iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.53489

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Time-Domain Video Watermarking Algorithm for Data Security & Content Authentication

Nishad P. Kulkarni[1], Aditya A. Patil[2], Dr. M .A Gangarde[3]
[1, 2, 3]*Pune Institute Of Computer Technology, Pune 411043, India*

Abstract: ***Video watermarking is an essential method employed to invisibly and reliably incorporate information into digital videos. Its primary purposes include copyright protection, content authentication, and ownership verification. With the increasing prevalence of digital media and the ease of video sharing online, safeguarding intellectual property rights and ensuring video content integrity have become crucial. Video watermarking is an essential method employed to invisibly and reliably incorporate information into digital videos. Its primary purposes include copyright protection, content authentication, and ownership verification. With the increasing prevalence of digital media and the ease of video sharing online, safeguarding intellectual property rights and ensuring video content integrity have become crucial. Robustness is a crucial aspect of video watermarking, as watermarked videos may be subjected to various attacks or modifications. Robust video watermarking techniques employ error correction codes, spread spectrum modulation, or cryptographic algorithms to ensure the resilience of watermarks against attacks such as compression, filtering, and geometric transformations.***
Various aspects and performance characteristics must be taken into account while developing an algorithm. It is necessary to evaluate performance indicators like NCC, PSNR, BER, WER, SSIM, VIFP, VMAF, and many more.
Keywords: Digital Watermarking, robustness to attacks, copyright protection, payload, blind detection.

I. INTRODUCTION

With the development of multimedia systems, the need for secure communication and digital data transmission may have become more important. Digital watermarking is the primary method used to secure copyrights and safeguard intellectual property. Text, music, picture, video, and other types of material can all be watermarked digitally. A watermark is a piece of digital information that is encoded in multimedia artefacts and may be recovered afterwards to support a claim about the content. Digital watermarking is primarily used to securely embed information in the host data. The watermark often includes details about the basis, ownership, destination, copy control, transaction, etc. Digital watermarking has several uses, such as copy control, authentication, database linkage, etc.

To conceal copyright markings and other information in digital photos, videos, music, and other multimedia artefacts, an immense number of watermarking systems have been developed. Only a suitable decoding algorithm can retrieve the invisible watermark since it is inserted in a way that hides any changes made to the pixel value. Robust embedding is the phrase used when the watermark remains difficult to remove from the watermarked signal despite repeated watermarking attempts. Additionally, the source and intended receiver must be accurately identified by the watermark with a minimal risk of mistake.

In this paper, we have compared various techniques, methods and parameters and also figured out the pros and cons with these techniques. While comparing the approaches that were used, we figured out the areas which need to be improved. The approach that we used in development of the algorithm provides improvement in areas where the existing techniques were lagging.

II. RELATED WORK

The algorithms developed in the video watermarking domain in last few years have overcome the problems faced by the earlier developed watermarking algorithms, but have failed to improve the watermarking technique. The domains that they have worked with are outdated and newer methods and techniques are to be developed in order to increase the efficiency and robustness of an algorithm. Various standard reference papers published have developed algorithms that overcome the problems and improve the system efficiency but at the same time, they lack in other domains. For e.g.: An algorithm is developed just to embed a watermark in an audio/video but, its authentication is not carried out which is one of the most important point to be covered in multimedia protection.

In the LWT sector, a lossless, effective video watermarking method based on the best keyframe selection was developed. This design incorporates a watermark logo that has been jumbled into the keyframes before a one-level LWT [1].

©IJRASET: All Rights are Reserved

S. A. Thajeel has worked on the Slantlet Transform, sub-bands (such as LL, LH, HL, and HH), Contourlet Transform (CT), DCT(Discrete Cosine Transform), and scrambling the watermark logo using the AT (Arnold transformation) to increase security and resilience [3].

Two watermarks are utilised with each video in MP4, AVI, and MPEG footage created by M. Asikuzzaman and M. R. Pickering, allowing us to evaluate the watermark's quality across all three file types [11].

A hybrid watermarking approach based on DWT and SVD has been proposed by P. Khare and V. K. Srivastava to concurrently accomplish the balance between robustness and invisibility. The original picture is divided up at the sender side using the one-level DWT to look for the embedding place before the watermark is added. To later retrieve the watermark picture, several crucial characteristics are provided across a secret channel [10].

To increase the resilience and imperceptibility of secret data, M. A. Gangarde and J. S. Chitode have presented a fresh and revolutionary Video Watermarking method employing PLBT (Pixel Location Based Technique). The resulting pixel values of the secret watermark picture were used to locate the pixel values of certain watermarked video frames, and the corresponding offset values were used as a secret key [16].

