (or decompressed) video for watermark embedding. Due to these factors, the proposed system isn't suitable for applications that demand real-time watermark embedding or extraction, such as broadcast monitoring. However, specific other applications like copyright protection, fingerprinting, or copy control don't necessitate real-time watermarking. The proposed scheme is well-suited for labeling stored videos like DVD films or TV movies that aren't encoded and broadcasted in real-time. The watermark detection and extraction processes are carried out within a relatively short timeframe, as the algorithm only processes one or a few watermarked frames instead of the entire watermarked video.

Since the embedding and extracting process of the watermark in the proposed system is applied to all frames in the video, the execution time becomes high. Therefore, in the future, we suggest utilizing the power of programmable hardware devices such as Field-Programmable Gate Arrays (FPGAs) to accelerate the embedding and extracting process.

7. References

[1] N. Zermi, A. Khaldi, R. Kafi, F. Kahlessenane, and S. Euschi, "A DWT-SVD based robust digital watermarking for medical image security," *Forensic science international*, vol. 320, p. 110691, 2021.

[2] A. Mohanarathinam, S. Kamalraj, G. Prasanna Venkatesan, R. V. Ravi, and C. Manikandababu, "Digital watermarking techniques for image security: a review," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, pp. 3221-3229, 2020.

[3] A. Fkirin, G. Attiya, A. El-Sayed, and M. A. Shouman, "Copyright protection of deep neural

network models using digital watermarking: a comparative study," *Multimedia Tools and Applications*, vol. 81, pp. 15961-15975, 2022.
[4] R. Munir, "A secure fragile video watermarking algorithm for content authentication based on Arnold Cat Map," in *2019 4th International Conference on Information Technology (InCIT)*, 2019, pp. 32-37.
[5] B. Aditya, U. Avaneesh, K. Adithya, A. Murthy, R. Sandeep, and B. Kavyashree, "Invisible semi-fragile watermarking and steganography of digital videos for content authentication and data hiding," *International Journal of Image and Graphics*, vol. 19, p. 1950015, 2019.
[6] M. Zairi, T. Boujiha, and A. Ouelli, "Secure fragile watermarking based on Huffman encoding and optimal embedding strategy," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 29, pp. 1132-1139, 2023.
[7] H. Ding, R. Tao, J. Sun, J. Liu, F. Zhang, X. Jiang, *et al.*, "A compressed-domain robust video watermarking against recompression attack," *IEEE Access*, vol. 9, pp. 35324-35337, 2021.
[8] N. Aissaoui, R. Kaibou, and M. S. Azzaz, "Real-Time FPGA Implementation of Digital Video Watermarking Techniques using Co-Design Approach: Comparative Study," in *2022 7th International Conference on Image and Signal Processing and their Applications (ISPA)*, 2022, pp. 1-6.
[9] F. Cao, T. Wang, D. Guo, J. Li, and C. Qin, "Screen-shooting resistant image watermarking based on lightweight neural network in frequency domain," *Journal of Visual Communication and Image Representation*, vol. 94, p. 103837, 2023.
[10] E. Farri and P. Ayubi, "A robust digital video watermarking based on CT-SVD domain and chaotic DNA sequences for copyright protection," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-25, 2022.
[11] M. Bistroń and Z. Piotrowski, "Efficient Video Watermarking Algorithm Based on Convolutional Neural Networks with Entropy-Based Information Mapper," *Entropy*, vol. 25, p. 284, 2023.
[12] Q. Liu, S. Yang, J. Liu, L. Zhao, P. Xiong, and J. Shen, "An efficient video watermark method using blockchain," *Knowledge-Based Systems*, vol. 259, p. 110066, 2023.
[13] A. Bhaskar, C. Sharma, K. Mohiuddin, A. Singh, O. A. Nasr, and M. Alwetaishi, "A robust video watermarking scheme with squirrel search algorithm," *Comput. Mater. Continua*, vol. 71, pp. 3069-3089, 2022.
[14] V. Adul and E. Mwangi, "A robust video watermarking approach based on a hybrid SVD/DWT technique," in *2017 IEEE AFRICON*, 2017, pp. 309-313.
[15] A. Karmakar, A. Phadikar, B. S. Phadikar, and G. K. Maity, "A blind video watermarking scheme resistant to rotation and collusion attacks," *Journal of king saud university-computer and information sciences*, vol. 28, pp. 199-210, 2016.
[16] S. Lagzian, M. Soryani, and M. Fathy, "A new robust watermarking scheme based on RDWT-SVD," *International Journal of Intelligent Information Processing*, vol. 2, pp. 22-29, 2011.
[17] P. Yang, Y. Lao, and P. Li, "Robust watermarking for deep neural networks via bi-level optimization," in *Proceedings of the IEEE/CVF International Conference on Computer Vision*, 2021, pp. 14841-14850.
[18] A. Shehab, M. Elhoseny, K. Muhammad, A. K. Sangaiah, P. Yang, H. Huang, *et al.*, "Secure and robust fragile watermarking scheme for medical images," *IEEE access*, vol. 6, pp. 10269-10278, 2018.
[19] X. Zhang and S. Wang, "Fragile watermarking with error-free restoration capability," *IEEE Transactions on Multimedia*, vol. 10, pp. 1490-1499, 2008.
[20] L. Rakhmawati, W. Wirawan, and S. Suwadi, "A recent survey of self-embedding fragile watermarking scheme for image authentication with recovery capability," *EURASIP Journal on Image and Video Processing*, vol. 2019, pp. 1-22, 2019.
[21] K. Sreenivas and V. Kamkshi Prasad, "Fragile watermarking schemes for image authentication: a survey," *International Journal of Machine Learning and Cybernetics*, vol. 9, pp. 1193-1218, 2018.
[22] F. M. Khalifa and M. G. Saeed, "Image Watermarking Using All Phase Discrete Cosine Biorthogonal Transform in Selected Pixel Blocks," *Polytechnic Journal*, vol. 10, pp. 68-73, 2020.
[23] P. Lefèvre, P. Carré, C. Fontaine, P. Gaborit, and J. Huang, "Efficient image tampering localization using semi-fragile watermarking and error control codes," *Signal Processing*, vol. 190, p. 108342, 2022.
[24] L. Agilandeeswari, M. Prabukumar, and F. A. Alenizi, "A robust semi-fragile watermarking system using Pseudo-Zernike moments and dual tree complex wavelet transform for social media content authentication," *Multimedia Tools and Applications*, pp. 1-53, 2023.
[25] N. Sivasubramanian and G. Konganathan, "A novel semi fragile watermarking technique for tamper detection and recovery using IWT and DCT," *Computing*, vol. 102, pp. 1365-1384, 2020.
[26] A. Hammami, A. Ben Hamida, and C. Ben Amar, "Blind semi-fragile watermarking

