A Novel Method of Invisible Video Watermarking Based on Index Mapping and Hybrid DWT-DCT

https://doi.org/10.3991/ijoe.v19i04.37581

Hussein Tuama Hazim[1(✉)], Nawar Alseelawi[2], Haider TH. Salim ALRikabi[2]
[1]Department of Electrical Engineering, College of Engineering, University of Misan, Maysan, Iraq
[2]Department of Electrical Engineering, College of Engineering, Wasit University, Wasit, Iraq
Hussein.tuama@uomisan.edu.iq

Abstract—Watermarking is widely used in multimedia preservation and communication, which comprises, and is therefore not limited to, data security and validation. Security, readability, imperceptibility, and resilience are some of the key advantages of this technology. However, there are still certain issues that need to be addressed, such as the ability to withstand a variety of assaults without substantially affecting the quality and value of embedded data. Based on its operational domain, the watermarking technology may be divided into two groups: spatial and frequency watermarking. An index mapping-based watermarking approach for copyright protection of multi-media color videos is presented in this paper. We offer a hybrid discrete wavelet transform and discrete cosine transform (DCT) watermarking algorithm for digital video watermarking of a color video watermark. Peak signal to noise ratio (PSNR), similarity structure index measure (SSIM), have been used to analyze the distortion produced by watermarking. It is suggested that the proposed video watermarking method provides greater imperceptibility in conjunction with each other with the human visual system and it offers higher robustness against different attacks.

Keywords—watermarking, information security, discrete cosine transform, discrete wavelet transform, video stream

1 Introduction

Video watermarking techniques have been in high demand in recent years as a result of digital computer technology's rapid expansion. This is because there are so many free videos available on the World Wide Web (WWW) that need to be copyright protected and ownership validated [1, 2]. A growing number of people are concerned about protecting their intellectual property rights and digital material. A digital watermarking technique is the greatest approach to safeguard multimedia goods from data theft by hiding information within the cover. The usage of digital watermark technology, which has grown more accessible, is predicated on the ability to conceal the watermark in a digital medium. The information about the owner of a copyright for this digital material is contained in the watermark. A trademark picture, a serial number, or any other digital information that describes the copyright might be used [3–5]. A watermark and a digital

interface can be combined for this digital interface to make it difficult to distinguish between them. The watermark is retrieved from the digital interface to establish their lawful owner whenever copyright validation is necessary. The watermark must be resistant to a variety of assaults, both deliberate and inadvertent [6–8]. A watermark must have specific characteristics to be effective, such as being undetectable and undeletable. Encoding is a component of every watermarking process. Watermark information is embedded in the image using an algorithm. to extract the watermark from the host cover and decoding algorithm [9–11]. The Information taken from the watermarked cover. The goal of this project is to create a hybrid discrete wavelet transform video watermarking technique based on discrete cosine transform It incorporates a strong ownership imprint into preserve copyright ownership, video frames are used. In digital watermarking, there is a complicated trade-off between three parameters: data payload, fidelity, and robustness. Figure 1 depicts it, and more information is provided below.

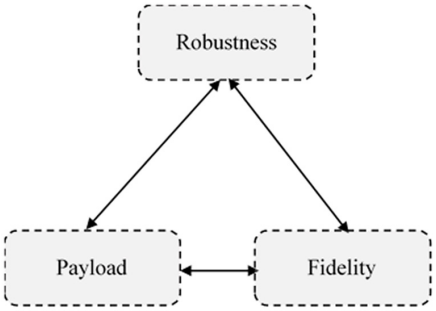

Fig. 1. Trade-off in digital watermarking

1.1 Payload

The number of bits that can be buried in digital data defines the data payload, which is inextricably linked to the number of alternative messages that may be inserted owing to the watermarking method. It should be noted that the size of the data payload is usually determined by the size of the host data. The greater the number of host samples accessible, the more bits that may be concealed. As a result, the capacity is frequently expressed in bits per sample.

1.2 Fidelity

Watermarking digital content is the process of embedding a watermark signal into the original content, which is certain to cause some distortion. One of the criteria in digital watermarking, as in lossy compression, is that the distortion be undetectable. In other words, a human observer should be unable to determine whether or not digital data has been watermarked. There should be no suspicious observable artefacts introduced throughout the watermarking procedure. The perceived resemblance between watermarked and unwatermarked data is also known as fidelity [12].

1.3 Robustness

The capacity of the detector to retrieve the concealed watermark from some changed watermarked data may be described as the resilience of a watermarking technique. The change might be malicious or non-malicious, for example, it can be caused by ordinary processing (filtering, lossy compression, noise addition) or by an attack aiming to erase the watermark. As a result, the watermark's resilience is measured by how long it survives assaults [13–15].

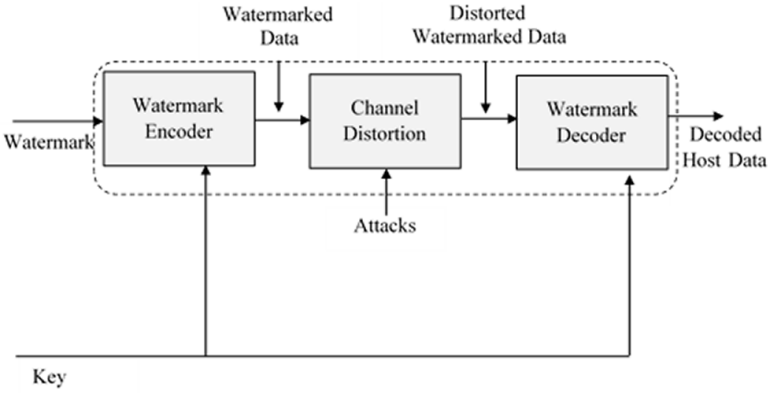

Fig. 2. Basic watermarking

Figure 2 shows the basic block diagram of watermarking. It has three phases. Phase One is an Embedding Phase. The embedding phase in which the watermark is embedded in the image is handled using an embedding algorithm with a secret key. After that a watermarked image is created. The image with the watermark is then transmitted over the network. The second stage is the distortion / attack phase. At this stage, where data is transferred over the network. Either a noise can be added with a watermarked image or some attack is made on a watermarked image. Therefore, our watermarked data is altered or destroyed. The third stage is the recovery / recovery phase. In the detection phase, a watermark is obtained or extracted by a dedicated detector from an image with a watermark using a specific detection algorithm and using a secret key.