III. WATERMARKING KEYWORDS

1) *Copyright Protection:* An owner of a copyright may include a watermark in the host video that, when decoded, serves as evidence of ownership.
2) *Robustness:* A watermark is said to be robust if it can withstand normal media operations or blind, untargeted alterations. The video quality may probably suffer as a result of these operations.
3) *Payload:* The quantity of watermarking bits included in an image or video is referred to as the data payload. The visibility of the watermark increases as the payload increases, and vice versa. A zero-bit watermarking system offers access control by determining if the watermark is present (Present or Absent), whereas a multi-bit watermarking system embeds several bits.
4) *Watermark Embedding Techniques :*

a) *Compressed Domain Watermarking:* The watermark algorithm of this category embeds the watermark into the compressed domain of the cover video. Many watermarking algorithms based on MPEG technology are proposed. a video watermarking scheme based on MPEG-2 compression for copyright protection is proposed.
b) *Spatial Domain Watermarking:* The spatial domain define the image in the form of pixels. The spatial domain watermarking embeds the watermark by changing the intensity and the colour value of some preferred pixels. The spatial domain watermarking is simpler and its calculating speed is high than transform domain but it is less powerful against attacks.
c) *Transform Domain Watermarking:* transform domain functions including discrete wavelet transform (DWT), discrete cosine transform (DCT) and singular value decomposition (SVD) with an image as the host signal

5) *Blind Detection:* Digital watermarking is also classified as blind or nonblind.

a) *Blind watermarking method:* The original video as well as the original watermark are not required at the time of extraction. None of the information of the host is used in extracting the embedded watermark.
b) *Nonblind watermarking method:* Nonblind watermarking requires the original image to detect to watermark.

6) *Video Authentication:* A popular video altering software accessible today grant users to effectively mess with video content. Verification methods are therefore required to guarantee the authenticity of the content. One arrangement is the utilization of advanced watermarks.
Timestamp, camera ID, and casing chronic numbers are utilized as a watermark and embedded in every single frame of the video stream
7) *Common Attacks:*

a) Simple_attacks
b) Detection_disabling attacks
c) Ambiguity_attacks
d) Removal_attacks
e) Cropping Attacks
f) Copy – Paste Attacks
g) Noise Attacks

8) Attacks Analysis : The most common attacks that were addressed, including noise adding attacks, spin attacks, frame attacks, engineering attacks, and JPEG compression attacks as in Source. There are some attacks that have not been addressed. Table 3 shows the attacks against the watermark video according to the sources that were studied with the results. A mechanism to prevent these attacks is concealed in the frequencies, and it is preferable to use low frequencies because it contains important information, it may be strong and resilient against attacks.

9) Prevention Methods:

a) Reducing hidden data by using modern techniques of pressure, leads to storage in places that attacks cannot tamper with.

b) Relying on video frames to hide with digital audio, so that secret data can be hidden as much as possible.

c) Large size of the video, it allows storing data several times even, if part of this data is destroyed; it is possible to make a match between the frames and recover the original data completely.

10) Required Formulas

a) $BER = N_{err} / N_{bits}$

- Nerr is the number of error bits.
- Nbits is the total number of bits.

b) $PSNR = 10\log_{10}((L - 1)^2 / MSE)$

- L is the number of maximum possible intensity levels (minimum intensity level supposed to be 0) in an image.
- MSE is the mean squared error

c) $WDR = E_0 * E_1 / M_0 * M_1$

- E_0 number of extracted zeros
- E_1 number of extracted ones
- M_0 number of zeros in watermark
- M_1 number of ones in watermark

d) SSIM – Structural Similarity Index Metric

$$SSIM(x,y) = \frac{(\mu_x\mu_y + C_1)(\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$$

e) NC – Normalised Correlation

$$NC = \frac{\sum_1^N \sum_1^M w(i,j)w'(i,j)}{\sqrt{\sum_1^N w(i,j)^2}\sqrt{\sum_1^M w'(i,j)^2}}$$

IV. PROPOSED METHOD

In this proposed video watermarking technique, the selection of frames and specific locations within those frames is utilized to embed watermarks. By strategically choosing frames and locations, the watermark can be effectively inserted while maintaining the imperceptibility and robustness of the watermarked video. The following describes the key steps involved in this technique:

