ISSN 2303-4521
Periodicals of Engineering and Natural Sciences *Original Research*
Vol. 10, No. 2, April 2022, pp.283-291

Improve a secure blind watermarking technique for digital video

Faten H. Mohammed Sediq Al-Kadei[1], Sohaib Najat Hasan[2]
[1, 2] Northern Technical University, Technical Institute Kirkuk, Kirkuk, Iraq

ABSTRACT

In recent years, digital watermark video has become increasingly popular in a range of industries, but because it is widely available on the Internet, it is simple to make unlawful copies and tamper with digital video. Watermarking digital video has become more popular as a method of detecting changes and preventing illegal duplication. This paper presents a video copyright protection system that is secure, blind, and robust. Two approaches that are resistant to diverse attacks are proposed in this research. The initial step is to encrypt a hybrid watermark (Message, Image) using two different encryption techniques (RSA and AES). The second is a steganography technique based on LSB-based robust watermarking, which embeds an encrypted secret bit Message and Image in key frames of an MP4 video file by utilizing the mean of the grayscale images that differ and take the most significant differences between the two images. The intensity of the histogram will become more consistent across all pixels as the encryption quality improves. For keyframe watermarking in the spatial domain, the proposed methods can maintain the watermarked information while achieving high imperceptibility and a Peak Single to Noise Ratio [PSNR] equivalent to more than 50 db, where quality measures (MSE, PSNR, and correlation coefficient) that calculate the levels of distortion caused by embedding a watermark in digital video produce good results.

Keywords: Image Encryption, Message Encryption, Hiding, Watermarking, AES, RSA, PSNR

Corresponding Author:

Faten H. Mohammed Sediq Al-Kadei
Northern Technical University, Technical Institute Kirkuk
Kirkuk, Iraq
faten.alqadhi@ntu.edu.iq

1. Introduction

Data ownership, authentication, and protection factors all play a role in the secure transfer of data over the internet. Data can be in the form of a character array, a picture, or a video. Digital watermarking and other information-hiding technologies for digital data have also received a lot of interest. Digital watermarking is a technique for hiding a text encoded with digital signals in a range of media, such as images, sounds, and video, inside the sign itself [1]. In Videos Digital watermarking, watermarks are categorized into three groups: photo watermarking, video watermarking, and audio watermarking. Among them, the most often used watermarking technique is video watermarking. Because video media content has the highest prevalence of copyright infringement and abuse [2]. The purpose of using video watermarking is to give the genuine owner of the video a personality. Different watermarking methods are necessary for different forms of digital content, such as still photographs, videos, and documents [3]. Watermark embedding, extraction, and detection are the three main components of a complete watermarking approach. It normally encrypts the data and adds copyright watermarks that aren't visible. Certification, symbols, digital signatures, and other copyright watermarks are examples of invisible copyright watermarks. For copyright protection, a variety of elements determine the viability of a digital watermarking algorithm, one of the most important of which is its resilience to various attacks. As a result, one of the key areas of digital watermarking research has been to improve algorithm robustness against a variety of attacks [4]. Steganography is used for hiding data in both science and art. In steganography, there are two methods for image embedding: 1) spatial domain and 2) transform domain. In the spatial domain, in the Least Significant Bits (LSBs), messages are immediately included. On the other hand, the transform domain changes the image coefficient's frequencies of the cover (e.g., wavelet, discrete cosine, or Fourier). Watermarks are directly embedded in the pixels of video frames using spatial domain technique, whereas the latter approach

adjusts the transform coefficients of video frames and embeds the data into it.In comparison to spatial domain approaches, frequency domain techniques are also undetectable [5].
Assessing their quality is the main purpose of comparing the cover and stego photos. To assess stego-image quality in this comparison, Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE) are used. The first step is to determine how different the original cover is from the noisy or distorted Stego image.

$$MSE = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} \left(S_{xy} - C_{xy} \right) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.(1)$$

The input image has X and Y coordinates, as well as N and M columns and rows. Sxy is the image that was made, and Cxy is the image that was used to make the cover.

PSNR=10 log 10 (C2max/MSE) …..…………… (2)

The MSE and PSNR can be calculated using equations (1) and (2), respectively.

The internet has grown into a critical instrument for information transfer, online commerce, money transfer, and payment. On the other side, cryptography assists in the effective protection of information in order to prevent interception.When cryptography is utilized, attackers are unable to hack videos since they lose control of their data prior to sending, making it hard to recover the originals.AES stands for Advanced Encryption Standard and is a set of principles for encrypting data AES is a symmetric key algorithm, which means it encrypts and decrypts data with the same key. The performance (security and speed) of AES was chosen because it is appropriate for encrypting data transferred over the Internet. RSA (Rivest-Shamir-Adleman) is an asymmetric encryption method that uses two independent keys called private (public) keys used to decrypt (encrypt) data. In the literarure, one of the most extensively used asymmetric public key encryption algorithms is the RSA algorithm [6,7]. This paper utilizes RSA and AES algorithms to encrypt the hybrid watermarks (Message and Image) respectively before embedding them in key frames of MP4 video file using a modified LSB data hiding technique.