2 Literature review

Watermarking techniques for video are categorized based on their application domain [16, 17]. Watermarks can be embedded in spatial domain using several approaches. This is improved by determining the pixel values for each video frame which has been received. These approaches are susceptible to common signal distortions and exploitation. Other methods, on the other hand, embed the watermark in the frequency domain, which will be more distortion-resistant.

2.1 Spatial domain

The watermark is included in the spatial domain watermarking techniques by directly changing the pixel values of the host image/video. The Least Significant Bit (LSB) approach is the most often utilized. The LSB of each pixel is utilized to insert the watermark or copyright information in this approach. This approach is the most straightforward, since it stores the watermark on the whole cover picture, allowing a smaller item to be inserted several times. A single surviving watermark might be regarded a success in the event of a data-destroying attack. They can withstand assaults like as cropping, noise, lossy compression, and so on. The key advantages of pixel-based techniques are that they are conceptually simple and have extremely low computing complexity, making them popular in video watermarking applications where real-time speed is a top need. They do, however, have several significant flaws. The requirement for exact spatial synchronization exposes users to de-synchronization assaults; failure to address the temporal axis exposes users to video processing and multiple frame collusion; and watermark improvement using just spatial analysis approaches is challenging.

2.2 Frequency domain

The watermark is inserted in frequency domain methods by changing the transform coefficients of the frames in the video stream. The Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform are the most widely utilized transformations (DWT) [18, 19]. The watermark is distributed throughout the whole domain of the original data. Transformation methods are used to translate the host image/video into the frequency domain. The watermark information is then stored using the modified domain coefficients [20–24]. Finally, the inverse transform is used to create the watermarked image/video. DWT has been used in several studies because of its multi-resolution capabilities, as well as the fact that it offers both spatial and frequency domain properties, making it compatible with the Human Visual System (HVS). Combining the DWT with additional algorithms to enhance robustness and invisibility is also a new trend. Recently, there has been a rapid increase in the usage of the internet and the World Wide Web, as well as multimedia technology and its applications. The dissemination of digital content through the internet has been made easier as a result of this. Retransmission, replication, and publication of digital multimedia works (video, music, and pictures) became possible through the Internet. Without the owner's permission, a huge volume of digital material is replicated and spread. As a result, there is a pressing need for safeguards against unlawful copying and dissemination. As a result, some safe mechanisms for lawful dissemination of these digital items have to be developed.

Various techniques for increasing robustness and imperceptibility have been presented in the literature. Sanjana Sinha et al. [25] introduced a complete technique for watermarking digital video in 2011 by combining the Discrete Wavelet Transform (DWT) and Principal Component Analysis into a hybrid digital video watermarking scheme (PCA). PCA helps disperse the watermark bits into uncorrelated coefficients by decreasing correlation among the wavelet coefficients generated from wavelet decomposition of each video frame. The binary watermark is inserted in the major components of the low frequency wavelet coefficients after the video frames are decomposed using DWT.

Filtering, contrast modification, noise addition, and geometric assaults are all possible attacks on the watermarked video, but the undetectable high bit rate watermark inserted is resistant to all of them. Manish Choubisa et al. [26] presented a DCT (Discrete Cosine Transformation) based digital watermarking approach that permuted the picture. Watermarks can be made invisible by changing the image's block DCT coefficient. The pictures are permuted before being converted into blocks, allowing for a resolution of 8 x 8 pixels, and the watermark images are then inserted by changing their DCT coefficient. The proposed system demonstrated that the procedure is extremely reliable. Poulami Ghosh et al. [27] presented a new watermarking approach in 2012 that included both visible and invisible watermarks in a video. Because digital data may be easily duplicated without deterioration in quality, data protection is required. Digital watermarking is a technique for embedding extra information into the host signal to assure multimedia data security and protection. Because both watermarks are present in the video frames, it is more resistant to assaults. The watermarking technique presented here deals with watermark embedding and extraction. The invisible watermark is embedded using the Discrete Wavelet Transform (DWT), and the Peak Signal to Noise Ratio (PSNR) is computed to determine the method's effectiveness. We use both visible and invisible watermarks in this approach to provide an extra layer of copyright protection. Because we're utilizing compound mapping to incorporate the visible watermark, the video's resilience is improved. The suggested technique works well on grayscale and uncompressed.avi video, and it might be applied to colorful videos in the future. Nisreen I Yassin et al. [28] proposed a complete method for digital video watermarking that involves embedding a binary watermark picture into the video frames. The Principal Component Analysis (PCA) transformation is done to each block in the two bands LL and HH after each video frame is split into sub-images using a two-level discrete wavelet transform. The watermark is incorporated in the PCA block of the two bands' maximal coefficient. A variety of video sequences are used to test the suggested system. The findings of the experiments reveal a high level of imperceptibility, with no discernible difference between the watermarked video frames and the original frames. JPEG coding, Gaussian noise addition, histogram equalization, gamma correction, and contrast adjustment are all assaults that the proposed system is resistant against. Nikita Kashyap et al. [29] used a 3-level discrete wavelet transform to create a robust picture watermarking approach for copyright protection (DWT). Using the alpha blending technique, a multi-bit watermark is inserted into the low frequency sub-band of a cover picture. It is discovered that inserting and extracting the watermark in the grayscale cover picture is easier than using other transform approaches. Statistical metrics such as peak signal-to-noise-ratio (PSNR) and mean square error are used to compare the proposed technique to the 1-level and 2-level DWT-based picture watermarking methods (MSE). The experimental findings show that the watermarks created with the proposed technique are undetectable, and that the quality of the watermarked and recovered images is enhanced.

3 Proposed methodology

The Methodology comprises two parts, one is watermark embedding part and second is watermark extraction part. The detailed procedure of watermark embedding and extraction is given below.

