A Fragile Watermarking Method for Content-Authentication of H.264-AVC Video

Mahmoud E. Farfoura[1], Osama A. Khashan[2*], Hani Omar[3], Yazn Alshamaila[4], Nader Abdel Karim[5], Hsiao-Ting Tseng[6] and Mohammad Alshinwan[7]

[1]Faculty of Information Technology, Applied Science Private University, Amman, Jordan. MEU Research Unit, Middle East University, Amman, Jordan. m_farfoura@asu.edu.jo Orcid: https://orcid.org/0000-0002-9010-6989

[2*]Research and Innovation Centers, Rabdan Academy, Abu Dhabi P.O. Box, United Arab Emirates. okhashan@ra.ac.ae, Orcid: https://orcid.org/0000-0003-1965-1869

[3]Faculty of Information Technology, Applied Science Private University, Amman, Jordan. MEU Research Unit, Middle East University, Amman. Jordan. h_omar@asu.edu.jo, Orcid: https://orcid.org/0000-0001-8253-162X

[4]King Abdullah II School of Information Technology, The University of Jordan, Amman, Jordan. y.shamaileh@ju.edu.jo, Orcid: https://orcid.org/0000-0002-4427-1465

[5]Department of Intelligent Systems, Faculty of Artificial Intelligence, Al-Balqa Applied University, Al-Salt, Jordan. Nader.salameh@bau.edu.jo, Orcid: https://orcid.org/0000-0001-8431-5218

[6]Department of Information Management, National Central University, Taoyuan, Taiwan. httseng@mgt.ncu.edu.tw, Orcid: https://orcid.org/0000-0002-8289-5236

[7]Faculty of Information Technology, Applied Science Private University, Amman, Jordan. MEU Research Unit, Middle East University, Amman, Jordan. m_shinwan@asu.edu.jo, Orcid: https://orcid.org/0000-0002-3864-7323

Journal of Internet Services and Information Security (JISIS), volume: 13, number: 2 (May), pp. 211-232. DOI: *10.58346/JISIS.2023.I2.014*

*Corresponding author: Research and Innovation Centers, Rabdan Academy, Abu Dhabi P.O. Box, United Arab Emirates.

Received: March 12, 2023; Accepted: April 15, 2023; Published: May 30, 2023

Abstract

This work proposes a blind fragile GOP-based watermarking technique that ensures the H.264-AVC video's content authenticity. In the H.264 video, the self-authentication code is created by securely hashing a number of intra prediction modes of I-frames in addition to motion vectors of P-frames and B-frames. The resulting authentication code is subsequently injected into the IPCM-Least block's Significant Bits (LSB) of some I-frames' luma and chroma pixel samples. To manage and regulate authentication data and watermark processes (embedding, detection, and verification), a key based on video footage and a secret key has been created. Intra prediction modes and motion vectors from the bitstream can be partially decoded to detect and confirm the hidden watermark data without the need for the original movie or complete video decoding. Several experiments were conducted to assess the sensitivity of the proposed method against signal processing, rate control and transcoding, conventional GOP-based and Frame-based attacks. Experimental simulations demonstrate that the implanted fragile watermark is sensitive to several low to harmful and content-preserving attacks. With only a modest bit-rate increase and hardly any perceptual quality deterioration, a large payload capacity is achieved. Experimental results show that the proposed method is suburb in term of imperceptibility, and lower effect on bit-rate. Applications like tamper-proofing, content-authentication, and covert communication are ideally suited for this technique. Based on achieved results, the devised method is capable of detecting any form of spatial and/or temporal manipulations which make it ideal for real-time applications.

Keywords: H.264-AVC; Inter-Intra forecast; IPCM; Motion Vectors; Content Authentication; Video Watermarking, Fragile Watermark.

1 Introduction

Because of the ease with which diverse digital multimedia files can be accessed, modified, and redistributed, multimedia content-authentication has evolved into a continuous and ongoing necessity for media-protection. Video authentication in a multimedia setting seeks to prove its reliability regarding time, order, and content. The integrity of digital video is guaranteed by a video authentication technique, which also confirms that the video being used hasn't been tampered with. By physically encoding a concealed code among the data, digital watermarking offers a viable means of preventing unauthorized copying and alteration of digital data (Wolfgang et al., 1999)(Krikor et al., 2009)(Baba et al., 2010)(Shkoukani et al., 2019)(Mauro Barni et al., 2005).