2. Literature survey

A number of researchers have experimented with video watermarking techniques. SURF-DCT is a robust watermarking approach that combines: discrete cosine transform, speeded-up robust features, and blind watermarking. Against geometric and traditional attacks, experiments demonstrated good invisibility and robustness of the method. Additionally, the tests revealed that it is able to protect images successfully with a normalized correlation coefficient value of more than 90% [8]. The Least Significant Bit (LSB) approach was modified using three output metrics: PSNR, MSE, and SSIM. Because of the production of a more durable, high-capacity, highly undetected image, the results showed an outperformance over current conventional techniques, with a lower MSE value a higher PSNR value compared to existing systems [9]. The encrypted obscured picture was properly secured using a two-level concealing strategy. The outcomes revealed that the approach encryption methods had made the system with a very secure image, with the hidden image integrity and validity being preserved by the large number of encryption keys [10]. Other research sought to develop a video steganography system that would provide appropriate security while allowing data (video frames) to be inserted in other video frames at a rapid computation speed. There are two ways to embed and encrypt video frames in a cover video file. To begin, a large number of different encryption keys were produced using two keys and the XOR bit operation. Secondly, in the selective cover video frame, high-quality video frames (bitmap color) were buried using a modified Least Significant Bit (LSB) approach, resulting in two layers of security [11]. Another approach is to create an image encryption system that strikes a balance between speed and complexity. The Advanced Encryption Standard (AES) is a symmetric-key algorithm and consists of rules for encrypting. In other words, AES uses the same key to encrypt and decrypt data. It was selected for its performance (security and speed). Accordingly, AES is ideal for encrypting data sent over the Internet [12].
RSA(Rivest-Shamir-Adleman) is an asymmetric encryption technology that performs encryption and decryption using two separate keys called public and private keys. As mentioned earlier that the RSA algorithm is one of the most widely used asymmetric public key encryption algorithms. The results of three tests were compared to elicit and debate the improved points in the RSA method encryption and decryption operations. In addition, for speeding up the encryption or decryption process, several programming techniques were utilized. A novel picture compression and encryption approach based on a modified JPEG methodology paired with the Hexa-Coding algorithm has been proposed in previous studies[13-16].

3. Video watermarks

Video watermarking is the process of adding watermarks to a video sequence in order to prevent unlawful copying and detect alterations. In the literature, various robust and fragile video watermarking technologies were developed to identify manipulations and address the issues of unauthorized copying and proof of ownership. A video watermark is a method of embedding electronic data into a video sequence for the purposes of identification annotation and copyright. Although image watermark operations can be applied to video watermarks, the repeating of information results in certain unnecessary features [17]. The following are some important factors to consider while developing video watermarking systems:

- Invisibility: In order for the watermark data encoded in the video to be imperceptible to the naked eye, it must be imperceptible. Overall, the insertion of watermark data cannot completely impact the visual element of the video.
- Robustness: It aims to assure that the data is protected from intruders by the watermark that has been inserted. Embedded watermarks can be detected in the footage even after the assault. Simple image processing methods such as contrast or enhancement, brightest gamma correction, and so on can be used to erase watermarks, either intentionally or accidentally.
- Security: Embedded data is tamper-proof, which is the most essential evidence of a digital item's protection from hackers.
- Capacity: To easily identify the video's owner, the amount of embedded data should be sufficient. Scientists proposed a number of alternatives for video watermarking, such as: copyright protection, video authentication, broadcast monitoring, copy control, and fingerprinting [18][19].

The primary video watermarking applications are listed below:

- Digital Fingerprinting: Digital fingerprinting is a means of establishing who owns what digitally. The person who owns the digital data has a fingerprint that is unique to them. A single piece of digital content may have many fingerprints since it pertains to distinct people.
- Copy control: For video watermarking, protected copy is a common technique. The aim of deploying a watermark is to identify whether video content is copyrighted. Protected copy is a popular video watermarking technique, it is used in this situation to indicate whether the video content is copyright protected. This watermark is recovered by substantially degrading the video sequence only.
- Broadcast Monitoring: This tool is primarily used in commercials to guarantee that the advertisement was broadcast according to the agreement. It can also be used to find out where unlicensed radio stations are broadcasting.
- Video Authentication: Users can successfully change video footage using today's common video editing tools. As a result, verification measures are required to ensure the content's validity; one method is the use of sophisticated watermarks. As a watermark, the timestamp, camera ID, and casing chronic numbers are inserted into every frame of the video stream.
- Copyright protection: To safeguard intellectual property, the owner of video data can include a watermark that represents copyright data in the video data. When someone violates the owner's copyrights, this watermark may be used to prove ownership in court. Watermarking a video to protect it from copyright infringement can be done in a number of ways [20][21].