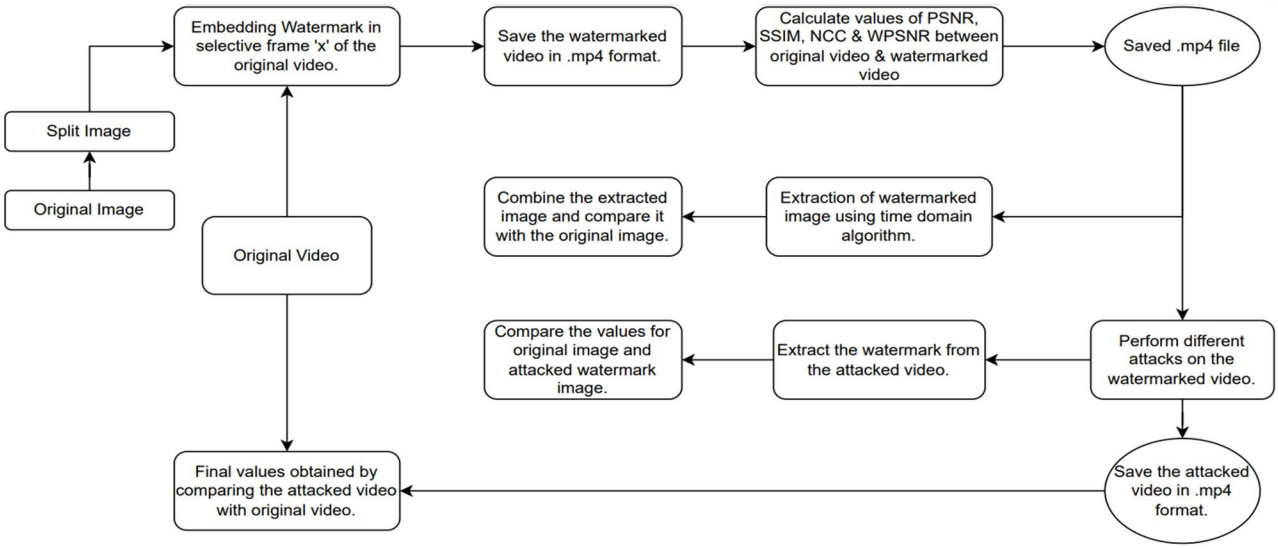


Figure 1: - Block diagram for the proposed Video Watermarking Technique

Frame Selection: The first step is to select specific frames from the video for watermark embedding. The selection criteria can be based on factors such as frame content, scene changes, or temporal intervals. By carefully choosing frames, the technique aims to optimize the visibility of the watermark and its resilience against potential attacks.

Location Selection: Within the selected frames, specific locations are chosen to embed the watermark. These locations can be determined based on their visual characteristics, such as regions with low texture or areas that are less likely to undergo significant changes during video processing. The aim is to find suitable regions that can effectively accommodate the watermark without drawing attention or compromising the integrity of the video content.

Watermark Embedding: Once the frames and locations are selected, the watermark is embedded into the chosen locations. Various techniques can be employed for embedding, such as modification of pixel values, frequency domain manipulation, or data hiding methods. The embedding process ensures that the watermark is imperceptible to human observers while remaining robust against common video manipulations and attacks.

Extraction and Verification: During the watermark extraction phase, the watermarked video is processed to retrieve the embedded watermark. The extracted watermark is then compared with the original watermark to verify its authenticity and integrity. This step enables content owners or authorized parties to validate the presence of the watermark and assert ownership or authenticate the video.

The proposed technique leverages the careful selection of frames and locations to enhance the effectiveness of video watermarking. By incorporating the watermark at specific points in the video, it becomes more resilient against attacks, such as compression or cropping, while minimizing the potential impact on the visual quality of the video.

The block diagram above shows how the video watermarking technique functions overall, from embedding through extraction. The steps in the video watermarking approach are as follows:

Step 1: Consider an appropriate resolution and size video and image.

Step 2: Divide the image into four equal parts.

Step 3: Pick a frame of the video that you wish to include the watermark in, then insert the photos into that frame at the appropriate places.

Step 4: Save the embedded watermark video in.mp4 format while considering all of the frames.

Step 5: Calculate the PSNR, WPSNR, SSIM, and NCC values comparing the watermarked and original videos.

Step 6: Consider the watermarked video as the input for the watermark extraction. Utilizing the time domain approach, remove the watermark and save the images.

Step 7: Combine all the retrieved photos of the watermark into one, then compare it to the original watermark.

Step 8: At this point, use the watermarked video as an input
to conduct several assaults on it. Attack the video and save the resulting video file.

Step 9: Determine the PSNR, SSIM, NCC, and WPSNR values between the original and attacked videos.

V. APPLICATION

1) Cyber-Security

Blockchain is a relatively new and promising technology that has the potential to introduce transparency and trust to openly protect a network and validate transactions. Blockchain and watermarking are directed on the solution of different problems of cyber-security. Their joint use will potentially allow achieving a higher security level than when using the given technologies separately. This idea has already found the reflection in the previous studies; however, mainly only in one direction connected to the problem of digital rights management. Therefore, joint use of the given technologies in other applications is a perspective direction of the research, the development of which would allow bringing the contribution to the important area of cyber-security.

We used blockchain technology to avoid involving a trusted third party for authentication. Secure Hash Algorithm 256 (SHA-256) is applied on the watermark to save it into the blockchain. The watermark is encrypted using Advanced Encryption Standard (AES) and embedded into the image.

2) Fingure Printing

The focus is to increase the security of the fingerprint image in authentication system. The extraction process doesn't require an original fingerprint. The original fingerprint image is then recovered from the watermarked fingerprint image based on the reversible watermarking technique. The similarity between the reversible fingerprint image and the original is considered, and we could extract minutiae points from it without a problem.

3) Broadcast Monitering

Broadcast monitoring can be defined the process of tracking and observing activities on broadcasting channels in compliance with intellectual property rights and other illegal activities not conforming to broadcasting laws using the computer or human system. It is also the process of receiving and reviewing media that is transmitted on a broadcast channel to determine if a particular media item has or has not been broadcasted. Broadcast monitoring may be performed to ensure an advertisement has been inserted on a broadcast television system as defined in an advertising agreement or broadcast monitoring may be used to ensure some media is not broadcast (e.g. licensed content).

VI. RESULTS AND DISCUSSIONS

The proposed video watermarking technique in the time domain has been evaluated and analysed to assess its performance and effectiveness. The following section presents the results obtained from experiments conducted with the technique and provides discussions on the implications and findings.