3.1 Watermark embedding

A watermark is a binary picture with either 1 or –1 pixel intensities that was mixed with a pseudorandom sequence with the same 1 or –1 value. Figure 3 depicts a block schematic of the embedding process. The suggested watermark embedding technique is shown in pseudocode in Listing 1. A one-level two-dimensional DWT is used to transform the Y component of a video sequence, and also the middle sub-bands (LH and HL) are then picked (as shown in Listing 1). These selected sub-bands (in alternating frame) were then transformed and reordered utilizing zigzag scan employing two-dimensional DCT. A watermark was then placed on the central frequency coefficient (25 percentages). (See line 11) Line 12 is a watermark image equation. The watermark strength was set by the magnitude factor (α). Finally, DCT and DWT were reversed, as indicated in Lines 13–14.

Algorithm 1: Watermark Embedding Pseudo code
Input: Cover Video, Watermark video
Output: Watermarked Video
1: Initialize: Watermark video, Cover Video, key, pseudo random, alpha, 2: Frames from = 1: Frame length (Cover Video) 3: 2D-DWT(video) → LL(Low Low), LH (Low High), HL(High Low), HH(High High) 4: From cover video (if frame is even frame Then) 5: 2D-DCT(HL) → x 6: Else If from cover video (if frame is odd frame Then) 7: 2D-DCT(LH) → x 8: End If 9: ZIGZAG scan of (x) → x* 10: Length of x* = L 11: Select middle frequency x* ((L*0.375)+1:(L*0.625)) → C 12: C + (α * pseudo random *Watermark Video) = CC 13: Apply inverse 2D-DCT 14: Apply inverse 2D-DWT 15: End For 16: Output watermarked video 17: calculate Quality parameter MSE, PSNR

It shows the detailed watermark embedding block diagram. Algorithm 1 shows the watermark embedding procedure [30]

3.2 Watermark extraction

The suggested watermark extraction scheme's pseudocode is shown in Listing 2. It's worth noting that the original video sequence was not required for this operation. Instead, an online forecast of the original pixel values was done. For picture prediction, we utilized a 33 mask in this research. The difference between D+ and C+, as mentioned in Line 18, was used to estimate the watermark. As a result, the sign of the forecast error from the actual value was encoded in a single bit (Line 19). This encoded bit might be multiplied with a pseudo random integer to approximate the watermark. The extraction would not yield the proper picture if the wrong pseudo random sequence was applied.

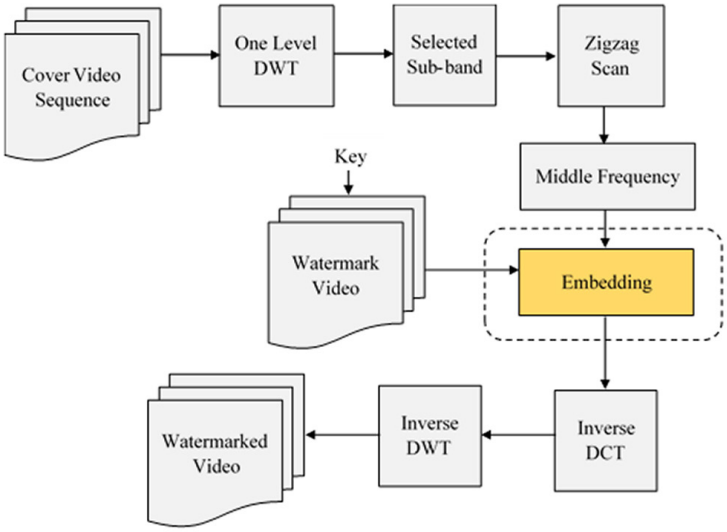

Fig. 3. Watermark embedding block diagram

Algorithm 2: Watermark Extraction Pseudo code
Input: Watermarked video
Output: Watermark video
1: Initialize: Watermark video, Cover Video, key, pseudo random, alpha, 2: For Frames = 1: length (watermarked video) 3: DWT2(watermarked video) → LL(Low Low), LH (Low High), HL(High Low), HH(High High) 4: if frame is even frame Then 5: 2D-DCT(HL) → x+ 6: Else if frame is odd frame Then 7: 2D-DCT2(LH) → x+ 8: End If 9: zigzag scan of (x+) → x** 10: L = Length of x* 11: choose middle frequency to x** ((L*0.375)+1:(L*0.625)) → C+ 12: set C+ to 0 and 1 13: If C+ = 0 Then 14: C+ = –1; 15: End If 16: Video Predicted → using Averaging filter (3×3 mask) 17: repeat step 3 to 11 → D+ 18: watermark delta estimation ← D+– C+ 19: sign (Delta) → watermark video 20: to reduce noise use median filter 21: End For 22: calculate NCC

4 Result analysis and discussion

The results are obtained for different cover video and watermark video. The different quality parameters are recorded for above videos. The following quality parameters

are obtained in different scenarios PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error), and NCC (Normalized Cross correlation). As shown in the Tables 1–4. The cover video is taken as a color video and watermark video is taken as a grayscale video. For different values of α results are taken. The value of α is taken as 12, 14, 16, 18, 20. The Output for 1st Dataset is:

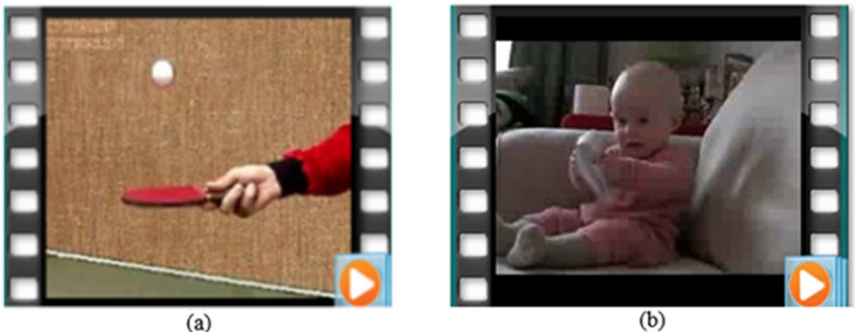

Fig. 4. (a) Cover video and (b) Watermark video

In above Figure 4 Cover video having 200 frames with 500 rows and 500 columns and watermark video having 200 frames with 250 rows and 250 columns. The following Figures 5 and 6 which show the results are taken from above two videos.