Adding or changing the pixel value of the embedding path of the video frame is the process of embedding a watermark in the spatial field. The benefits of spatial domain watermarking include simplicity, reduced processing time, and low computational complexity [22].

Some of the methodologies that use spatial domain watermarking are:

The first is the Least Significant Bit (LSB) approach, which involves embedding the watermark within the least significant bits of the original video. The LSB, which communicates the least amount of relevant information, is replaced with the watermark bits in this approach, making it untraceable. The watermark can be applied anywhere on or in a particular area of the video frame. Another approach is to construct a pseudo-random noise and apply it to the brightness channel of cover media pixels using correlation-based algorithms. [23][24].

4. Proposed method

A technique for verifying digital data such as images, documents, and videos is digital watermarking. Watermarking provides copyright protection for digital material by obscuring some crucial information. The use of encryption and embedding methods to hide encrypted hybird watermarks (Message, Image) over an mp4 video file is offered as an intelligent solution to video watermarking .This work is categorized into three stages:

first, frames are extracted from a video file, then important frames are chosen. Key-frame extraction tries to improve recognition efficiency by reducing computer complexity and removing unneeded frames. The second step is to encrypt hybird watermarks (Message, Image) using (RSA, AES) encryption techniques, and the third step is to use a modified LSB technique to hide the encrypted watermarks in keyframes throughout the video file (Figure 1).

The proposed research algorithms' software was written in the Microsoft Visual Studio (Python platform 3.7) programming language, which is widely recognized as one of the most popular programming languages in the domains of computer vision and image processing due to its numerous advantages, including the ease with which video processing can be implemented.

The main algorithms for the proposed system were summarized in the steps below:
Step 1: Find and open the secret MP4 video file.
Step 2: Take frames out of the video file.
Step 3: Determine key frames.
  Step 3.1: Convert frames to grayscale images.
  Step 3.2: Compare and contrast grayscale images.
  Step 3.3: Take the mean of the grayscale images that differ.
  Step 3.4: Select N frames of most significant changes between the two images.
Step 4: Choose the watermarks (Image and Message).
Step 5: Using the AES technique, encrypt the watermark image.
Step 6: Using the RSA technique, encrypt the watermark message.
Step 7: Hide encrypts blind watermarks in the key frames of an mp4 video file using a modified LSB technique.
Step 8: To produce a video, combine stego frames.
Step 9: Generate the stego Mp4 video.

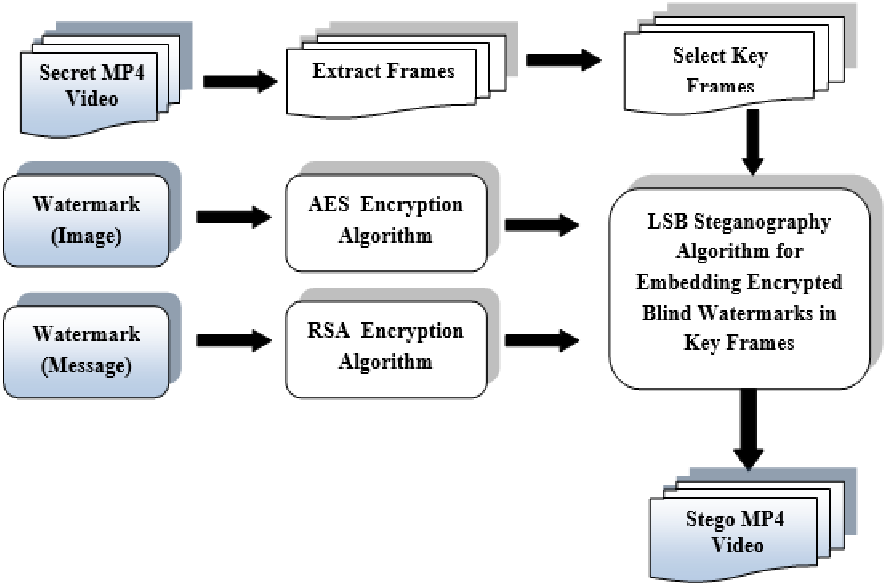


Figure 1. Hiding encrypted watermarks (message, image) in Mp4 video key frames

As shown in Figure 2, to recover the original (Secret) video, reverse the procedures to un-hide and decrypt it:
1st, load the Stego Mp4 video file.
2- Take frames out of the Stego video.
3- From the stego video, select key frames.
4- Remove encrypts blind watermarks (Message, Image) from an MP4 video file by un-hiding them.
5- Using the RSA and AES methods, decrypt hybrid blind watermarks (Message, Image).
6- Recover the original message and image watermarks
7- Combine frames to recover a MP4 video file.
8- Recovery MP4 video file.