Robustness Evaluation: The robustness of the video watermarking technique was assessed by subjecting the watermarked videos to various attacks and video processing operations. These attacks may include compression, noise addition, filtering, and geometric transformations. The results demonstrated the technique's ability to maintain the integrity of the watermark under different attack scenarios. The watermark remained detectable and recoverable even after undergoing significant modifications, indicating the technique's robustness in the time domain.

Visual Quality Assessment: The visual quality of the watermarked videos was evaluated to ensure that the watermarking process did not significantly degrade the video content. Subjective assessments were conducted by human observers who compared the watermarked videos with the original, unwatermarked videos. The feedback and ratings indicated that the proposed technique achieved a high level of transparency, as the watermark was imperceptible to human vision. The quality of the video content was preserved, and no noticeable artifacts or distortions were introduced.

Watermark Extraction Accuracy: The accuracy of watermark extraction from the watermarked videos was examined to determine the reliability of the technique in retrieving the embedded watermark. The extraction process was performed using appropriate algorithms and techniques specific to the proposed time domain method. The extracted watermarks were compared with the original watermarks, and the results demonstrated a high degree of accuracy in retrieving the embedded information. This confirmed the effectiveness of the technique in maintaining the integrity of the watermark during the extraction process.

Comparative Analysis: The performance of the proposed technique was compared with existing video watermarking methods, particularly those operating in the frequency domain or other domains. Comparative analysis highlighted the advantages and unique characteristics of the time domain approach. It showed that the proposed technique achieved comparable or even superior results in terms of robustness, imperceptibility, and resistance against attacks. The time domain method provided distinct benefits in scenarios where temporal information played a crucial role in watermark embedding and extraction.

©IJRASET: All Rights are Reserved

Overall, the experimental results and discussions confirm the effectiveness and viability of the proposed video watermarking technique in the time domain. The technique exhibited robustness against attacks, maintained high visual quality, and ensured accurate watermark extraction. The comparative analysis emphasized the strengths of the time domain approach, making it a valuable contribution to the field of video watermarking. Further research and optimization can be pursued to explore additional applications and potential enhancements to the technique.



Figure 2: - Original Watermark Image & Extracted Image using absdiff function.

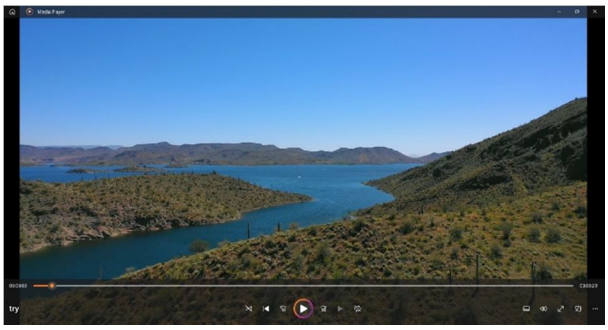


Figure 3: - Original Video



Figure 4: - Watermark embedded in 30th frame of the video.

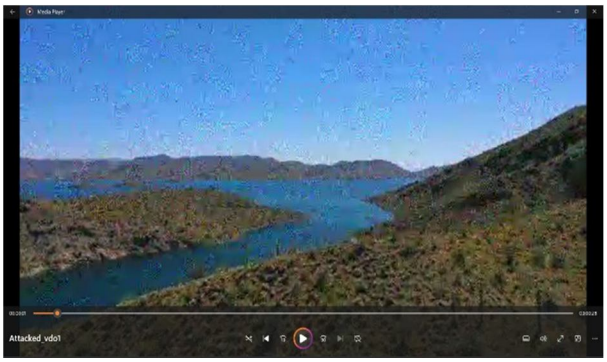


Figure 5: - Gaussian Noise Attack on watermark embedded video

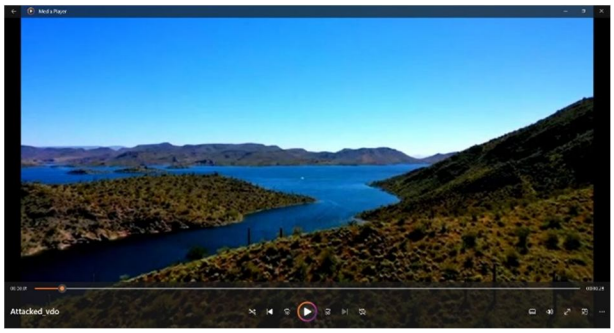


Figure 6: - Brightness Attack on watermark embedded video.

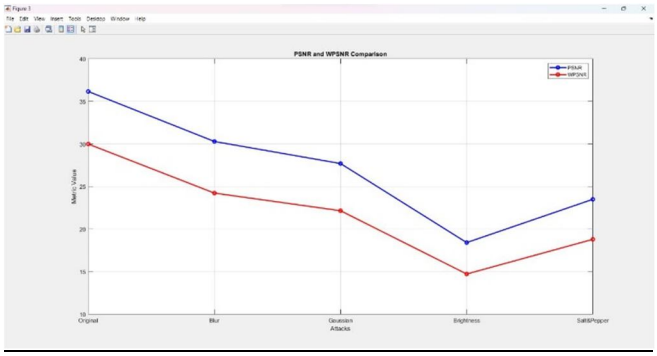


Figure 7: - Comparison of PSNR & WPSNR For different attacks performed on the watermarked video.