Recently, some video stream owners or producers have begun to express concern over video transcoding (Ahmad et al., 2005), a crucial technology for providing Internet users with ubiquitous

access to multimedia content via a range of access methods and devices. Thus, it is essential to safeguard against transcoding or to re-encode video streams. Hard authentication (Zhu et al., 2004) is a type of authentication watermark that disallows any changes to multimedia information. Any alteration to the multimedia content will cause the watermark to lose its integrity because it is so weak.

The standardization organizations such as ITU-T/MPEG and ISO/IEC MPEG establish the H.264-AVC coding standards (ISO, 2003).

It certainly has a higher compression efficiency than the MPEG-2 video standard, which is frequently cited as being up to a factor of two higher. Early methods for the watermarking video were adapted from (Horowitz et al., 2003) still picture watermarking techniques (M Barni et al., 2000)(Cappellini et al., 2001); however, they cannot be directly applied to the H.264 standard since they hide the watermark in each frame individually. A watermarking technique should be fast and included during the video encoding in real time processing. Therefore, this method meets this criterion since it will be applied directly during the video encoding process during the production time. It is not possible to apply the conventional watermarking methods straight to H.264-AVC video streams without experiencing some unanticipated issues. These methods were originally designed for the compressed bitstream of MPEG-2/4 (Dai et al., n.d.).

The H.264-AVC coding standard's copyright protection and content-authentication problems have drawn the attention of numerous researchers In this paper (Golikeri et al., 2007), an arbitrarily strong watermarking approach is proposed. This technique is resistant to compression. A non-blind vigorous watermarking scheme built on the Human Vision-Model (HVM) is suggested in (Noorkami & Mersereau, 2007). Although this solution eliminates the error pooling impact in (Wolfgang et al., 1999), it still has two drawbacks: 1) There was no way to convert the payload capacity. 2) The ability to extract any watermarks from the original video is required. In their hybrid watermarking approach, Guo et al. (Qiu et al., n.d.) combined a durable watermark implanted in the DCT range with a fragile watermarking placed in movement vectors while encoding. Their solution has security issues because it only uses diagonal parts for embedding. The resilient technique put forward in (Noorkami & Mersereau, 2007) is expanded in (Noorkami & Mersereau, 2008) to add the watermark in P-frames while considering spatiotemporal analysis to maintain visual quality.

(Proefrock et al., n.d.) suggested that the watermark be incorporated by reactivating part of the skipped macroblocks to authenticate the H.264 video. This system has various shortcomings: 1) Skipped macroblocks are 16x16 macroblocks, and embedding in them may have a noticeable effect. 2) The decoder gets the transmitted Skipped macroblocks without a header, coded coefficients, or prediction data. Reactivating them will result in a bigger bit-rate increase because more data will be transferred while active.

In order to insert a watermark, Kapotas et al. (Kapotas & Skodras, n.d.) presented an approach for fragile using the intra-IPCM-block type. The luma and chroma components' Least Significant Bits (LSB) are used for the spatial domain of the embedding. Outside of IPCM-blocks, this approach is unable to identify harmful content alteration. Kim (Kim et al., n.d.) developed a method to incorporate the bit of watermark in the trailing sign bit. By altering the optimal block is selected by Rate-Distortion Optimization, Liu et al. (Liu & Chen, 2008) incorporated watermark bits in the data (RDO). The "0" and "1" bits can be concealed by imposing different block sizes on the prediction modes. In (Hu et al., n.d.)(Yang et al., n.d.) (Abualigah et al., 2017) (Khashan et al., 2023), authors used qualified luma 4x4 blocks' intra-prediction modes to secrete informational data-based on mapping regulations and matrix coding. In essence, the approaches of (Hu et al., n.d.) and (Yang et al., n.d.) conceal the hidden data by changing the mapping rules and best intra-prediction mode for particular I.4-blocks, which may result in visual distortion. The rules, however, could have been better for each sequence because they were established from the statistical analysis of a few trial sequences. Also, it should be possible to do the watermark extraction using the mapping rules.

We describe an enhanced low-complexity content authentication approach for H.264-AVC video in order to get over the issues in (Kapotas & Skodras, n.d.)(Hu et al., n.d.)(Yang et al., n.d.). Our strategy works by GOP-based hiding a legible watermark (Mauro & Franco, 2004) in the LSB of each I-luma frame and chroma pixel samples of an IPCM-block. The intra-prediction modes of 4x4 and 16x16 I-frames and the motion vectors of macroblocks in P- and B-frames are directly used in the proposed method to extract a self-authentication code. Then, using a content-based key derived from invariant features and a secret key that is only known to the owner of the video stream, this code is hashed and encrypted. **Figure 1** shows the block diagram of the suggested technique. Watermark detection is done immediately in the compressed domain without the need for the original video.

