Video Watermarking with Digital Signature and Fingerprinting

Milan Gupta and Wei Qi Yan
Auckland University of Technology, Auckland 1010 New Zealand

ABSTRACT

A digital watermark, which is embedded in an image sequence or video frames as the form of a binary string or visual logo, is a small size of visible data. Thus, the quality of embedded videos is often slashed due to watermarking. Comparative video watermarking is a highly innovative method that was designed to unravel this issue. In this chapter, singular value decomposition (SVD) and discrete wavelet transform (DWT) are employed for video watermarking, inverse transform (IDWT) is adopted to extract the video watermark. The digital signature is also utilized to increase the authenticity of watermarks and verify any changes. This approach is combined with digital fingerprinting as well to get the improved results. Throughout the designed attacks, the merits of the new watermarking paradigm such as robustness, convergence, and stability are attained with security and authenticity by calculating the metrics such as MSE, PSNR, entropy, SSIM, etc.

Keywords: Video Watermarking, DWT, SVD, PSNR, Entropy, Digital Signature, Digital Fingerprinting

INTRODUCTION

Digital watermarking is a way of embedding secure information into digital media for transcoding. A machine-detectable pattern that could be put on several documents for anti-counterfeiting purposes was identified in 1979. A number of years later, a method for embedding an identification code into an audio signal was identified by researchers. Researchers firstly employed the term digital watermark in 1988. The notion of digital watermarking gained widespread acceptance in the early 1990s. The first information hiding workshop (IHW), which included digital watermarking as one of its key topics, was held in 1996 (Gupta, 2021).

A watermark is visible where it is easily seen by the owner and observer or invisible where decoding algorithms can be identified by the originator (Gupta, 2021). The watermark needs to be durable for this application so that it cannot be broken by digital media alteration. The algorithm needs to be blind, another prerequisite for watermarking for copyright protection. The host media is not needed to remove the watermarking information for blind operations. Security is an important issue that requires only the owner to change the watermark. The number of special sessions held at recent conferences and the efforts made on related European projects such as Certimark and Encrypt are a good indication of the increasing interest in this topic, whereas watermarking robustness has usually been associated with the possibility of decoding error or resistance to removal of watermarks, the definition of watermarking protection is still fuzzy.

Recent work has been accepted that security attacks have wider applications than robustness attacks, as the former is concerned not only with the simple impairment of communication mechanism but also with the achievement of rights given by the system's hidden parameters. Watermarking helps to recognize the actual possessor of digital information. It is one of the potential strategies for securing digital information.

Digital watermarking is an effective approach for protecting intellectual property and copyrights by shielding multimedia data such as photographs, videos, or audio files from information such as signatures, logos, or manuscripts. However, a high risk of piracy is also seen by copyright owners, especially large Hollywood studios and music labels. Using analogue devices leads to a lower risk in the past than using digital media; copying an analogue file contributes to consistency degradation. However, songs and movies can be generated without any quality degradation using digital media recording, because the data is a stream of 0's and 1's.

Cryptography provides a small security measure; once the decrypted material enters the consumer, there will be no further security. Therefore, further content protection is required, even after it is decrypted. The watermarking is a popular approach that is used to comply with the creator's copyright rights. The knowledge is hidden inside the content in digital watermarking. Digital watermarking can withstand various types of attacks, including compression, conversion from digital to analogue, and changes in file format. In order to fulfil all these processes, a watermark can be created.

For copy prevention and copyright protection, watermarking has been well-thought-out. The watermark may be used in copyright protection applications to recognize the copyright holder and ensure sufficient payment of the royalties. Although copyright security and copy prevention have been major drivers of watermarking field research, there are a range of earlier applications for which watermarking has been used. It includes broadening, monitoring, monitoring activities, and confirmation. Medical photographs, satellite images, and photos taken by mobile phone cameras include other applications.

Usually, one hidden key is used in the watermarking process. The essential element of information that the material is legitimate or not by identifying the watermark is the hidden key. Insertion or embedding is called positioning in watermarking process. The process that the watermark is extracted is called watermark extraction. The use of a watermark is also a solution for copyright security and authentication of ownership; the digital data becomes much stable and is safe from infringement. There are various types of methods available for watermarking including watermark extraction. Each of them offers various characteristics and functions that can be used for multiple purposes.

Digital watermarking has been utilized for multiple functions, such as copyright protection, broadcast tracking like watermarked videos from an international news agency, hidden or subchannel communications, etc. If visible information is embedded in the media as a watermark, the watermark is termed as visible digital watermark. This may be a logo or a text that marks a digital medium (Po-Chyi, et al. 2017; Langelaar, Setyawan, & Lagendijk, 2000).

In this chapter, we take advantage of digital videos as the host media for watermarking which is referred to as video watermarking. This is often applied to verify the believability of digital media or to acknowledge the identity of the owner of the media. So, the purpose of this research work is to come up with an approach that overcomes the limitations of the existing watermarking process by providing more secure and robust ways of video watermarking.

In this chapter, a watermarking method is proffered for copyright protection of digital videos. The watermarking is implemented based on two mathematical transforms. The first one is the discrete wavelet transformation (DWT), while the second is singular value decomposition (SVD). These two models are from frequency domain and spectrum domain respectively, thus are completely distinct and generate different outcomes, however, the levels of security against an attack are distinguished. A watermark is embedded in the video that carries the hidden data regarding sender and receivers to verify whether the watermark has been tampered or not (Natarajan & Govindarajan, 2015). The digital fingerprinting is combined with watermarking to achieve the improvised results. Video fingerprinting takes use of d a digital

rights management (DRM) which is use of technological tools to identify, extract, and represent the attributes belonging to a video file. This is to identify the video by its unique "fingerprint".