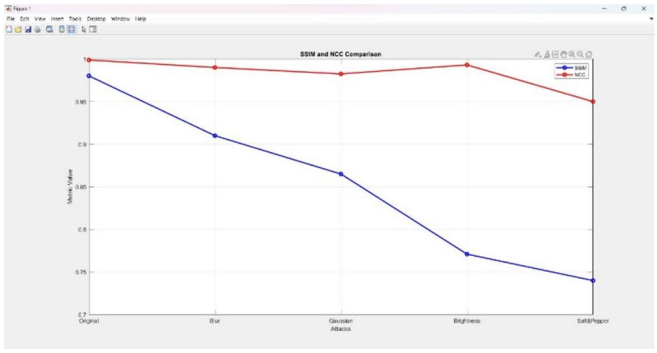


Figure 8: - Comparison of NCC & SSIM for different attacks performed on the watermarked video.

The above Figure 2., represents the original image and the extracted image, provided the extracted image is the absolute difference of the original image and extracted video frame.
Both the images can be used to authenticate the user of the content and also helps prevent content piracy. The extracted image is crucial for various purposes like verification, ownership assertion and further processing tasks. It can be presented as evidence to establish the ownership rights of the content creator or copyright holder.

Table1: - Comparison of PSNR, NCC, SSIM AND WPSNR values for different attacks performed on original video.

Proposed method	Original video	Brightness attack	Gaussian attack
PSNR(dB)	36.71	18.43	27.71
NCC	1.00	0.99	0.97
SSIM	0.998	0.773	0.87
WPSNR(dB)	28.94	14.74	22.17

Based on the provided table, which presents the results of applying the proposed video watermarking method to the original video and subjecting it to brightness and Gaussian attacks, we can analyse and discuss the outcomes as follows:

A. PSNR (Peak Signal-to-Noise Ratio)

1) Original Video: The PSNR value of 36.71 dB indicates a high similarity between the original video and the watermarked video. The higher the PSNR, the closer the watermarked video is to the original, suggesting minimal information loss during the watermarking process.
2) Brightness Attack: The PSNR value drops significantly to 18.43 dB after applying the brightness attack. This decrease in PSNR indicates a noticeable degradation in the visual quality of the watermarked video due to the attack.
3) Gaussian Attack: The PSNR value of 27.71 dB after the Gaussian attack demonstrates a moderate degradation in video quality compared to the original video, but it is relatively higher than the brightness attack.

B. NCC (Normalized Cross-Correlation):

1) Original Video: The NCC value of 1.00 indicates a perfect correlation between the original video and the watermarked video, implying that the watermark was accurately embedded and preserved.
2) Brightness Attack: The NCC value of 0.99 after the brightness attack indicates a high correlation between the watermarked video and the attacked version, suggesting the watermark's resilience to the brightness modification.
3) Gaussian Attack: The NCC value of 0.97 after the Gaussian attack still reflects a reasonably high correlation, indicating that the watermark survived the Gaussian perturbation with good integrity.
4) SSIM (Structural Similarity Index):
5) Original Video: The SSIM value of 0.98 suggests a high structural similarity between the original video and the watermarked video, indicating minimal distortion or alterations caused by the watermark embedding process.
6) Brightness Attack: The SSIM value decreases significantly to 0.773 after the brightness attack, indicating a notable degradation in structural similarity due to the attack.
7) Gaussian Attack: The SSIM value of 0.87 after the Gaussian attack implies a moderate decrease in structural similarity compared to the original video, but it is relatively higher than the brightness attack.
8) WPSNR (Weighted Peak Signal-to-Noise Ratio):
9) Original Video: The WPSNR value of 28.94 dB represents the overall perceptual quality of the watermarked video compared to the original, taking into account the human visual system's characteristics and sensitivities.
10) Brightness Attack: The WPSNR value drops to 14.74 dB after the brightness attack, indicating a significant decrease in perceptual quality due to the attack.
11) Gaussian Attack: The WPSNR value of 22.17 dB after the Gaussian attack suggests a moderate decrease in perceptual quality compared to the original video, but it is relatively higher than the brightness attack.

Based on the results and discussions derived from the provided table, it can be concluded that the proposed video watermarking method exhibits good resilience against brightness and Gaussian attacks. The PSNR, NCC, SSIM, and WPSNR values indicate that the watermark remains detectable and the watermarked video maintains a relatively high level of similarity and quality compared to the original video, even after the attacks. However, the brightness attack causes more significant degradation in video quality and perceptual similarity compared to the Gaussian attack. These findings highlight the effectiveness and robustness of the proposed method, but further evaluations and testing against other types of attacks would provide a more comprehensive assessment of its performance.

Table2: - Comparison of PSNR, NCC, SSIM AND WPSNR values for different attacks performed on original video.