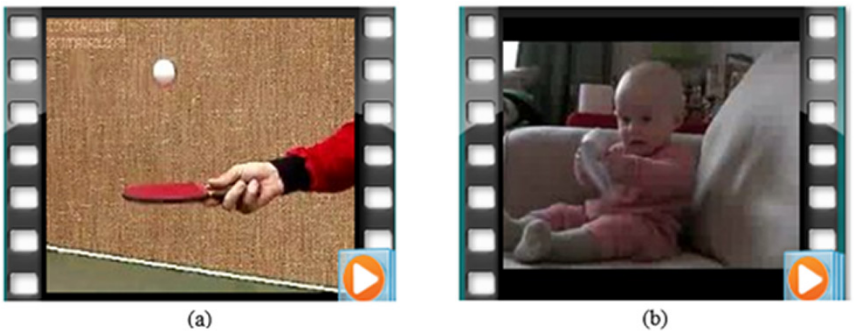

Fig. 5. (a) Watermarked video (b) Recovered (extracted) watermark

Table 1. PSNR, MSE and NCC for Tennis ball video

	A	**12**	**14**	**16**	**18**	**20**
Reference	PSNR	41.44	40.33	38.35	37.25	37.05
	MSE	4.41	6.23	10.45	11.34	12.05
	NCC	0.612	0.657	0.704	0.754	0.768
Proposed Method	PSNR	44.34	42.45	40.56	39.05	38.89
	MSE	2.55	3.45	6.34	9.46	10.67
	NCC	0.853	0.884	0.906	0.927	0.953

Following graph is plotted for alpha value and PSNR. The results show that for Proposed method PSNR is better

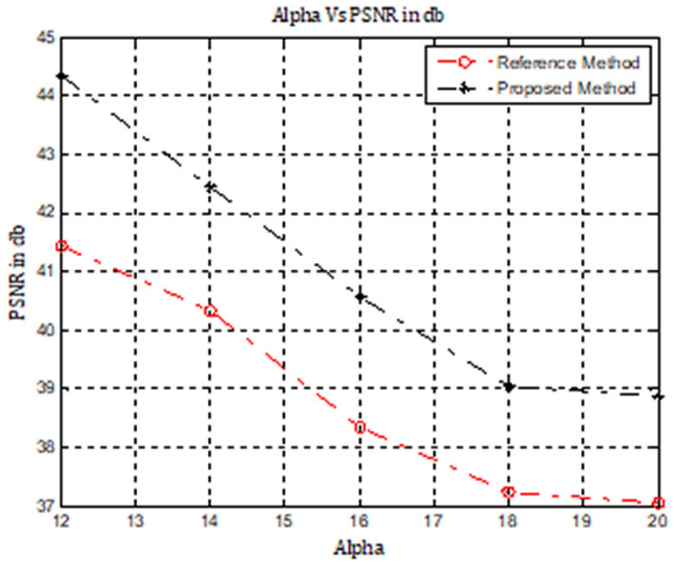

Fig. 6. Graph of alpha Vs PSNR

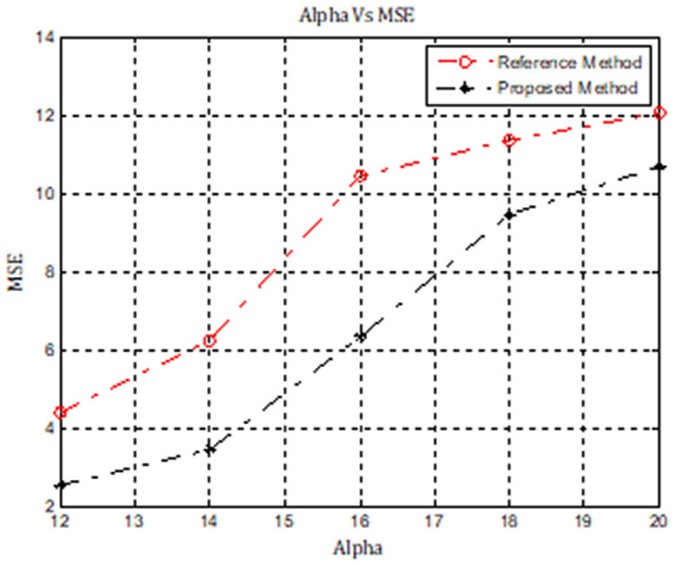

Fig. 7. Graph of alpha Vs MSE

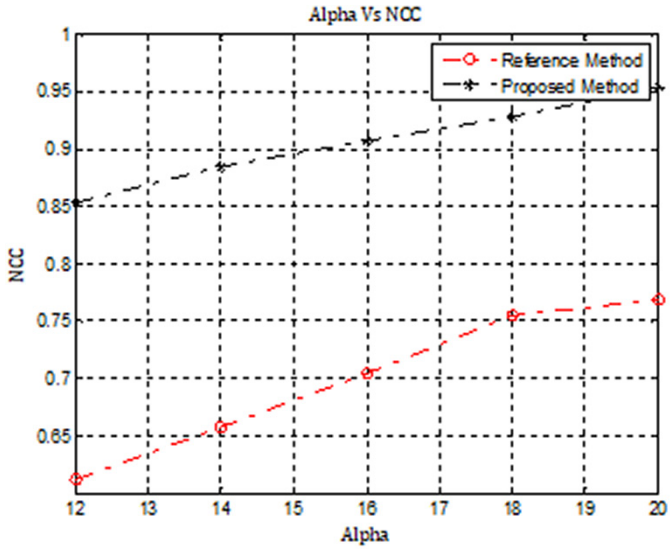

Fig. 8. Graph of alpha Vs NCC

Figures 7 and 8 are graphs of alpha verses MSE and NCC respectively. The graph of alpha verses NCC shows, for proposed method watermark recovery is more as compared with reference paper results. The Output for 2nd Dataset is:

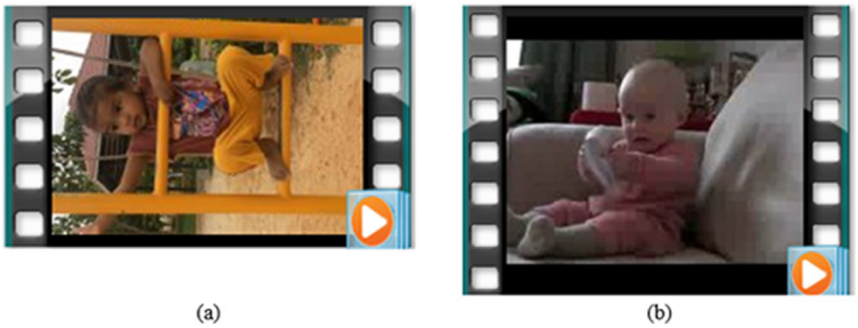

Fig. 9. (a) Cover video and (b) Watermark Video

In above Figure 9 Cover video having 200 frames with 1000 rows and 1500 columns and watermark video having 200 frames with 500 rows and 750 columns. The following results are taken for above two videos.

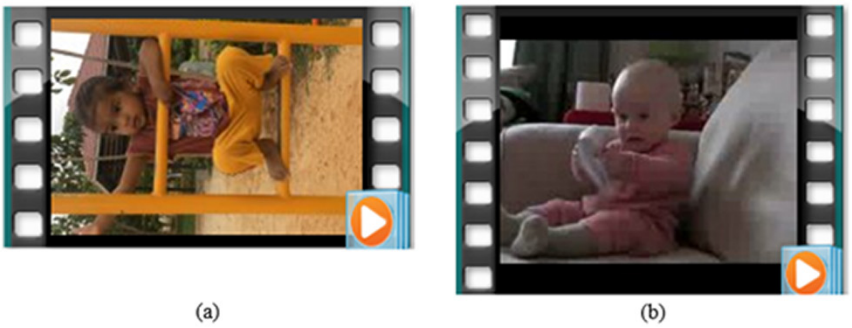

Fig. 10. (a) Watermarked video (b) Recovered (extracted) watermark

Table 2. PSNR, MSE and NCC for child video

	A	12	14	16	18	20
Reference	PSNR	41.92	40.45	38.32	37.56	37.90
	MSE	4.21	6.67	10.87	11.54	12.34
	NCC	0.617	0.658	0.703	0.758	0.766
Proposed Method	PSNR	44.78	42.23	40.56	39.45	38.89
	MSE	2.87	3.76	6.65	9.89	10.32
	NCC	0.856	0.885	0.908	0.922	0.954

Figures 11–13 are plotted for alpha value and PSNR. The results show that for Proposed method PSNR is better