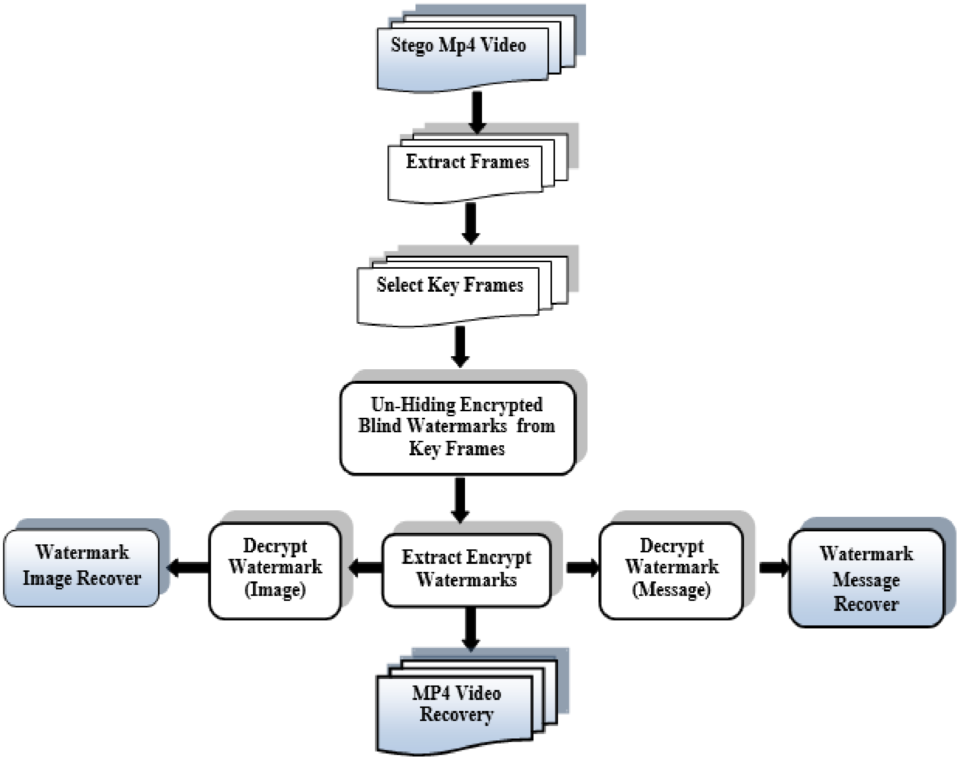

Stego Mp4 Video
Extract Frames
Select Key Frames
Un-Hiding Encrypted Blind Watermarks from Key Frames
Watermark Image Recover
Decrypt Watermark (Image)
Extract Encrypt Watermarks
Decrypt Watermark (Message)
Watermark Message Recover
MP4 Video Recovery

Figure 2. Unhiding and decrypting watermarks (message, image) from key frames of a Stegio Mp4 video

5. Results and discussion

The method has been evaluated on a variety of watermarks, images, and messages, as well as secure cover MP4 videos (Sample 1, 2 and 3) (see Table 1). The proposed method was designed with the Microsoft Visual Studio (Python platform 3.7) programming language libraries, and it's a great way to manage movies with tools like histograms and math to back it up. Figures (4, 5, and 6) showed variety examples of how the suggested method steps work. The experimental results showed that the Stego video key frames performed well, with low correlation and a high PSNR.As follows, the proposed system became operational and applicable:-

a) The initial step is to extract frames from the secret MP4 video, and then use the mean of the grayscale frames that deviate to choose important key frames that contain more video details.

b) Choose a watermark image and use the AES technique to encrypt it.

c) Choose a watermark message and encrypt it with the RSA technique.

d) The message and image pixels' histograms were evaluated, and they indicated a good correlation (Figure 3).

e) The encrypted secret watermarks (message, image) were embedded in key frames of the cover MP4 video using the LSB approach in the second step. The quality of each cover key frame was then determined using PSNR.

f) All of the cover key frames utilized in the concealing operation were of high quality, according to the results. As a measure, PSNR was more than 50 Db (see Table 2).