In this book chapter, the selected literature will be surveyed, later the methodologies are delineated, the experimental results will be expounded as the follow, and the conclusion will be drawn finally.

RALATED WORK

In this book chapter, the work related to digital watermarking is explicated. Firstly, the digital watermarking approaches based on the frequency domain of digital videos are surveyed. We see that frequency domain is suitable for watermarking (Deepak & Prachi, 2018). In order to accomplish the watermark embedding, in this chapter, two singular value matrices are generated and have been employed to host watermarks. All video frames are taken as the watermarking objects by using the proffered algorithms. DWT is applied to watermark video frames. With high stability, SVD is conducted based on the obtained HL2 subbands, and watermark embedding is implemented (Muthumanickam & Arun, 2018).

A distinct method of video watermarking has been developed by paying zero cost, digital files are very easy to be copied. Users mostly download and share multimedia data such as images, audio clips, and video footages. Hence, there is a great possibility of digital information being duplicated. Therefore, it necessitates prohibiting the copyright of digital media (Anjali & Parul, 2018).

In order to support SVD and MR-SVD in fast motion frames, one of the algorithms based on wavelets, SVD, and transform split the frames of the cover video into red, green, and blue (RGB) bands. While most of the prevailing watermarking schemes have placed the watermark in each video frame, which spends enormous time and also has a noticeable impact on the quality of the video, the projected methodology selects only the fast motion frames in each shot to host the watermark (Imen, 2018).

Another approach took use of Haar wavelet transform and LSB in digital watermarking for the purpose of video authentication (Pallavi, 2018) (Wahid, et al. 2018) (Harahap & Khairina, 2020). This aids to remove random noises by embedding a visual watermark so as to prevent attacks in the least significant part of the cover image. The results show that the planned method provided excellent hidden invisibility, reasonable security, and well-hidden attacks (Tasheva, Tasheva, & Nakov, 2017) (Saqer & Barhoom, 2016).

Finally, Hash algorithms were introduced to apply cryptography on a watermarked image for achieving the purposes of authentication and security in watermarking. MD5 was accommodated with LSB substitution (Nurul, Muhammad, & Juanda, 2018)(Pradhan, Sekhar, & Swain, 2018)(Khairina, Harahap, & Lubis, 2018), similar approaches were proposed where Hash algorithm was applied to specifically the selected pixels (Mohd, *et al*. 2018).

A watermarking approach mingling with the digital signature was taken advantage of Hash algorithm and asymmetric key cryptography together to achieve a high level of security and authenticity. Thus, the sender's private key was generated with a digital signature, the receiver's public key was employed to encrypt the media data and signatures (Antony & Uma, 2014)(Li´skiewicz, Reischuk, & Wölfel, 2017). Individual signature was computed from the selected pixels which are hidden in the designated pixels of the same image. This method preserved the size of the image and does not create any significant distortions

which are visible to human eyes (Sahib, *et al*. 2018). The digital watermarking was combined with fingerprinting techniques to identify the copyrights for colour images (Hsieh, Chen, & Shen, 2014). It involved the fingerprint and watermarked image generation and the authentication of logo detection phase.

In this paper, we propose SVD in the frequency domain associated with DWT for video watermarking. The watermarked video is segmented into single frames. The LSB method has been applied to visual watermarking.

METHODS

The proposed algorithm encapsulates two branches: Watermark embedding and watermark extraction. The flowchart of the proposed watermarking scheme follows the steps shown as Figure 1.
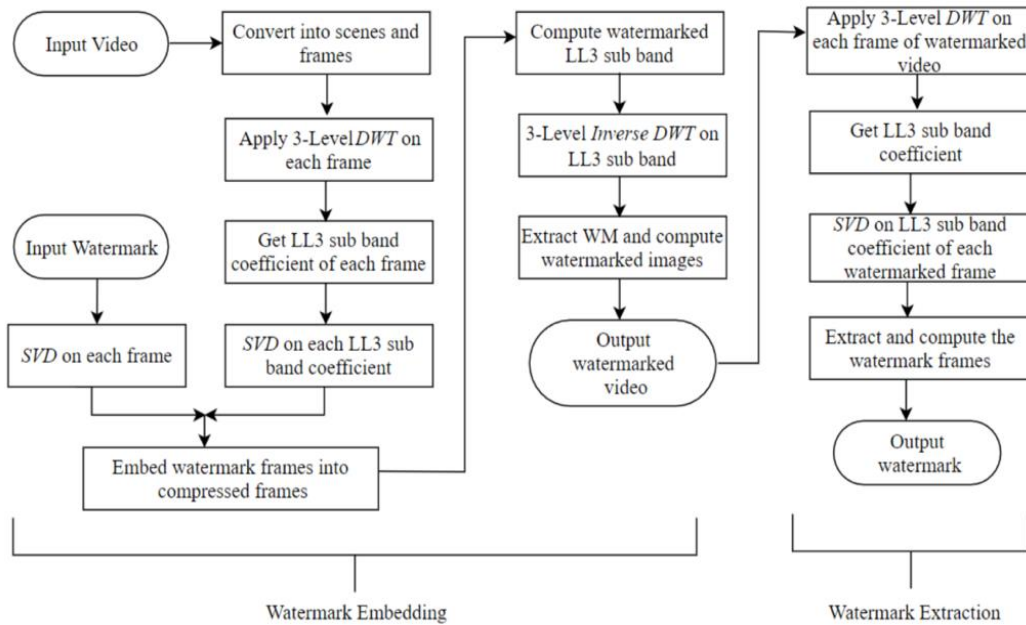
Figure 1. The proposed watermarking scheme

The steps for watermark embedding:

- Decompose the watermark image into m different watermark images.

$$W = W_1, W_2, W_3, ..., W_m \tag{1}$$

- Apply singular value decomposition (SVD) for each of the watermark images.

$$[Uw(j). Sw(j) . Vw(j)] = SVD(W(j)) \tag{2}$$

where $j = 1,2,3,...,m$.