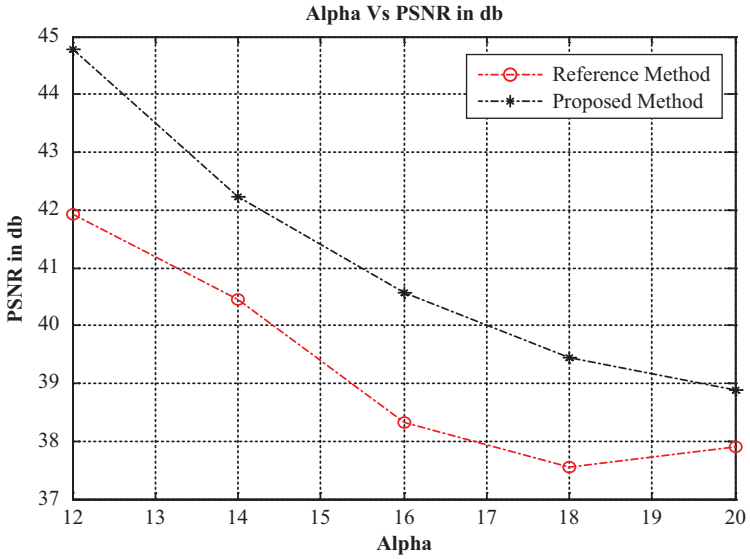

Fig. 11. Graph of alpha Vs PSNR

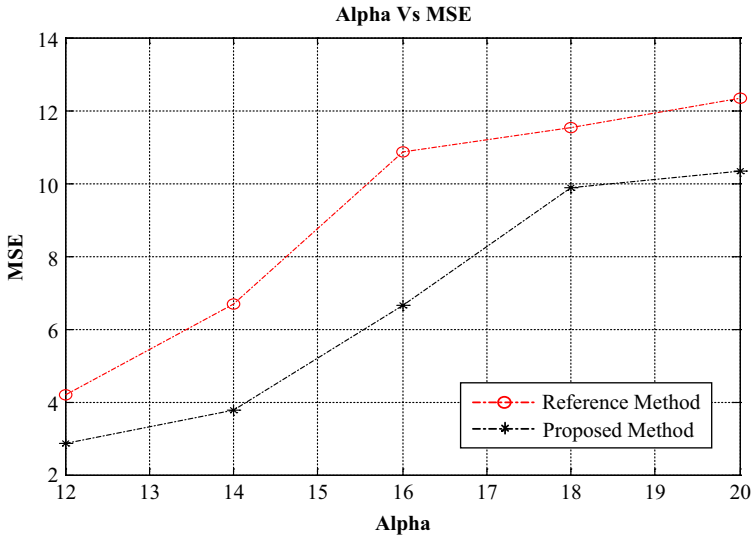

Fig. 12. Graph of alpha Vs MSE

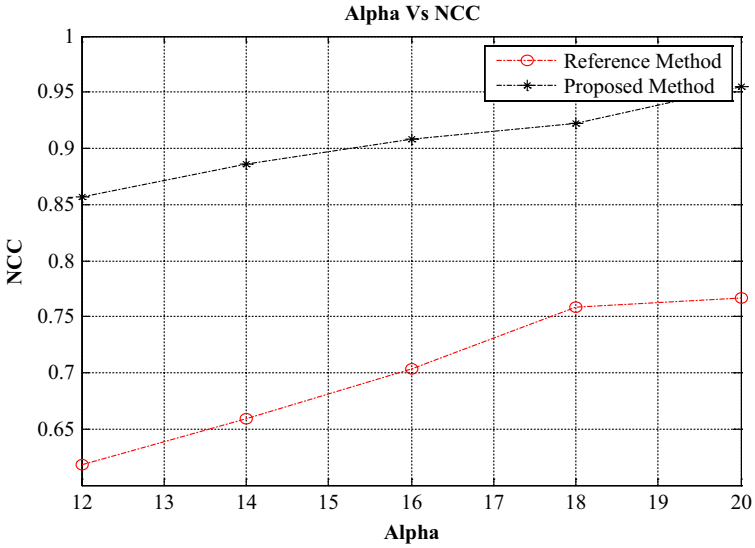

Fig. 13. Graph of alpha Vs NCC

Figures 12 and 13 are graphs of alpha verses MSE and NCC respectively. The graph of alpha verses NCC shows, for proposed method watermark recovery is more as compared with reference paper results.

4.1 Attacks on watermarked video

In this category we have applied different attack on watermarked video for checking robustness of the proposed algorithm. The attacks are mentioned below,

1. Salt and Pepper Noise attack
2. Compression Attack
3. Histogram Equalization Attack
4. Averaging filter Attack
5. Median Filter Attack
6. Gaussian Noise Attack
7. Gaussian filter Attack
8. Cropping Attack

The Salt and Pepper Noise and Compression Attack is given in details. And remaining attacked with their output parameters are mentioned in Table 5.

4.2 Salt and pepper noise attack

The salt and pepper noise added in the watermarked video with noise intensity of 0.09. As shown in Figures 14–16 with Table 3.

Fig. 14. Noise attack

Fig. 15. Recovered watermark

Table 3. NCC for noise attack

	A	12	14	16	18	20
Reference	NCC	0.6012	0.6354	0.6975	0.7456	0.7678
Proposed	NCC	0.7112	0.7867	0.8356	0.8632	0.9167

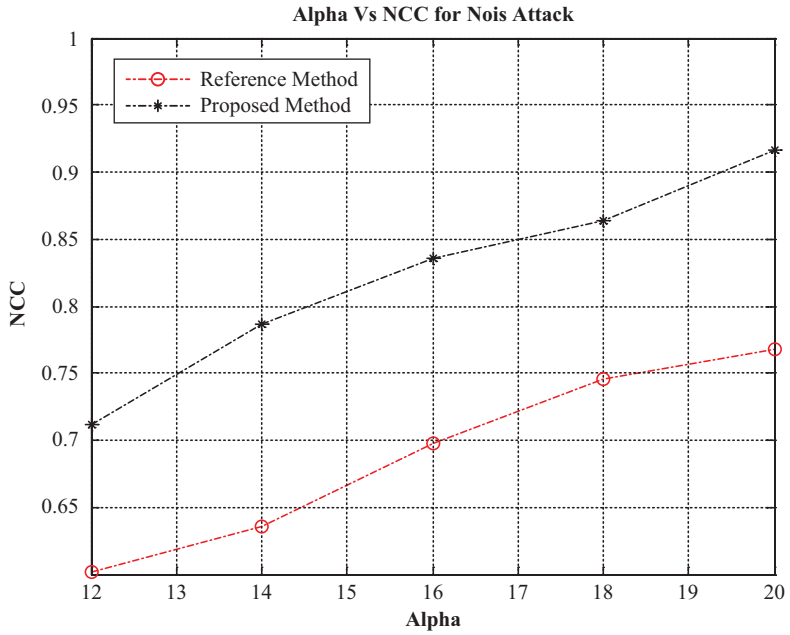

Fig. 16. Graph of alpha Vs NCC for noise attack

4.3 Compression attack

The watermarked video is compressed. After compression watermark removed from attacked video and values of NCC recorded. As shown in the Figures 17–19 with Table 4.

Fig. 17. Compression attack

Fig. 18. Recovered watermark

Table 4. NCC for compression attack

	A	12	14	16	18	20
Reference	NCC	0.6122	0.6367	0.6875	0.7465	0.7601
Proposed	NCC	0.7234	0.7767	0.8302	0.8645	0.8999

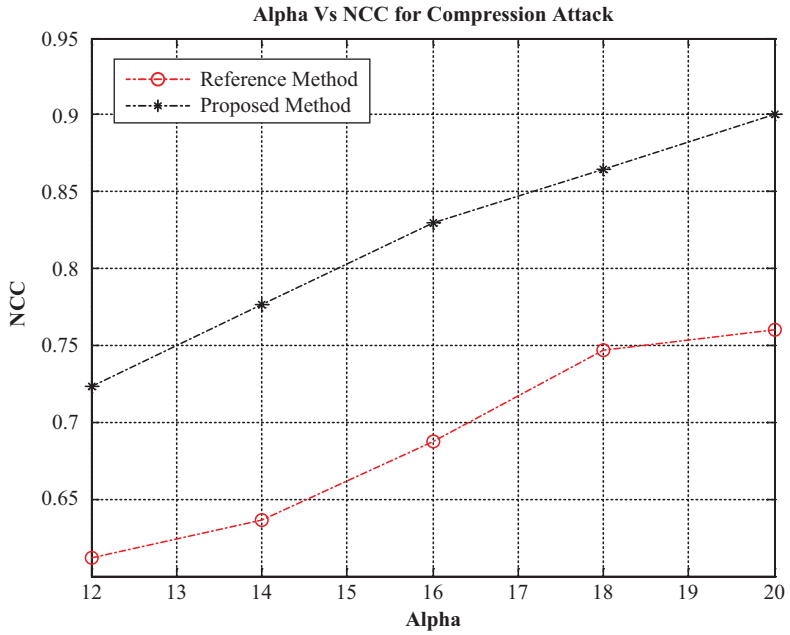

Fig. 19. Graph of alpha Vs NCC for compression attack

The all attacks with their value of NCC are mentioned in the following Table 5. The following Attacks are applied on results of 1st dataset. The tennis ball is cover video and child video as a watermark. For these attacks analysis we consider value of $\alpha = 20$.