Table 1. Samples of MP4 Video Files

Video Name	Video Size (MB)	No. of Frame	Frame Rate	Frame Size
Sample1	3.92	475	30	1280 x 720
Sample2	10	1655	25	640 x 480
Sample3	17.6	1946	24	1280 x 720

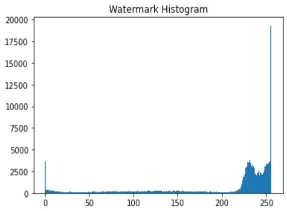
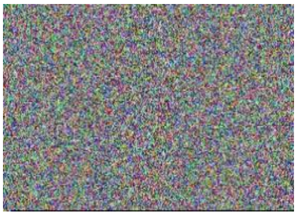
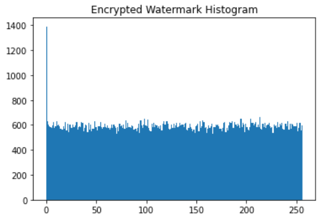
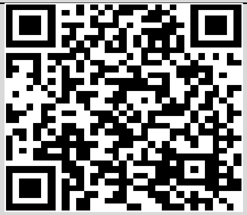
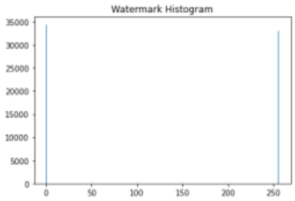
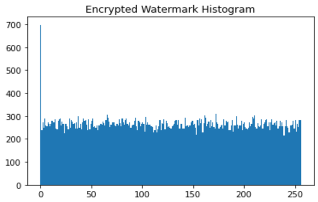
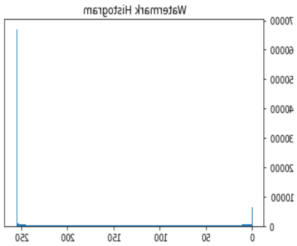
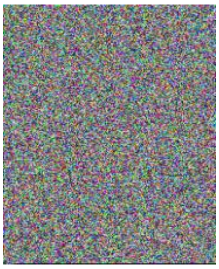
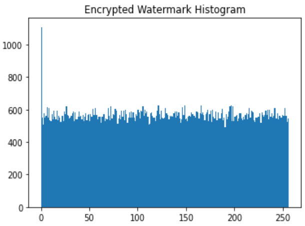
Watermark Images	Watermark Image Histogram	Encrypt Watermark Image	Encrypt Watermark Image Histogram
			
			
			