- Split the host video into scenes and frames.
- Apply DWT on each frame of the scene to retrieve the *LL3(j)* subband coefficients.
- Apply SVD for each compressed frame of the jth scene.

$$[U_i(j) \cdot S_i(j) \cdot V_i(j)] = svd(LL_{3i}(j)) \tag{3}$$

where *i* is the number of video frame in the seq *j*.

- Add watermark information into each compressed frame of the jth scene.

$$D_i(j) = S_i(j) + K \times S_w(j) \tag{4}$$

where *K* is watermarking strength.

- Compute watermarked *LL3'* subband coefficients and apply 3-level inverse DWT to get WM components.

$$LL_{3i}'(j) = U_i(j) \cdot D_i(j) \cdot V_i(j) \tag{5}$$

- Reconstruct all watermarked frames and retrieve the watermarked video.

The steps for watermark extraction:

- Apply 3-level DWT to each frame of the jth sequence of watermarked video to retrieve $LL_3'(j)$ subband coefficients.
- Apply SVD to each compressed frame of the jth sequence of the watermarked video.

$$[U_i'(j) \cdot S_i'(j) \cdot V_i'(j)] = SVD (LL_{3i}'(j)) \tag{6}$$

where *i* is frame sequence in *j*-th scene, SVD(·) is the singular value decomposition function.

- Extract the watermark image *w'*(*j*) for the jth sequence

$$W'(j) = U_w'(j) \cdot S_w'(j) \cdot V_w'(j) \tag{7}$$

where $S_w'(j) = (S_i'(j) - S_i(j))/K$

- Finally, a single watermark is reconstructed from the extracted watermark images.

$$W = W_1 + W_2 + W_3 + \cdots + W_m \tag{8}$$

A digital signature is a kind of cryptographical methods. The process of a digital signature is quite akin to the handwritten signature having a digital certificate that is applied to verify the identity. The signature affirms that the verifying information is originated from the party having the respective signature on it.

Cryptography, as well known, means keeping communication security and providing a better mechanism of information security by using encryption and decryption. Cryptography is implemented at present by

using any of the following three ways: symmetric key (SKC), asymmetric key (AKC) – using public-private keys, hash functions (one-way cryptography).

The Hash function is to generate a unique value for the data on which it is being applied. Hashing is employed to provide authentication in a much better way than that of encryption, which is a way of generating a hash value according to the visual contents of the applied image. There are a wealth of Hash algorithms with different techniques like message Digest (MD5), secure hash algorithm (SHA), etc. MD5 is the most famous one in the family of Hash algorithms.

In digital signature, Hash is generated from the original message, the digital signature is produced with the sender's private key, this data is encrypted with the receiver's public key. On the receiver's side, the data is decrypted with the receiver's private key as it was encrypted by using the receiver's public key. The digital signatures will be verified with the sender's public key at the receiver side, which confirms that it has been sent by the intended sender without an intruder involved. Later, Hashing is calculated based on received data at the receiver's side and compared against what was sent with the message. If both match, then all good; Otherwise, it indicates there is a data breach or compromise of security in the data transfer.
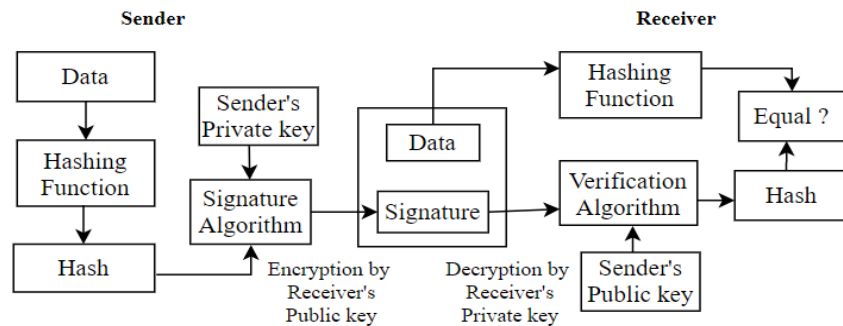

Figure 2. The proposed scheme of digital signature

The proposed algorithm of video watermarking is extended further to uplift the privacy, security, and authentication in the field of video watermarking. As we know, digital signature guarantees that the contents of the transit message will not be altered, the message is originated via the intended sender only. Through considering the high degree of privacy, security, and authenticity provided by a digital signature, we fully make use of digital signature along with Hash algorithms to generate the watermarks. Now, this watermark is able to be used for video watermarking to verify the authenticity and ownership of any video footage. The proposed algorithm is combined with Hash algorithm and digital signature during the watermarking time. The steps of video watermarking with digital signature are:

- Segment the host video into frames.
- Apply the hash function (MD-5) to the cover image (or frame) to generate the message digest (Di).
- Apply encryption scheme (RSA) to this digest to generate the digital signature (Si).
- This digital signature itself is used as a watermark which will be embedded video frames, from where it is generated.
- Use the watermarking embedding steps for each video.

6

- Finally, the embedded watermark is reconstructed along with the digital signatures, the same is used as a watermark for corresponding frames/images.