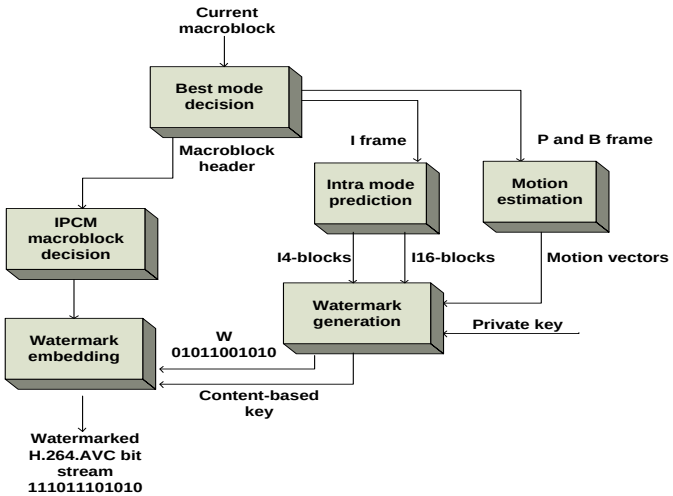


Figure 1: Block Diagram of the Proposed Method

The remainder of the study is structured as follows: Section 2 briefly summarizes the intra- and inter-prediction within the H.264-AVC encoder. The suggested watermarking approach is described in depth in Section 3, including the steps involved in generating authentication information, embedding the watermark, detecting it, and verifying it. We give experimental findings and performance analysis in Part 4, and we wrap up this report with summaries and recommendations for future research in Section 5.

2 Intra/Inter Prediction in H.264-AVC

Intra/Inter Prediction Overview

The H.264-AVC standard uses the spatial and temporal correlations of video to get intra prediction and inter prediction, respectively. During each I-frame in H.264-AVC, intra prediction is carried out on blocks of two different sizes: 16x16 (I16-block) and 4x4 (I4-block). While the I.16-block performs better when coding portions of a smooth picture, the I4-block performs better when coding regions of a picture with a lot of small details (textures). Each 4x4 sub-block is forecast using an I4-block, which is built using nearby, earlier coded, and rebuilt blocks. With the I4-block, 9 forecast methods are available, eight of which are directional (DC methods 0, 1, 3, 4,.. 8), and there is one for directionless (DCL-mode = 2).

The I16-block includes four prediction modes: the first four are directional (mode = 0, 1, 3), the third is asymmetric, and the fourth is directionless (DC-mode = 2).

Seven alternative block sizes can be assigned to a 16×16 macroblock, the same as in H.264-AVC inter prediction (or so-called modes). Three different block sizes can be used: 16×16, 16×8, and 8×16. Each 8×8 sub-macroblock leads to four additional modes: 8×8, 8×4, 4×8, and 4×4. Using a block-matching technique, each sub-macroblock in an inter-coded macroblock is predicted from an area of the same size in a reference image (Richardson, n.d.). Quarter-sample resolution is available for the luma component of the motion vector, which is the offset between the two areas. Blocks as tiny as 4×4 can broadcast individual motion vectors, while a single macroblock can transmit up to 16 motion vectors. Each motion vector is anticipated from the vectors of surrounding, previously coded partitions since motion vectors for neighboring partitions are frequently highly correlated (Richardson, n.d.). Importantly, intra/inter prediction modes and motion vectors have a delicate character, meaning that the re-encoding procedure may impact motion estimation behavior (Qiu et al., n.d.). The reader is directed to [8- 24] for additional details on motion estimation and compensation techniques.

Intra Mode Prediction Sensitivity

The H.264-AVC is a lossy compaction, implying that some data is lost in the created stream. Re-encoding a video sequence will thus result in a new sequence of video that is similar to the original video but not precisely the same. To assess the effect of re-encoding on intra prediction modes, we re-encoded

two representative video sequences (mobile, foreman) of 30 frames length; for two quantization parameters (*QP* = 28, 32). **Table 1** reported the possible cases we found; we list four cases as shown:

{Case 1}: Prediction mode changes from one 16×16 mode to a different 16×16 mode.

{Case 2}: Prediction mode changes from a 16×16 mode to a set of 4×4 modes.

{Case 3}: Prediction mode changes from a set of 4×4 modes to a 16×16 mode.