Figure 3. Original and encrypted watermarking images histograms

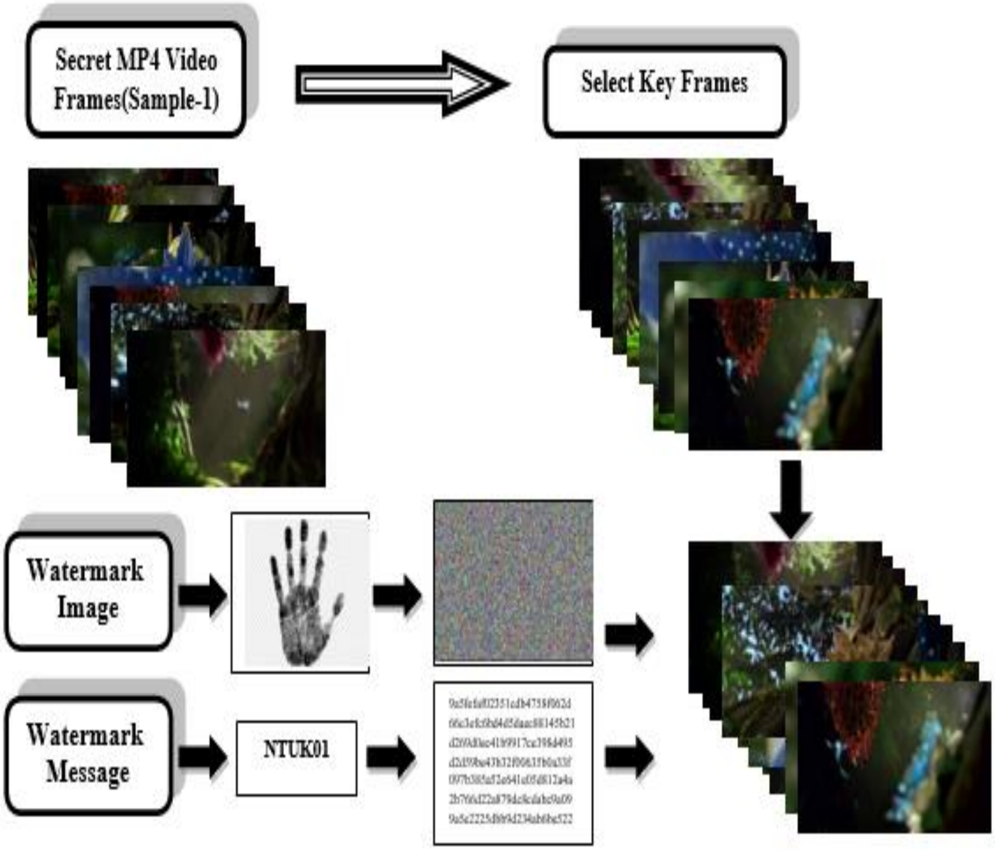


Figure 4. The proposed method’s stages for sample -1 MP4 video

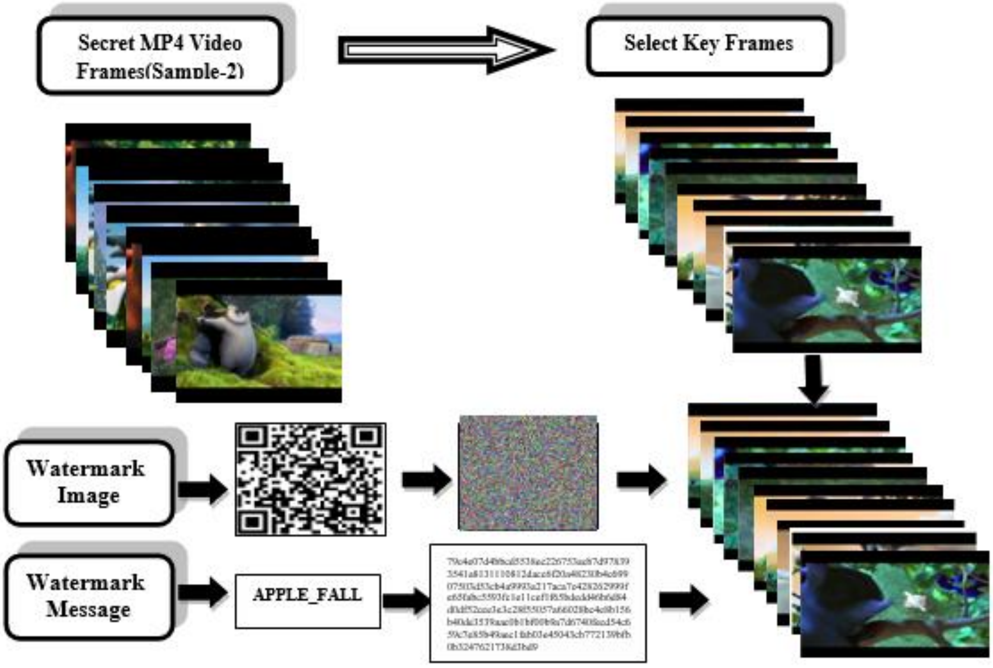


Figure 5. The proposed method’s stages for sample -2 MP4 video

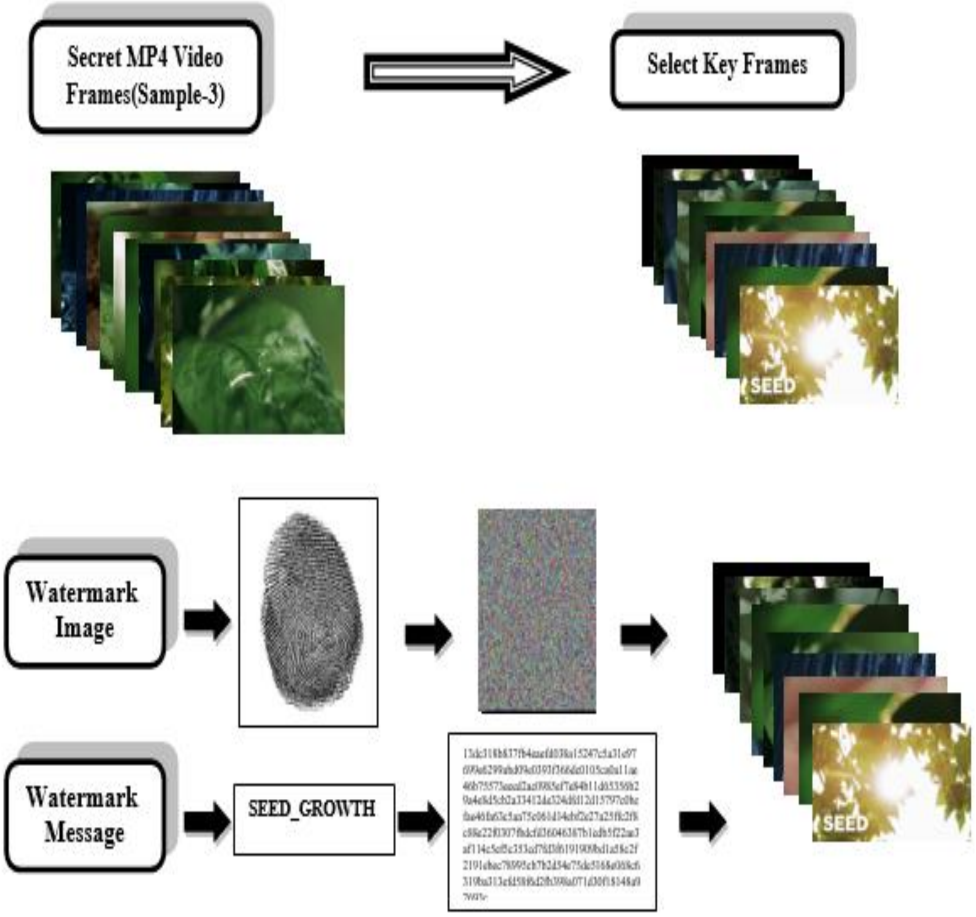
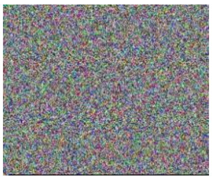