The steps of watermark extraction with digital signature:

- Follow the watermarking extraction steps for each frame/image. It will provide the extracted watermark (Wi, i.e., the digital signature embedded as a watermark) and actual digital signature (Si) sent with each frame/image.
- Apply a decryption scheme (RSA) to this digital signature (Si) and retrieve the message digest (Di).
- Retrieve the message digest (Di') by applying the decryption scheme (RSA) on the extracted watermark (Wi).
- The two message digests (i.e., Di' and Di) are compared to verify the authenticity, integrity, and ownership of the respective image/frame or video.

The proposed approach in this chapter is combined with the digital fingerprinting method to have better efficiency and robustness. It takes use of image secret sharing (ISS) that generates a share image from two images. After generating the feature image from the base image, another identifiable (or logo) image is added to generate the secret shared image. This method has two phases:

(1) Initially, feature extraction is applied to extract the features of the base image and then scrambling is employed to disarrange the authentication logo to a scrambled logo image. After this, the fingerprint is generated by using extracted features and the scrambled logo, this is called fingerprint generating. Finally, the fingerprint is employed as a watermark and is embedded in the base image, to generate the watermarked image. We have stored the fingerprint in a database to use in the next phase.

(2) This phase detects the watermark first and procced with fingerprint detection. After watermark retrieval, the watermark features of the suspect image are extracted by using feature extractor. Now, logo restoration is conducted by using the extracted watermark and the extracted features to recover and rearrange the scrambled logo. Finally, logo comparison is accomplished and the detection is completed if the accuracy rate of the restored logo is high enough; Otherwise, the next available fingerprint is retrieved from the database, then it returns to logo restoration step, which takes as input the retrieved fingerprint instead of the extracted watermark. The process continues to loop until no fingerprint is available or authentication logo is discovered.

For various continuous frames of a video, we have a watermarking scheme from frame-by-frame perspective. In this scheme, we embed a different pseudo-random watermark in each video frame as shown in eq.(9).

$$F'_t = F_t + \alpha \cdot W_t(K) \tag{9}$$

where F'_t represents the luminance of the t-th video frame, F_t is the luminance of the t-th watermarked frame, α is the embedding strength and K is a secret key. Each inserted watermark $W_t(K)$ has a normal distribution with unit variance and zero mean which is different at every instant t. Regarding the pseudo-random generator, $K+t$ is employed as a seed to retrieve this property. The perceptual shaping is introduced to improve the invisibility of the watermark even if a global embedding strength has been used in practice.
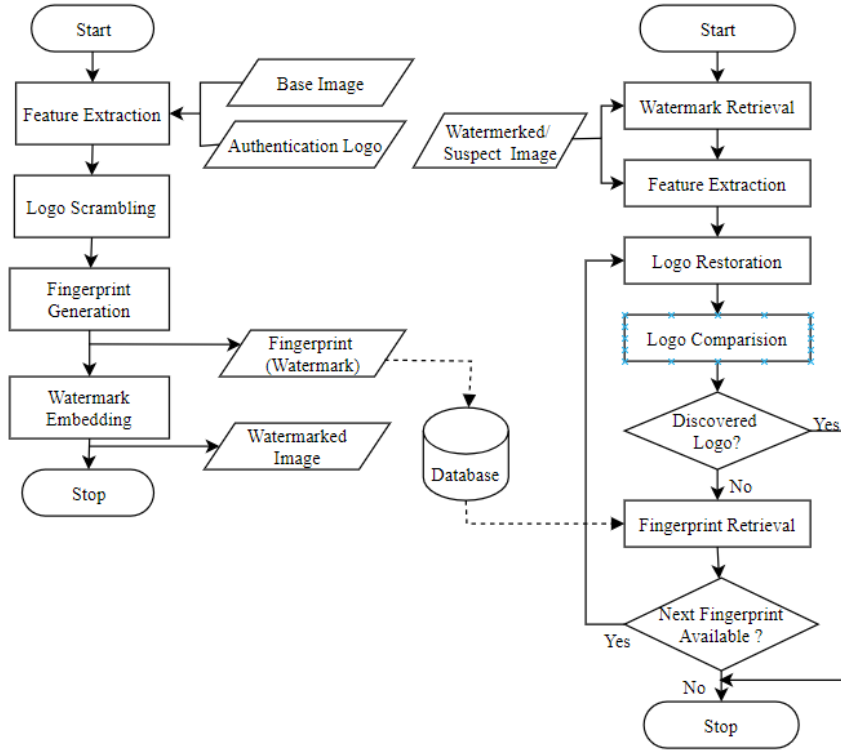
Figure 3. Fingerprint & watermarked image generating and logo detection

RESULTS

The proposed approach is applied to evaluate the performance. The videos are segmented into a sequence of frames to leverage and enrich the sample datasets. A rich assortment of images/frames are employed in the watermarking process with the proposed watermarking approach. Figure 4 shows the images from the datasets.

The proposed watermarking approach is employed to multiple images and video frames, so as to generate the watermarked images. SSIM is applied to measure the effectiveness of the watermarked image and extracted watermark, i.e., to evaluate the performance of the proposed watermarking approach with these samples.

Structural Similarity Index Measure (SSIM) is an alternative visual quality metric that is used to measure the similarity between two videos. It is a full reference metric. The weakness of PSNR and MSE metrics is that sometimes they do not represent the several distortions perceived by the human visual system. SSIM is more effective at estimating the perceptual quality of images than the PSNR and MSE as it considers image degradation as a perceived change in structural information. Structural information is the idea that the pixels have strong interdependencies especially when they are spatially close. These dependencies carry important information about the structure of the objects in the visual scene. The similarity measure using SSIM is already proven very robust and versatile in various environments. SSIM output varies from -1.0 to 1.0, where -1.0 represents very noticeable distortion and 1.0 stands for perfect quality. The SSIM is given as eq.(10).