{Case 4}: Prediction mode changes from a 4×4 mode to another 4×4 mode.

Table 1: The Percentage of Intra Prediction Mode Changed Blocks (No. of Changed I.4-Blocks Over 1584 Blocks in a QCIF Frame)

Sequence	QP	{Case 1}	{Case 2}	{Case 3}	{Case 4}
foreman	28	0.03	0.10	0.11	0.20
	32	0.04	0.11	0.12	0.22
mobile	28	0.02	0.11	0.14	0.28
	32	0.03	0.15	0.18	0.31

It can be seen that {Case 4} is the dominant case with the lower *QP* (higher fidelity); we also found that the percentage of prediction mode change increased in the sub-blocks with few numbers of residuals. As a result, utilizing the intra prediction modes in designing a content-authentication scheme entails a higher fragility of watermarks.

Intra PCM (Pulse Code Modulation)

The Intra PCM (Pulse Code Modulation) mode is an alternative intra mode of coding a macroblock. It has the size of 16×16 denoted as IPCM-block, if a macroblock type is set to IPCM, then the usual prediction, transform and coding processes are bypassed, and the actual values of pixel enter the encoder remaining stages. In other words, no compression is applied for the encoded macroblock. In some non-typical images, such like noise and/or very low quantizer parameters (high fidelity), PCM may be more efficient (Richardson, n.d.). Basically, in the normal H.264 encoder, the number of the generated IPCM-blocks is very small.

Since no compression is incurred in an IPCM-block. It is a small number of IPCM-blocks in some I-frames that will be enough to carry many watermark bits. Actually, it is a tradeoff issue between the generated bit-rate and the payload of the hidden data. On the other hand, to solve the rareness problem of IPCM-blocks, a few lines of code can be added to the normal reference encoder (Reference Software, n.d.), we added the following code in the procedure "encode_one_macroblock_high" just before calling the function ‘‘compute_mode_RD_cost’’:

1. ***if*** *(image -> mb_nr == N && image -> type == I_SLICE)*
2. ***for*** *(j = 0; j < 14; j++)*
3. *enc_mb.valid[j] = 0;*
4. ***end for;***

5. ***end if;***

The encoder will be forced by this code to encode the Nth macro-block of all I-frames in IPCM intra mode.

So far, we conclude that a content-authentication scheme utilizing intra prediction modes, motion vectors and IPCM-blocks can be a useful scheme encompasses high fragility to detect any attempt to re-encode or manipulate the contents of watermarked bitstream. More details in the following sections about the proposed approach.

3 The Suggested Watermarking Approach

In the suggested method, the authentication information, which consists of the motion vectors of both P and B frames and the encrypted and hashed intra-prediction forms of I4-block and I16-block of I-frames, is embedded in some I-frames' Least Significant Bits (LSB) of both the luma and chroma pixel samples of the IPCM-block in a GOP-based manner. The luma and chroma pixels are pseudo-randomly selected for embedding based on the content-based generated public key. Intra and inter-frames are safeguarded as a result. I-frames, in particular, are chosen for watermark embedding because they are essential to every H.264-AVC stream. Any tampering with them would immediately affect the subsequent P- and B-frame's perceptual quality, making it obvious that tampering had occurred. Any inaccuracy in I-frames may affect other frames since they serve as the reference frames for inter-predicting P- and B-frames.

A content-based public key (K) is produced from pseudo-randomly selected sixteen intra-prediction modes of sixteen I4-blocks for a particular macroblock in the frame in order to prevent the intra-collusion attack (Furht & Marques, 2003) that occurs when the same key is used for watermark embedding in all frames. The private key (S) is then used to scramble the public key to create the final key, which is subsequently used in: 1) Producing the authentication data. 2) Deciding which pixel samples to use for embedding.

The processes for creating and authenticating information, embedding watermarks, and finally detecting and demonstrating watermarks are expressed in the following sections.

Authentication Information Generation Process

We process each GOP separately in order to authenticate it in the H.264-AVC data flow, allowing us to identify the attacked sequences individually. Consequently, every GOP contains an encrypted hash value. The GOP-based strategy is shown in **Figure 2**. There are two order sequences introduced by the GOP-based authentication mechanism. The watermarked sequence's GOP order sequence is represented by a GOP order sequence (GOS), and the current frame order is represented by a frame order sequence (FOS). Any GOP-based attacks must be detected by the GOS, whereas the FOS must detect any frame-based assaults. The I4-block and I16-block forecast modes (IV), motion vectors (MV), frame ordering

sequence (FOS), and GOP order sequence (GOS) are the inputs to SHA-256 which is a one-way hash cryptographic method (Schneier et al., 1996). Using the content-based key (K), the FOS, MV, IV, and GOS are hashed and encrypted. Equation (1) represents the watermark generation process.