Figure 6. The proposed method’s stages for sample -3 MP4 video

Table 2. After the Hiding Operation, the PSNR of Cover Video Key Frames

Key Frame No.	Cover Video Key Frame	Encrypted Watermark Image	Encrypted Watermark Message	Stego Video Key Frame	PSNR
319			9a5fefaf02351cdb4758f062d66c3efc6bd4d5daec88145b21d269d0ec41b9917ce398d495d2d59be43b32f00635b0a33f097b385a52e641e05d812a4a2b766d22a879dc8cdabc9a099a5e2225dbb9d234ab6be522f58756ce2625e88b2c1c0d396a92d1cf7a7f32c143de51ec75d9de50a4639574b94cdc5cc2eecbb79b8a8f		**54.9987**
1087			79c4e07d4bbcd5538ec226753a4cb7d978393541a8131110812dacc6f20a48230b4c69907503d53cb4a9993a217aca7c428262999fe65fabc5593fc1e11cef1f65bdedd46b6d84d0df52cce3e3c28f55057a66028bc4e8b156b40de3539aac0b1bf00b9a7d6740fecd54c659c7e85b49aec1fab03e45043cb772139bfb0b3247		**53.4272**
1552			13dc318b837fb4eaefd038a15247c5a31e97699e6299abd09e0393f366dc0105ca0a11ae46b75573eeed2ac0985ef7e84b11d65356b29a4e8d5cb2a33412de324dfd12d15797c0bcfae46fa63c5aa75c061d14ebf2e27a25ffc2f8c88e22f0307fbdcfd36046387b1cdb5f22ae3af114c5ef5c353cd7fd3f6191909bd1a58c2f		**54.9180**

7. Conclusion

An effective manner to video watermarking is to employ encryption and embedding technologies to hide encrypted hybird watermarks (Message, Image) over an mp4 video file. This paper presents a safe, blind, and robust video copyright protection system that uses hybrid techniques to encrypt watermarks (message, image) with different cipher algorithms (RSA for message watermark and AES for image watermark) and then hide them in keyframes after extracting frames from various MP4 videos.The suggested approach provides good encryption-decryption quality and good hide by producing good MSE and PSNR values.The histogram will reflect a more uniform intensity of the histogram value across all pixels as the encryption quality improves. The PSNR value exceeded 50 db, showing that the differences between the cover and stego key frames are invisible to the naked eye. The image intensity did not change significantly since the encrypted message and image were embedded in the key frames using mainly the LSB approach.

Declaration of competing interest

The authors declare that they have no any known financial or non-financial competing interests in any material discussed in this paper.

References

[1] G. Nagaraju, P. Pardhasaradhi, V. S. Ghali, and G.R.K Prasad, “Secure hybrid watermarking technique in medical imaging”, *Eur. J. Mol. Clin. Med*, vol.07, no. 05, pp. 160-167, 2020.

[2] G. Doerr and J. L. Dugelay, “A guide tour of video watermarking,” *Signal Process. Image Commun.*, vol. 18, no. 4, pp. 263–282, 2003.

[3] B. Sridhar and C. Arun, “An interlacing technique-based blind video watermarking using wavelet,” *Int. J. Comput. Inf. Eng.*, vol. 9, no. 6, pp. 1521–1524, 2015.