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c1)(2\sigma_{xy} + c2)}{(\mu_x^2 + \mu_y^2 + c1)(\sigma_x^2 + \sigma_y^2 + c2)} \qquad (10)$$

8

where μ_x is the average of x, μ_y is the average of y, σ_x^2 is the variance of x, σ_y^2 is the variance of y, σ_{xy} is the covariance of x and y, and c1,c2 are constant variables to stabilize the division. SSIM takes advantage of luminance, contrast, and structure comparison functions to estimate the perceived quality of an image. The luminance comparison is carried between the original image and the degraded image by using the eq. (11).

$$LC = \frac{2\mu_x\mu_y}{\mu_x^2+\mu_y^2}$$ (11)

where $\mu_x = \bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$, $\mu_y = \bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i$. The contrast comparison between the original image and the degraded image is calculated by using the eq. (12).

$$CC = \frac{2\sigma_x\sigma_y}{\sigma_x^2+\sigma_y^2}$$ (12)

where $\sigma_x^2 = \frac{1}{N-1}\sum_{i=1}^{N}(x-\bar{x})^2$, $\sigma_y^2 = \frac{1}{N-1}\sum_{i=1}^{N}(y-\bar{y})^2$. The structural comparison for the original and the degraded image is done by using eq. (13).

$$SC = \frac{\sigma_{xy}}{\sigma_x\sigma_y}$$ (13)

where $\sigma_x = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i-\mu_x)^2}$, $\sigma_y = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i-\mu_y)^2}$, $\sigma_{xy} = \frac{1}{N-1}\sum_{i=1}^{N}(x-\bar{x})(y-\bar{y})$, N as the size of the image(s), x_i and y_i as the intensity of the original and the degraded image, and $\bar{x}$ and $\bar{y}$ as the mean intensity of respective images, all these three comparisons are combined to calculate SSIM as,

$$SSIM(x,y) = LC \cdot CC \cdot SC$$ (14)

$$SSIM(x,y) = \frac{2\mu_x\mu_y}{\mu_x^2+\mu_y^2} \cdot \frac{2\sigma_x\sigma_y}{\sigma_x^2+\sigma_y^2} \cdot \frac{\sigma_{xy}}{\sigma_x\sigma_y}$$ (15)

This is as same as what we have seen earlier with c_1 and c_2 are 0.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y+c1)(2\sigma_{xy}+c2)}{(\mu_x^2+\mu_y^2+c1)(\sigma_x^2+\sigma_y^2+c2)}$$ (16)

Mean square error (MSE) for various images is quite low while the respective Peak Signal to Noise Ratio (PSNR) is quite high. This indicates that the effectiveness and performance of the proposed approach image watermarking from the given dataset are good. The other metric like similarity structure index measure (SSIM) is quite high and approaches 1.00, which reveals that the similarity of the images before and after watermarking remains intact by using the proposed. Similarly, mean, variance, and entropy in Table 1 signify the effectiveness and robustness of the proposed solution with a given dataset.

There are several types of tampering methods that is able to be implemented in a watermarked image before extracting the watermarks. The proposed approach is evaluated by applying several attacks on the watermarked images. The watermark is extracted post-attack(s) and the parameters are calculated to measure the performance of the applied process/approach as it is calculated in earlier cases.

Various signal processing operations to conduct the noise modifications/attacks (non-geometrical attacks) are implemented based on the watermarked image of Lena. The attacks of salt & pepper noises (with variance 0.05 and 0.01) are applied to evaluate the results of the proposed approach, it shows the respective PSNR and Normalized Correlation (NC) values for the attacked watermarked images and the extracted watermarks in Figure 5. The image dataset is shown as Figure 4.
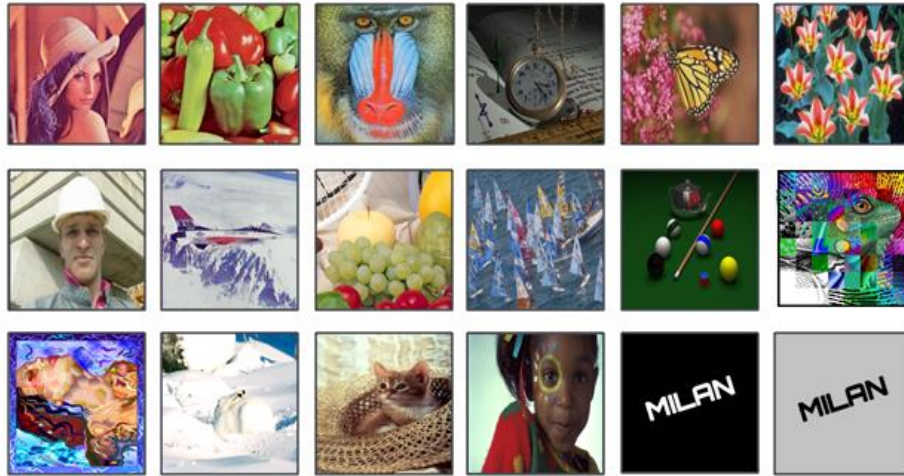
Figure 4. Sample images or video frames from datasets
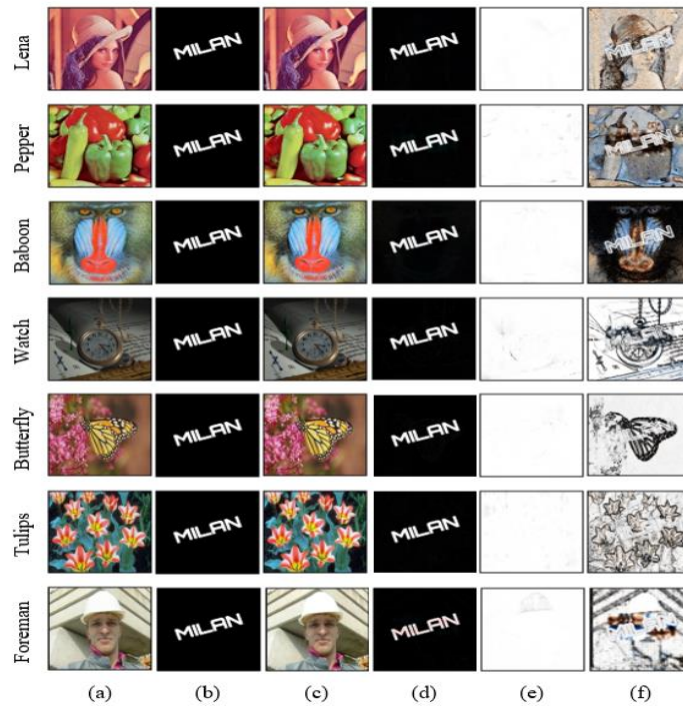