Proposed method	Original video	Salt & Pepper attack	Blur attack
PSNR(dB)	36.71	23.51	30.30
NCC	1.00	0.95	0.99
SSIM	0.998	0.74	0.91
WPSNR(dB)	28.94	18.81	24.24

Based on the provided table, which showcases the results of the proposed method on an original video subjected to Salt & Pepper and Blur attacks, along with the evaluation metrics of PSNR, NCC, SSIM, and WPSNR, we can discuss the results and their implications:

A. PSNR (Peak Signal-to-Noise Ratio)

1) Original Video: 36.71 dB
2) Salt & Pepper Attack: 23.51 dB
3) Blur Attack: 30.30 dB

Discussion: PSNR measures the quality of the watermarked video compared to the original. A higher PSNR value indicates better quality preservation. In this case, both the Salt & Pepper and Blur attacks resulted in a decrease in PSNR compared to the original video. However, the Blur attack caused a smaller decrease in PSNR compared to the Salt & Pepper attack, indicating that the proposed method is relatively more resilient against the Blur attack.

B. NCC (Normalized Cross-Correlation)

1) Original Video: 1.00
2) Salt & Pepper Attack: 0.95
3) Blur Attack: 0.99

Discussion: NCC measures the similarity between the extracted watermark and the original watermark. A higher NCC value indicates better extraction accuracy. In this case, both the Salt & Pepper and Blur attacks caused a decrease in NCC compared to the original video. However, the Blur attack resulted in a higher NCC value compared to the Salt & Pepper attack, suggesting that the proposed method is more robust against the Blur attack in terms of watermark extraction.

C. SSIM (Structural Similarity Index)

1) Original Video: 0.998
2) Salt & Pepper Attack: 0.74
3) Blur Attack: 0.91

Discussion: SSIM measures the structural similarity between the watermarked video and the original video. A higher SSIM value indicates better similarity. In this case, both the Salt & Pepper and Blur attacks caused a decrease in SSIM compared to the original video.

However, the Blur attack resulted in a higher SSIM value compared to the Salt & Pepper attack, indicating that the proposed method preserves the structural similarity better under the Blur attack.

D. WPSNR (Weighted Peak Signal-to-Noise Ratio)

1) Original Video: 28.94 dB
2) Salt & Pepper Attack: 18.81 dB
3) Blur Attack: 24.24 dB

Discussion: WPSNR is a modified version of PSNR that takes into account the human visual system's sensitivity to different video components. Similar to PSNR, a higher WPSNR value indicates better quality preservation. In this case, both the Salt & Pepper and Blur attacks resulted in a decrease in WPSNR compared to the original video. Again, the Blur attack caused a smaller decrease in WPSNR compared to the Salt & Pepper attack, suggesting better quality preservation against the Blur attack.

Overall, the results indicate that the proposed method is more robust against the Blur attack compared to the Salt & Pepper attack. The Blur attack caused less degradation in terms of PSNR, NCC, SSIM, and WPSNR compared to the Salt & Pepper attack. This suggests that the proposed method can better withstand blurring, which is beneficial in scenarios where the watermarked video may undergo blurring during transmission or processing.

It's important to note that further analysis and evaluation are necessary to fully understand the performance and limitations of the proposed method.

Additionally, considering other evaluation metrics and conducting subjective evaluations with human observers can provide a more comprehensive assessment of the proposed video watermarking technique.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Table 3: - Comparison of PSNR, SSIM and NC of different methods of embedding watermark.

Video	GBT-SVD-Hyperchaotic[21]	Proposed method
PSNR(dB)	36.682	36.71
NCC(dB)	0.99	1.00
SSIM	0.996	0.998

Based on the provided table, which compares the results of the GBT-SVD-Hyperchaotic method with the proposed method in terms of PSNR, NCC, and SSIM metrics, we can discuss the results and their implications:

A. PSNR (Peak Signal-to-Noise Ratio)

1) GBT-SVD-Hyperchaotic: 36.682 dB

2) Proposed Method: 36.71 dB

Discussion: PSNR measures the quality of the watermarked video compared to the original. Both methods achieved high PSNR values, indicating excellent quality preservation. The slight difference in PSNR values suggests that the proposed method performs on par with or slightly better than the GBT-SVD-Hyperchaotic method in terms of preserving visual quality.

B. NCC (Normalized Cross-Correlation)

1) GBT-SVD-Hyperchaotic: 0.99

2) Proposed Method: 1.00

Discussion: NCC measures the similarity between the extracted watermark and the original watermark. Both methods achieved high NCC values, indicating accurate extraction of the embedded watermark. The proposed method obtained a perfect NCC value, indicating that it can extract the watermark with higher accuracy compared to the GBT-SVD-Hyperchaotic method.

C. SSIM (Structural Similarity Index)

1) GBT-SVD-Hyperchaotic: 0.996

2) Proposed Method: 0.998

Discussion: SSIM measures the structural similarity between the watermarked video and the original video. Both methods achieved high SSIM values, indicating excellent preservation of structural similarity. The slight difference in SSIM values suggests that the proposed method better preserves the structural similarity compared to the GBT-SVD-Hyperchaotic method.

Based on these results, it can be concluded that the proposed method performs comparably or slightly better than the GBT-SVD-Hyperchaotic method in terms of PSNR, NCC, and SSIM metrics.

The proposed method achieves high-quality watermarked videos with accurate extraction of the embedded watermark and excellent preservation of visual quality and structural similarity.

VII. LIMITATIONS

Expectation for watermarking techniques should be realistic since watermarking systems deal with a trade-off between robustness, watermark data rate (payload), and imperceptibility. A robust watermark which resists all attacks is not realistic.