Table 5. Different attacks

Attack	Normalized Cross Correlation	
	Reference Method	Proposed Method
Salt and Pepper Noise attack	0.7678	0.9167
Compression Attack	0.7601	0.8999
Histogram Equalization Attack	0.8522	0.9176
Averaging filter Attack	0.8765	0.9234
Median Filter Attack	0.8876	0.9425
Gaussian Noise Attack	0.8123	0.9023
Gaussian filter Attack	0.8567	0.9123
Cropping Attack	0.8234	0.9009

The following Attacks are applied on results of 2nd dataset as shown in Table 6. The Child is cover video and 2nd child video as a watermark. For these attacks analysis we consider value of $\alpha = 20$.

Table 6. Different attacks

Attack	Normalized Cross Correlation	
	Reference Method	Proposed Method
Salt and Pepper Noise attack	0.7756	0.9199
Compression Attack	0.7867	0.9088
Histogram Equalization Attack	0.8455	0.9122
Averaging filter Attack	0.8876	0.9299
Median Filter Attack	0.8977	0.9479
Gaussian Noise Attack	0.8233	0.9122
Gaussian filter Attack	0.8655	0.9243
Cropping Attack	0.8344	0.9122

The Proposed scheme performs better than the reference method. It withstands for all mentioned attacks.

5 Conclusion

This study offers a unique spatio-frequency domain-based invisible watermarking technique. Watermarking was used on the Y component sub-band of a video sequence to carry out the method. The binary watermark image was encoded in the DWT and DCT middle frequency coefficients. The suggested method was able to extract the embedded watermark with visually acceptable quality without the requirement for the original sequence, according to the findings presented here. Based on the video samples, the best magnitude factor was 16, which resulted in a PSNR of up to 38.89 and a normalised Cross correlation (NCC) of up to 0.9535 (in the Tennis ball stream, for example). This algorithm is also robust for Noise and Compression attack.

6 References

[1] M.-S. Hsieh, D.-C. Tseng, and Y.-H. Huang, "Hiding digital watermarks using multiresolution wavelet transform," *IEEE Transactions on Industrial Electronics*, vol. 48, no. 5, pp. 875–882, 2001. https://doi.org/10.1109/41.954550

[2] A. Vaish and S. Jayswal, "A systematic review on various reversible data hiding techniques in digital images," *Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science)*, vol. 14, no. 8, pp. 2421–2435, 2021. https://doi.org/10.2174/2666255813666200221140837

[3] J. Li and A. Sui, "A digital video watermarking algorithm based on DCT domain," in *2012 Fifth International Joint Conference on Computational Sciences and Optimization*, 2012: IEEE, pp. 557–560. https://doi.org/10.1109/CSO.2012.127

[4] D. Fan, X. Zhang, W. Kang, H. Zhao, and Y. Lv, "Video watermarking algorithm based on NSCT, pseudo 3D-DCT and NMF," *Sensors*, vol. 22, no. 13, p. 4752, 2022. https://doi.org/10.3390/s22134752

[5] H. T. ALRikabi and H. T. Hazim, "Secure chaos of 5G wireless communication system based on IOT applications," *International Journal of Online & Biomedical Engineering*, vol. 18, no. 12, 2022. https://doi.org/10.3991/ijoe.v18i12.33817

[6] X. Jing, Y. Liu, X. Chen, and P. Zhou, "The domain block video watermarking scheme based on video sequences' characteristics and DCT," in *2012 7th International Conference on Computer Science & Education (ICCSE)*, 2012: IEEE, pp. 448–452. https://doi.org/10.1109/ICCSE.2012.6295111

[7] M. Mosleh, S. Setayeshi, B. Barekatain, and M. Mosleh, "A novel audio watermarking scheme based on fuzzy inference system in DCT domain," *Multimedia Tools and Applications*, vol. 80, no. 13, pp. 20423–20447, 2021. https://doi.org/10.1007/s11042-021-10686-6

[8] N. Alseelawi and H. T. Hazim, "A novel method of multimodal medical image fusion based on hybrid approach of NSCT and DTCWT," *International Journal of Online & Biomedical Engineering*, vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28011

[9] P. Campisi and A. Neri, "3D-DCT video watermarking using quantization-based methods," in *2007 15th European Signal Processing Conference*, 2007: IEEE, pp. 2544–2548.

[10] X. Wang, C. Liu, and D. Jiang, "A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT," *Information Sciences*, vol. 574, pp. 505–527, 2021. https://doi.org/10.1016/j.ins.2021.06.032

[11] I. A. Aljazaery and A. H. M. Alaidi, "Encryption of color image based on DNA strand and exponential factor," *International Journal of Online & Biomedical Engineering,* vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28021

[12] M. Cedillo-Hernandez, A. Cedillo-Hernandez, and F. J. Garcia-Ugalde, "Improving dft-based image watermarking using particle swarm optimization algorithm," *Mathematics*, vol. 9, no. 15, p. 1795, 2021. https://doi.org/10.3390/math9151795

[13] H. Tao, L. Chongmin, J. M. Zain, and A. N. Abdalla, "Robust image watermarking theories and techniques: A review," *Journal of Applied Research and Technology*, vol. 12, no. 1, pp. 122–138, 2014. https://doi.org/10.1016/S1665-6423(14)71612-8

[14] M. Cedillo-Hernandez, F. Garcia-Ugalde, M. Nakano-Miyatake, and H. Perez-Meana, "Robust watermarking method in DFT domain for effective management of medical imaging," *Signal, Image and Video Processing*, vol. 9, no. 5, pp. 1163–1178, 2015. https://doi.org/10.1007/s11760-013-0555-x

[15] A. H. M. Alaidi, R. a. M. Al_airaji, I. A. Aljazaery, and S. H. Abbood, "Dark web illegal activities crawling and classifying using data mining techniques," *International Journal of Interactive Mobile Technologies,* vol. 16, no. 10, 2022. https://doi.org/10.3991/ijim.v16i10.30209

[16] L. Sharma, A. Anand, N. K. Trivedi, M. Sharma, and J. Singh, "Digital video watermarking: Features, techniques, and challenges," *Annals of the Romanian Society for Cell Biology,* pp. 3376–3385, 2021.