Figure 5. Watermarking images (a) cover images (b) watermark images (c) watermarked images (d) extracted watermarks (e) SSIM for cover images / watermarked images (f) SSIM for extracted watermark

Gaussian noisy attacks with variance 0.05 and 0.01 are also applied to show the attacked watermarked and extracted watermark along with the respective PSNR and NC values. Similarly, speckle attack is applied

on watermarked images with variance equals 0.05 and 0.01. Figure 6 shows the respective PSNR and NC values along with attacked watermarked and extracted watermark.

The rotation attack is a geometric attack applied by moving/rotating the image clockwise/anti-clockwise to introduce modifications. The watermarked image of Lena is attacked with different angles and evaluated in each case. The extracted watermarks with respective PSNR and NC values are shown in Table 1 and Figure 7. The resizing and cropping attacks are also geometric attacks. The resizing attack is implemented by changing the size of the watermarked image and restoring it to the same level. These attacks were implemented based on the watermarked image of Lena like other attacks. The respectively extracted watermarks along with PSNR and NC values are shown in Figure 7.

Now, different datasets having multiple video frames are tackled with various approaches. These datasets are verified/tested against already existing watermarking attacks (i.e., SVD, 2-DWT). The same datasets were applied to our proposed approach and the combination of our approach with the digital signature as shown in Figure 4.

The average PSNR values for different datasets were calculated for watermarked images / videos against each of these three approaches. Table 2 represents the result classification of PSNR values for watermarked images/videos with different approaches.

Table 1. Results with watermarked images and extracted watermarks

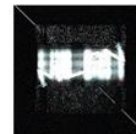| Image	Parameters	MSE	PSNR	SSIM	Mean	Variance	Entropy
Lena	WM Image	2.65	54.71	0.99	131.56	3.86E+03	7.81
	Extracted WM	3.39	53.64	0.67	14.37	2.86E+03	2.84
Pepper	WM Image	1.74	56.54	0.99	114.08	4.84E+03	7.72
	Extracted WM	4.26	52.65	0.53	15.12	2.81E+03	3.23
Baboon	WM Image	2.43	55.09	0.99	129.77	3.55E+03	7.82
	Extracted WM	3.85	53.09	0.22	18.29	2.83E+03	3.79
Watch	WM Image	1.95	60.81	0.99	75.36	2.08E+03	7.30
	Extracted WM	3.83	57.89	0.78	13.90	2.85E+03	2.36
Butterfly	WM Image	1.76	58.25	0.99	107.17	3.20E+03	7.64
	Extracted WM	2.70	56.39	0.80	14.05	2.91E+03	2.42
Tulips	WM Image	1.36	59.37	0.99	104.83	5.48E+03	7.79
	Extracted WM	2.35	56.99	0.72	14.30	2.91E+03	2.70
Foreman	WM Image	2.20	49.49	0.99	158.72	3.99E+03	7.56
	Extracted WM	10.82	39.09	0.75	12.95	2.95E+03	2.79

11

Attack	Salt & Pepper (var = 0.05)	Salt & Pepper (var = 0.01)	Gaussian (var =0.05)	Gaussian (var =0.01)	Speckle (var =0.05)	Speckle (var =0.01)
Attacked Frame	(PSNR = 50.90)	(PSNR = 52.23)	(PSNR = 52.11)	(PSNR = 53.217)	(PSNR= 48.15)	(PSNR = 51.14)
Extracted Watermark	(PSNR = 48.90) (NC = 0.73)	(PSNR = 49.44) (NC = 0.85)	(PSNR = 48.92) (NC = 0.66)	(PSNR = 52.68) (NC = 0.7)	(PSNR = 48.70) (NC = 0.85)	(PSNR = 50.44) (NC = 0.91)

Figure 6. PSNR and NC results for salt & pepper, Gaussian, and speckle attack

The existing approach has adopted a 2-level DWT transform for the watermarking process while the proposed approach has employed a slightly different way with 3-level DWT for various videos and its frames to commence the video watermarking. Table 2 shows that the results of the proposed approach are much better than the existing approaches with respect to the PSNR values based on different datasets. The overall average result of all the datasets with the proposed approach is higher than the existing approach.

Our approach is combined with the digital signature, we have calculated the average PSNR values for each dataset which has the mixed result as compared to the previous approach. Our proposed scheme outperforms the existing approach. We have applied digital signatures to achieve much security, privacy, and authenticity which may lead to little compromise based on PSNR values for a few datasets depending on the nature of videos and images.