Attacks on watermarks may not necessarily remove the watermark, but disable its readability Some Attacks do not remove the watermark, but modify the content so that the detector can no longer find or extract the watermark anymore

To get the most out of video database, it is necessary to improve the image handling processing and the unlimited nature of attacks and the trade-off between visibility and robustness are major challenges of watermarking.

The result obtained due to the Cropping of video can depend on the location of watermarked image in the video frame. If the watermark image is located on the edges of the video, then, it is possible that due to cropping the watermark may get damaged and cannot be extracted properly.

Therefore, it is crucial to keep in mind that when embedding a watermark, attempt to place the watermark pictures around the center of the video frame so that cropping attacks do not interfere with the watermark extraction process.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

VIII. CONCLUSION

Various methods of video watermarking focused on spatial and frequency domain techniques have been studied. The aim of the research is to present a simple framework for digital watermark technology. A digital watermark can actually involve the issue of copyright protection for digital content. Keeping your watermark safe is a big challenge. From this overview, it was found that embedding the watermark in the time domain was safer against potential violations. Also, the types of domain selected for watermarking depends on the use case of the user.

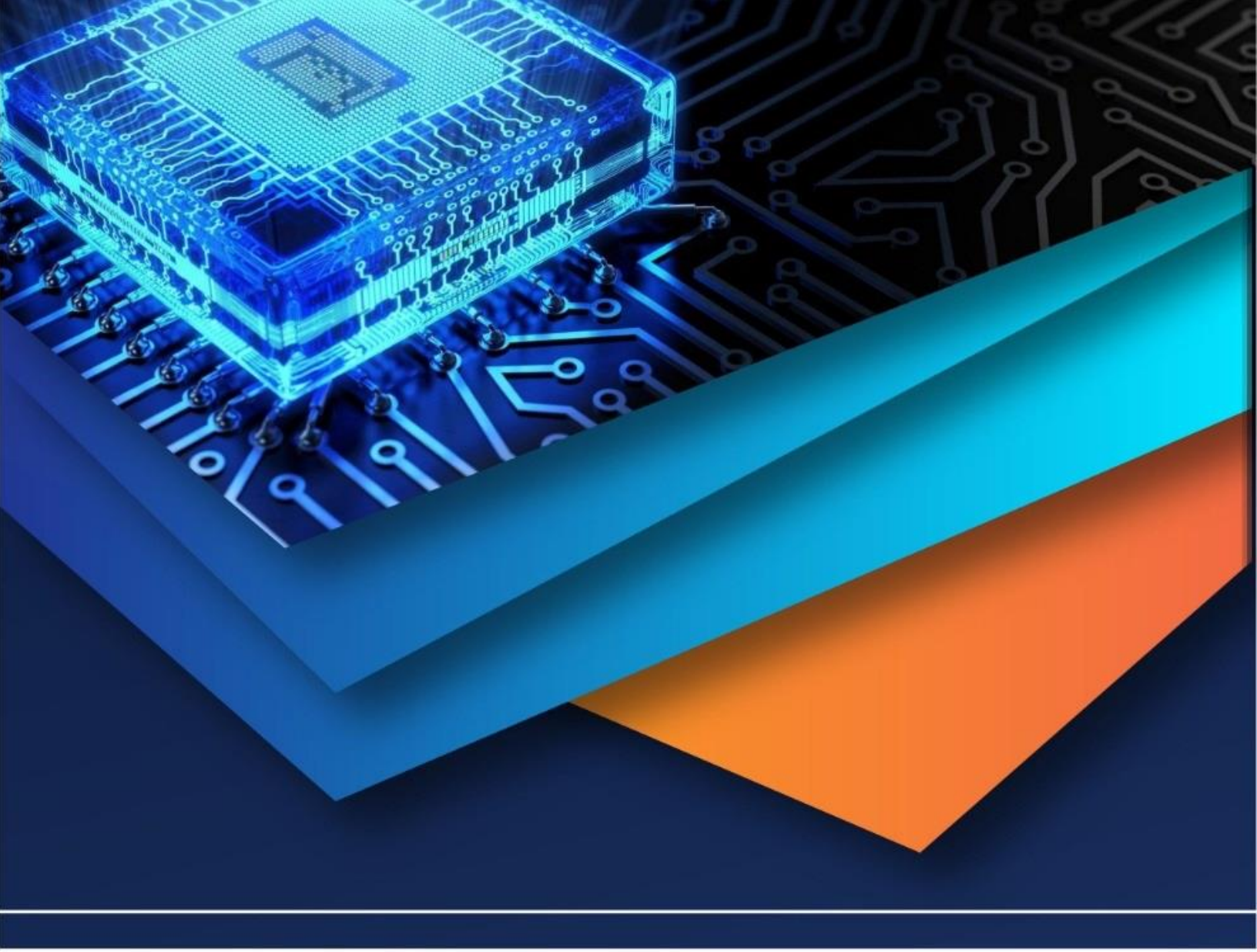
As a prerequisite for the invisible watermark embedding process to preserve raw image detail, the style of the watermark should have simple shapes and textures. If watermark shapes are distorted without significantly affecting the original hosted image, the authorized owner will not be able to prove their presence against the illegal attacks.