[17] H. A. Naman and M. Al-dabag, "Encryption system for hiding information based on internet of things," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 15, no. 2, 2021. https://doi.org/10.3991/ijim.v15i02.19869

[18] H. T. Salim and H. T. Hazim, "Enhanced data security of communication system using combined encryption and steganography," *International Journal of Interactive Mobile Technologies*, vol. 15, no. 16, pp. 144–157, 2021. https://doi.org/10.3991/ijim.v15i16.24557

[19] I. A. Aljazaery and M. R. Aziz, "Combination of hiding and encryption for data security," *International Journal of Interactive Mobile Technologies*, vol. 14, no. 9, pp. 34–47, 2020. https://doi.org/10.3991/ijim.v14i09.14173

[20] R. A. Azeez, M. K. Abdul-Hussein, and M. S. Mahdi, "Design a system for an approved video copyright over cloud based on biometric iris and random walk generator using watermark technique," *Periodicals of Engineering Natural Sciences*, vol. 10, no. 1, pp. 178–187, 2021. https://doi.org/10.21533/pen.v10i1.2577

[21] H. H. Mirza, H. D. Thai, Y. Nagata, and Z. Nakao, "Digital video watermarking based on principal component analysis," in *Second International Conference on Innovative Computing, Informatio and Control (ICICIC 2007)*, 2007: IEEE, pp. 290–290. https://doi.org/10.1109/ICICIC.2007.267

[22] E. Chrysochos, V. Fotopoulos, and A. N. Skodras, "Robust watermarking of digital images based on chaotic mapping and DCT," in *2008 16th European Signal Processing Conference*, 2008: IEEE, pp. 1–5.

[23] S. A. Al-Taweel and P. Sumari, "Robust video watermarking based on 3D-DWT domain," in *TENCON 2009-2009 IEEE Region 10 Conference*, 2009: IEEE, pp. 1–6. https://doi.org/10.1109/TENCON.2009.5395859

[24] S. A. Mostafa, A. Tolba, F. Abdelkader, and H. M. Elhindy, "Video watermarking scheme based on principal component analysis and wavelet transform," *International Journal of Computer Science and Network Security*, vol. 9, no. 8, pp. 45–52, 2009.

[25] S. Sinha, P. Bardhan, S. Pramanick, A. Jagatramka, D. K. Kole, and A. Chakraborty, "Digital video watermarking using discrete wavelet transform and principal component analysis," *International Journal of Wisdom Based Computing*, vol. 1, no. 2, pp. 7–12, 2011.

[26] M. Choubisa, K. Hiran, and S. Singh, "Permutation based invisible digital watermarking technique using DCT domain," *International Journal of Computer Applications,* vol. 30, pp. 40–44, 2011.

[27] P. Ghosh, R. Ghosh, S. Sinha, U. Mukhopadhyay, D. K. Kole, and A. Chakroborty, "A novel digital watermarking technique for video copyright protection," *Computer Science and Information Technology*, pp. 601–609, 2012. https://doi.org/10.5121/csit.2012.2360

[28] N. I. Yassin, N. M. Salem, and M. I. El Adawy, "Block based video watermarking scheme using wavelet transform and principle component analysis," *International Journal of Computer Science Issues (IJCSI)*, vol. 9, no. 1, p. 296, 2012. https://doi.org/10.1109/ICEngTechnol.2012.6396128

[29] N. Kashyap and G. Sinha, "Image watermarking using 3-level discrete wavelet transform (DWT)," *International Journal of Modern Education and Computer Science,* vol. 4, no. 3, p. 50, 2012. https://doi.org/10.5815/ijmecs.2012.03.07

[30] J. Panyavaraporn and P. Horkaew, "DWT/DCT-based invisible digital watermarking scheme for video stream," in *2018 10th International Conference on Knowledge and Smart Technology (KST)*, 2018: IEEE, pp. 154–157. https://doi.org/10.1109/KST.2018.8426150

7 Authors

Hussein Tuama Hazim, His Major is Master of electronic and telecommunication engineering from University of Pune, India. Works as lecturer at Department of electrical engineering in university of Misan in Amarah, Misan city Iraq where he thought several courses. His current research interest includes wireless communication, artificial intelligent, deep learning, intelligent control systems and internet of things. The number of articles in international data base is 8. Contact: +9647735717775. E-mail: hussein.tuama@uomisan.edu.iq

Nawar Alseelawi, is faculty member college of engineering, electrical engineering department, university of Misan in Misan city, Amarah, Misan, Iraq. He received his master in electronics and telecommunication from university of Baghdad, Iraq. The number of articles in national data base – 1. The number of articles in international data base – 4. E-mail: nawar.alseelawi@uom.edu.iq

Haider Th. Salim ALRikabi, He is presently Asst. Prof and one of the faculty College of Engineering, Electrical Engineering Department, Wasit University in Al Kut,Wasit, Iraq. He received his B.Sc. degree in Electrical Engineering in 2006 from the Al Mustansiriya University in Baghdad, Iraq. His M.Sc. degree in Electrical Engineering focusing on Communications Systems from California state university/Fullerton, in USA in 2014. His current research interests include Communications systems with the mobile generation, Control systems, intelligent technologies, smart cities, the Internet of Things (IoT), Renewable Energy, Smart Cities, Security Systems,and Communication Networks. Al Kut city–Hay ALRabee, Wasit, Iraq. E-mail: hdhiyab@uowasit.edu.iq. The number of articles in national databases – 20, and the number of articles in international database – 65.

Article submitted 2022-12-21. Resubmitted 2023-01-23. Final acceptance 2023-01-24. Final version published as submitted by the authors.