Overall, we have witnessed that the proposed approach has performed better for video watermarking, if it is combined with digital signature which ensures more privacy, security, and authenticity as compared to the existing approaches.

Attacks	Rotate (10 degrees)	Rotate (5 degrees)	Rotate (2 degrees)	Resize (512 to 256 to 512)	Cropping
Attacked Frame	(PSNR = 49.34)	(PSNR = 52.23)	(PSNR = 53.45)	(PSNR = 48.34)	(PSNR = 45.33)
Extracted Watermark	(PSNR = 48.11) (NC = 0.68)	(PSNR = 48.50) (NC = 0.71)	(PSNR = 48.72) (NC = 0.76)	(PSNR = 51.83) (NC = 0.88)	(PSNR = 15.58) (NC = 0.43)

Figure 7. PSNR and NC results for rotation, resizing, and cropping attack

12

Table 2. Comparisons with PSNR (Watermarked images/videos)

Classes	SVD (2-DWT)	Our approaches	Our approach with digital signatures
Beach	52.1	54.15	52.83
Foreman	37.12	39.06	38.19
Multiple Scene Type	53.12	55.12	53.26
Different Times of Day	45.54	48.23	43.89
Plants and Butterfly	56.54	58.45	57.16
General Traffic	48.15	51.64	46.37
Average	48.76	51.10	48.61

CONCLUSION

In this book chapter, we have investigated and applied a little different way of watermarking process for videos by using SVD and DWT methods. As we know, most of the previously existing approaches and ways of the watermarking process are based on images only and not using digital signatures as a watermark, we have shown how the digital signatures are employed as a watermark along with the 3-level wavelet and SVD techniques. In particular, the use of Hash algorithm and digital signature as a watermark resolved the issue of achieving a high level of security, privacy, and authenticity.

For watermarking, we embed an image watermark to implement video watermarking. After tampered with various attacks, the performance of this new enhanced algorithm is evaluated through MSE, PSNR, Entropy, SSIM, etc. The proposed approaches are verified with different datasets and several attacks are implemented based on the watermarked videos/images.

The algorithmic solution of this book chapter is based on a cascading of two efficient mathematical transforms: SVD in spectrum domain and DWT in frequency domain (Ding, Yan, & Qi, 2000; Ding, Yan, & Qi, 2001; Yan & Qi, 2001; Ding, Yan, & Qi, 2002; Ian, *et al.*, 2008, Thompson, et al. 2008). The two transforms show a high degree of complementary, thus different levels of robustness are achieved by using combinations against the attacks. The use of Hash algorithm and digital signatures as a watermark took it further to attain the security and authenticity of the watermark (Bansal, Yan, & Kankanhalli, 2003; Gupta, 2021; Liu & Yan, 2014; Weir & Yan, 2011, Yan, 2019).

The approaches implemented in this book chapter can be extended further to achieve more robustness, speed, and to cover different types of images and videos in future. The use of binary images like QR codes doesn't go well with the provided approach. The binary images do not use the concept of RGB so the given approach can be taken as a base and modified or improvised further to incorporate watermarking for binary images as well.

The evaluation or benchmarking of the watermarking process was conducted based on various parameters like PSNR, MSE, SSIM, Variance, Entropy, etc in the given solution. The same can be extended to cover the evaluation on distributions which can give more accurate/close results and provide coverage over a wide range of parameters.

REFERENCES

Anjali, S., & Parul, B. (2018) Different video watermarking techniques - A review. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology,* 3(1), 1890-1894.

Antony, R., & Uma, M. (2014) Using digital signature. *International Journal of Computer Network and Security*, 6(1), 16-21.

Atrey, P., Yan, W., Chang, E., Kankanhalli, M. (2004) A hierarchical signature scheme for robust video authentication using secret sharing. International Multimedia Modelling Conference, 330-337.

Atrey, P., Yan, W., Kankanhalli, M. (2007) A scalable signature scheme for video authentication. Multimedia Tools and Applications 34 (1), 107-135.

Bansal, M., Yan, W., Kankanhalli, M. (2003) In *Proceedings of IEEE Pacific Rim Conference on Multimedia*, Volume 2, Pages 965-969.

Deepak, C., & Prachi, S. (2018) Digital video watermarking scheme using wavelets with MATLAB. *International Journal of Computer Applications*, 180(14), 30-34.

Ding, W. & Yan, W. (2000) Digital image scrambling and digital watermarking technology based on Conway's game. *Journal of North China University of Technology*, 12 (1), 1-5.

Ding, W., Yan, W., Qi, D. (2001) Digital image watermarking based on U-system. *Journal of Image and Graphics*, 6 (6), 552-557.

Ding, W., Yan, W., Qi, D. (2001) Cox's and Pitas's schemes for digital image watermarking. *Journal of Northern China University of Technology*, 12 (3), 1-12.

Ding, W., Yan, W., Qi, D. (2002) Digital image watermarking based on discrete wavelet transform. *Journal of Computer Science and Technology*, 17 (2), 129-139.

Fu, W., Yan, W., Kankanhalli, M. (2005) Progressive scrambling for MP3 audio. IEEE International Symposium on Circuits and Systems (ISCAS), 5525-5528.

Gupta, M. (2021) *Improving Security for Video Watermarking*. Master's Thesis. Auckland University of Technology, New Zealand.

Gutub, A. & Al-Shaarani, F. (2020) Efficient implementation of multi-image secret hiding based on LSB and DWT steganography comparisons. *Arabian Journal for Science and Engineering,* volume 45, pages 2631–2644.