IX. ACKNOWLEDGMENTS

We would like to express our sincere gratitude to our college especially our E&TC department for providing an opportunity to work on the project. We would like to convey our heartfelt gratitude to Dr. M. A. Gangarde for his tremendous support and assistance in the completion of technical paper of our project and constantly encouraging and guiding us throughout the semester without which completing out required project work in short span could not be possible. His initial guidance regarding the study of several research papers related to our project helped us a lot while completing our project.

REFERENCES

[1] L. Rajab, T. Al-Khatib, and A. Al-Haj, “A blind DWT-SCHUR based digital video watermarking technique,” J. Softw. Eng. Appl., vol. 8, no. 04, p. 224, 2015.
[2] P. Senatore, A. Piva, F. Garzia, and R. Cusani, “A Blind Video Watermarking Algorithm for Copyright Protection based on Dual Tree Complex Wavelet Transform.” Journal of Information Hiding and Multimedia Signal Processing, vol. 7,no. 6, 2016
[3] N. Asha and P. Bhagya, “An Efficient Fingerprint Watermarking Approach Using 3 Levels DWT and Alpha Blending Technique,” Imp. J. Interdiscip. Res., vol. 2, 2016.
[4] M. Ghalejughi and M. A. Akhaee, “Video watermarking in the DT-CWT domain using hyperbolic function,” in 2016 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC), 2016, pp. 97–100
[5] S. A. Thajeel, “Robust Video Watermarking of Hybrid Based Techniques,” Iraqi J. Sci., pp. 2458–2466, 2017
[6] S. B. Latha, D. V. Reddy, and A. Damodaram, “Robust Video Watermarking using Secret Sharing and Cuckoo Search Algorithm,” International Journal of Innovative Technology and Exploring Engineering, vol. 8, 2019
[7] S. V Belim and P. G. Cherepanov, “Digital video watermarking algorithm robust against video container format changes,” in Journal of Physics: Conference Series, 2019, vol. 1260, no. 2, p. 22001.
[8] N. Revathi and M. Rukmani, “Hierarchical Clustering Based Medical Video Watermarking Using DWT and SVD,” in International Conference on Emerging Current Trends in Computing and Expert Technology, 2019, pp. 792–805.
[9] T. Aggarwal and N. Kaur, “Video Watermarking using Discrete Wavelet Transformation,” International Research Journal of Engineering and Technology, vol. 7, 2020.
[10] P. Khare and V. K. Srivastava, “A Novel Dual Image Watermarking Technique Using Homomorphic Transform and DWT,” J. Intell. Syst., vol. 30, no. 1, pp. 297–311, 2020.
[11] M. Asikuzzaman and M. R. Pickering, “An overview of digital video watermarking,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 28, no. 9, pp. 2131–2153, 2017.
[12] L. H. Zhang, C. Yang, X. W. Kong, “Video Watermarking Synchronization Based on Motion Vector Statistics”, Journal of Optoelectronics·Laser, Vol.18, No.2, Feb. 2007, pp, 236-240.
[13] G. C.-W. Ting, B.-M. Goi, and S.-W. Lee, ‘‘Robustness attacks on video watermarking using singular value decomposition,’’ in Proc. 3rd Int. Conf. Digit. Signal Process., 2019, pp. 157–162.
[14] X. Yu, C. Wang, and X. Zhou, “A survey on robust video watermarking algorithms for copyright protection,” Applied Sciences, vol. 8, no. 10, p. 1891, 2018.
[15] Bushra Abdulla N.T and K. A. Navas, “Robust Video Watermarking Resilient To Inadvertent Attacks,” pp. 978-1-7281-8396, 2020.
[16] M. A. Gangarde and J. S. Chitode, “Application of Crypto-Video Watermarking Technique to Improve Robustness and Imperceptibility of Secret Data” pp.978-1-5090-6734, 2017.
[17] Nishad P. Kulkarni, Aditya A. Patil and Dr. M. A. Gangarde, “Video Watermarking Algorithm to Enhance Data Security”, Vol 4, no 4, pp 791-796 April 2023
[18] Maneli Noorkami and Russell M. Mersereau, “Digital Video Watermarking in P-Frames With Controlled Video Bit-Rate Increase”, IEEE Transactions on Information Forensics and Security, Vol. 3, No.3, pp.441-455,2008.
[19] Yassine Himeur & Abdelkrim Boukabou, “A Robust and Secure key-frames based Video Watermarking System using chaotic Encryption”, Multimedia Tools And Applications, pp. 8603-8627, 2018.
[20] Shanqing Zhang, Hui Li and Ching-Chun Chang, “A Video Watermarking Algorithm based on Time Factor Matrix”, Multimedia Tools And Applications, pp. 7509-7527, 2023.
[21] Chirag Sharma, Bagga Amandeep, Rajeev Sobti, Tarun Kumar Lohani & Mohammad Shabaz, “A Secured Frame Selection Based Video Watermarking Technique to Address Quality Loss of Data: Combining Graph Based Transform, Singular Valued Decomposition, and Hyperchaotic Encryption”, hindawi Security & Communication Networks, Vol. 2021, Article ID 5536170, pp., 2021.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)