[4] C. Wei and L. Zhaodan, “Robust watermarking algorithm of color image based on DWT-DCT and chaotic system”, in *Proceedings of the 1st IEEE International Conference on Computer Communication and the Internet (ICCCI)*, Wuhan, China, 2016, pp. 370–373.

[5] M. Kumar, S. Sriastava, and A. Hensman, “A hybrid novel approach of video watermarking”, *Int. J. Signal Processing, Image Processing and Pattern Recognition*, vol.9, no.10, pp. 395-406, 2016.

[6] M. K. I. Rahmani, K. Arora, and N. Pal, “A crypto-steganography: A survey”, *International Journal of Advanced Computer Science and Applicatio*, vol. 5, no. 7, pp. 149-154, 2014.

[7] A. A. J. Altaay, S. B. Sahib, and M. Zamani, “An introduction to image steganography techniques”, in

Proceedings of the International Conference on Advanced Computer Science Applications and Technologies (ACSAT), Kuala Lumpur, Malaysia, 2012, pp. 122-126.

[8] S. A. Nawaz, J. Li, U. A. Bhatti, A. Mehmood, M. U. Shoukat, and M. A. Bhatti, “Advance hybrid medical watermarking algorithm using speeded up robust features and discrete cosine transform,” *PLoS One*, vol. 15, no. 6, pp. e0232902, 2020.

[9] R. O. Ogundokun, O. C. Abikoye, S. Misra, and J. B. Awotunde, “Modified Least Significant Bit Technique for Securing Medical Images,” in *European, Mediterranean, and Middle Eastern Conference on Information Systems*, 2020, pp. 553–565.

[10] F. H. M. S. Al-kadei, “Two-level hiding an encrypted image”, *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 2, pp. 961-969, 2020.

[11] F. H. M. S. Al-kadei, “Robust video data security using hybrid cryptography-technique”, *Periodicals of Engineering and Natural Sciences*, vol. 8, no. 3, pp.1741-1751, August 2020.

[12] F. T. A. Hussien, A. M. S. Rahma ,and H. B. A. Wahab, “A Secure Environment Using a New Lightweight AES Encryption Algorithm for E-Commerce Websites”, *Security and Communication Networks*, 15 pages, December 2021.

[13] F. H. M. S. Al-kadei, H. A. Mardan, and N. A. MINAS,” Speed Up Image Encryption by Using RSA Algorithm”, in *Proceedings of the 6th International Conference on Advanced Computing & Communication Systems*, Coimbatore, India, 2020, pp. 1302-1307.

[14] A. N. Nasret, A. B. Noori, A. A. Mohammed, Z. S. Mahmood, “Design of automatic speech recognition in noisy environments enhancement and modification”, *Periodicals of Engineering and Natural Sciences*, vol. 10, no. 1, pp.71-77, January 2022.

[15] M. D. Hassan, A. N. Nasret, and M. R. Baker, “Enhancement automatic speech recognition by deep neural networks”, *Periodicals of Engineering and Natural Sciences*, vol. 9, no. 4, pp. 921-927, November, 2021.

[16] M. H. Rasheed, O. M. Salih, and M. M. Siddeq, ”Joint image encryption and compression schemes based on hexa-coding”, *Periodicals of Engineering and Natural Sciences*, vol. 9, no. 2, pp.569-580, April 2021.

[17] 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, 2022.

[18] P. S. Sethuraman, and R. Srinivasan, “Survey of digital video watermarking techniques and its applications,” *Eng. Sci.*, vol. 1, no. 1, p. 22-27, December 2016.

[19] S. B. Latha, D. V. Reddy, and A. Damodaram, “Video watermarking using neural networks,” *Int. J. Inf. Comput. Secur.*, vol. 14, no. 1, pp. 40–59, 2021.

[20] M. Asikuzzaman and M. R. Pickering, “An overview of digital video watermarking,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 9, pp. 2131–2153, 2017.

[21] K. M. Lande, “Survey of digital watermarking techniques and its application,” in *Int. J. of Innovative Tech. and Exploring Eng.*, vol. 6, no. 6, pp. 437-441, June 2019.

[22] V. C. S. R. Shankar, R. V. Prasad, R. V. Adiraju, R. V. V Krishna, and D. Nandan, “A Review Paper Based on Image Security Using Watermarking,” in *Proceedings of International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications*, 2021, Telangana, India, pp. 697–706.

[23] P. Singh and R. S. Chadha, “A survey of digital watermarking techniques, applications and attacks,” *Int. J. Eng. Innov. Technol.*, vol. 2, no. 9, pp. 165–175, March 2013.

[24] C. Hui and L. Fei, “A digital watermarking algorithm with high efficiency based on DWT and LSB,” *DEStech Trans. Comput. Sci. Eng.*, no. aicae, 2019.