Gutub, A., (2022) Boosting image watermarking authenticity spreading secrecy from counting-based secret-sharing. *CAAI Transactions on Intelligence Technology.*

Gutub, A. (2022) Watermarking images via counting-based secret sharing for lightweight semi-complete authentication. *International Journal of Information Security and Privacy* (IJISP) 16(1).

Gutub, A. (2022) Adopting counting-based secret-sharing for e-Video watermarking allowing fractional invalidation. *Multimedia Tools and Applications*, volume 81, pages 9527–9547

Harahap, M., & Khairina, N. (2020) Dynamic steganography least significant bit with stretch on pixels neighborhood. *Journal of Information Systems Engineering and Business Intelligence*, 6(2).

Hassan, S., & Gutub, A. (2021) Efficient image reversible data hiding technique based on interpolation optimization Fatuma. *Journal for Science and Engineering*, volume 46, pages 8441–8456.

Hassan, F., Gutub, A. (2022) Improving data hiding within colour images using hue component of HSV colour space. *CAAI Transactions on Intelligence Technology.*

Hsieh, S., Chen, C., & Shen, W. (2014) Combining digital watermarking and fingerprinting techniques to identify copyrights for color images. *The Scientific World Journal* (pp. 1-14)

Ian, T., Bouridane, A., Kurugollu, F., Yan, W. (2008) Video watermarking using complex wavelets. In *Multimedia Communication Security: Recent Advances*, pp. 197-216, NOVA publisher.

Imen, N. (2018) A novel blind and robust video watermarking technique in fast motion frames based on SVD and MR-SVD. *Hindawi Security and Communication Networks*, pp. 1-16.

Kheshaifaty, N., Gutub, A. (2021) Engineering graphical captcha and AES crypto Hash functions for secure online authentication. *Journal of Engineering Research* (JER).

Langelaar, G.C., Setyawan, I., & Lagendijk, R. (2000) Watermarking digital image and video data. *IEEE Signal Processing (Magazine)*, 17(5), 20-46.

Li´skiewicz, M., Reischuk, R., & Wölfel, U. (2017) Security levels in steganography insecurity does not imply detectability. *Theoretical Computer Science* (pp. 1-15).

Liu F., & Yan, W. (2014) *Visual cryptography for image processing and security: Theory, methods, and applications*, Springer

Mohd, W., Nasir, A., Muhammad, H., & Sahib, K. (2018) On combining MD5 for image authentication using LSB substitution in selected pixels. In *Proceedings of International Conference on Engineering and Emerging Technologies* (pp. 1-6).

Muthumanickam, S., & Arun, C. (2018) Performance analysis of 2 levels DWT-SVD based non-blind and blind video watermarking using range conversion method. *Microsystem Technologies*, 1-9.

Natarajan, M., & Govindarajan, Y. (2015) A study of DWT-SVD based multiple watermarking scheme for medical images. *International Journal of Network Security*, 17(5), 558-568.

Nurul, K., Muhammad, K., & Juanda, H. (2018) The authenticity of image using Hash MD5 and steganography least significant bit. *International Journal of Information System & Technology*, 2(1), 1-6.

Pallavi, M. (2018) Digital watermarking system for video authentication. *International Journal of Advanced Research in Computer and Communication Engineering*, pp. 1-4.

Po-Chyi, S., Chin-Song, W., Fan, C., Ching-Yu, W., & Ying-Chang, W. (2017) A practical design of digital watermarking for video streaming services. *Journal of Visual Communication and Image Representation*, 42, 161–172.

Pradhan, A., Sekhar, K., & Swain, G. (2018) Digital image steganography using LSB substitution, PVD, and EMD. *Mathematical Problems in Engineering*, pp. 1-12.

Sahib, K., Muneeza, W., Tawab, K., Nasir, A., & Muhammad, H.Z. (2018) Column level image authentication technique using hidden digital signatures. In *Proceedings of International Conference on Automation and Computing* (pp. 1-6).

Sahu, A. & Gutub, A. (2022) Improving grayscale steganography to protect personal information disclosure within hotel services. *Multimedia Tools and Applications*.

Saqer, W., & Barhoom, T. (2016) Steganography and hiding data with indicators-based LSB using a secret key. *Engineering, Technology & Applied Science Research*, 6(3), 1013-1017.

Tasheva, A., Tasheva, Z., & Nakov P. (2017) Image-based steganography using modified LSB insertion method with contrast stretching. In *Proceedings of International Conference on Computer Systems and Technologies* (pp. 151-158).

Thompson, I., Bouridane, A., Kurugollu, F., Yan, W. (2008) Video watermarking using complex wavelets. Nova Science Publishers.

Wahid, M., Ahmad, N., Zafar, M.H., & Khan, S. (2018) On combining MD5 for image authentication using LSB substitution in selected pixels. In *Proceedings of International Conference on Engineering and Emerging Technologies* (pp. 1-6).

Weir, J., Yan, W. (2011) A comprehensive study of visual cryptography. *Springer Transactions on DHMS* (LNCS 6010, pp. 70–105).

Yan, W., Qi, D. (2001) Mapping-based watermarking of 2D engineering drawings. *International Conference on CAD/Graphics*, 464 – 469.

Yan, W., Weir, J. (2010) Fundamentals of Media Security. Bookboon.

Yan, W. (2019) Introduction to Intelligent Surveillance: Surveillance Data Capture, Transmission, and Analytics. Springer London.

Yan, W., & Qi, D. (2001) Mapping-based watermarking of 2D engineering drawings. In *Proceedings of International Conference on CAD/Graphics*, 464 – 469.