scheme for video authentication in video surveillance context," *Multimedia Tools and Applications*, vol. 80, pp. 7479-7513, 2021.
[27] Q. Su, D. Liu, Z. Yuan, G. Wang, X. Zhang, B. Chen, *et al.*, "New rapid and robust color image watermarking technique in spatial domain," *IEEE Access*, vol. 7, pp. 30398-30409, 2019.
[28] W. Wan, J. Wang, Y. Zhang, J. Li, H. Yu, and J. Sun, "A comprehensive survey on robust image watermarking," *Neurocomputing*, vol. 488, pp. 226-247, 2022.
[29] Z. Yuan, Q. Su, D. Liu, and X. Zhang, "A blind image watermarking scheme combining spatial domain and frequency domain," *The visual computer*, vol. 37, pp. 1867-1881, 2021.
[30] P. Venugopala, H. Sarojadevi, N. N. Chiplunkar, and V. Bhat, "Video watermarking by adjusting the pixel values and using scene change detection," in *2014 Fifth International Conference on Signal and Image Processing*, 2014, pp. 259-264.
[31] V. Bánoci, M. Broda, G. Bugár, and D. Levický, "2D-Spread spectrum watermark framework for multimedia copyright protection," in *2014 24th International Conference Radioelektronika*, 2014, pp. 1-4.
[32] R. Al-janabi, "A New Digital Watermarking Algorithm Based on Image Comparison Technique," *Int.J.Computer Technology & Applications*, vol. 6, pp. 7-11, 2015.
[33] J. Upadhyay, B. Mishra, and P. Patel, "A modified approach of video watermarking using DWT-BP based LSB algorithm," in *2017 International Conference on Information, Communication, Instrumentation and Control (ICICIC)*, 2017, pp. 1-6.
[34] N. F. Hassan and R. Abbas, "Proposed video watermarking algorithm based on edge or corner regions," *Engineering and Technology Journal*, vol. 36, pp. 25-32, 2018.
[35] H. Marmolin, "Subjective MSE measures," *IEEE transactions on systems, man, and cybernetics*, vol. 16, pp. 486-489, 1986.
[36] S. Winkler and P. Mohandas, "The evolution of video quality measurement: From PSNR to hybrid metrics," *IEEE transactions on Broadcasting*, vol. 54, pp. 660-668, 2008.
[37] U. Sara, M. Akter, and M. S. Uddin, "Image quality assessment through FSIM, SSIM, MSE and PSNR—a comparative study," *Journal of Computer and Communications*, vol. 7, pp. 8-18, 2019.
[38] Z. Jalil, M. A. Jaffar, and A. M. Mirza, "A novel text watermarking algorithm using image watermark," *International Journal of Innovative Computing, Information and Control*, vol. 7, 2011.
[39] M. Alghoniemy and A. H. Tewfik, "Geometric distortion correction in image watermarking," in *Security and Watermarking of Multimedia Contents II*, 2000, pp. 82-89.
[40] Diniesh, V. C. ., Prasad, L. V. R. C. ., Bharathi , R. J. ., Selvarani, A., Theresa, W. G. ., Sumathi, R. ., & Dhanalakshmi, G. . (2023). Performance Evaluation of Energy Efficient Optimized Routing Protocol for WBANs Using PSO Protocol. International Journal on Recent and Innovation Trends in Computing and Communication, 11(4s), 116–121. https://doi.org/10.17762/ijritcc.v11i4s.6314
[41] Moore, B., Clark, R., Martinez, J., Rodriguez, A., & Rodriguez, L. Anomaly Detection in Internet of Things (IoT) Data Streams. Kuwait Journal of Machine Learning, 1(4). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/151
[42] Kamble, S.D., Saini, D.K.J.B., Jain, S., Kumar, K., Kumar, S., Dhabliya, D. A novel approach of surveillance video indexing and retrieval using object detection and tracking (2023) Journal of Interdisciplinary Mathematics, 26 (3), pp. 341-350.