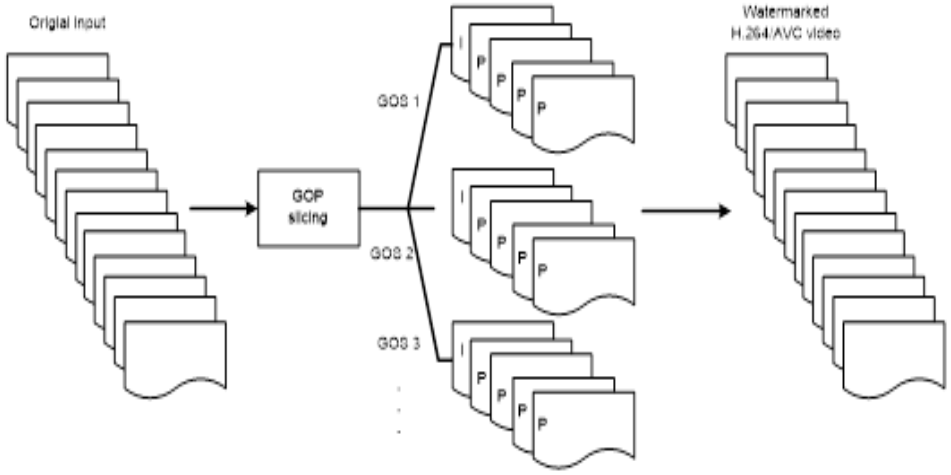


Figure 2: GOP-Based Authentication Approach

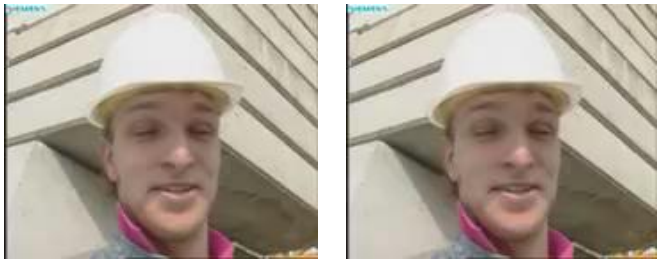
$$W = E(H(IV, MV, FOS, GOS), K) \quad (1)$$

where E(•) is an encryption function which scrambles its inputs based on the value of K.

Watermark Embedding Process

Spread Spectrum (Cox et al., n.d.), Least Significant Bits (Gonzalez et al., n.d.), and Quantization Index Modulation (Chen & Wornell, n.d.) are only a few of the embedding techniques that can be found in the literature. Robust watermarking approaches are typically supported by spread spectrum watermarking and quantization index modulation techniques (Laouamer, L., 2020). As a result, LSB modulation techniques are a better option when it comes to authentication methods. Because they require less computing effort, we may adapt them to embed the watermark payload.

The secret authentication information created from the previous section and encoded as a binary sequence with the notation $S = \{w_i \mid i = 0,1, \ldots, L, s_i \in \{0,1\}\}$ makes up the watermark payload, where L is the length of watermark. The conical payload is the generated IPCM-block pixel samples in some I-frames in every GOP. Gonzalez (Gonzalez et al., n.d.) claimed that up to 3 low bits of an 8-bit pixel data sample is altered without any scarification of perceptual quality. Therefore, we applied our embedding technique to a standard representative video sequence *foreman*, so we embed a total of 6 bits, 3 bits in the luma samples and another three bits in the chroma samples into LSB's of 98th macroblock of 1st frame of *foreman*. **Figure 3** illustrate that the degradation is unnoticeable in the visual quality of the watermarked frame.



(a) (b)

Figure 3: Visual Comparison of (a) Original and (b) Watermarked 1st Frame of Foreman (QCIF)

We modulated the LSB's of the luma and chroma samples of IPCM-blocks generated in some I-frames in the modified encoder using the normal odd-even parity in accordance with the generated binary sequence *S*. The number of changes to the LSBs used for embedding the watermark is limited to one. 50% of the embedded bits will not have an impact on the sample pixel if the watermark data *S* and the selection pixels are allocated evenly. As a result, the distortion is minimal and has no impact on the perception of the watermarked frame.

Watermark Detection and Verification Process

The H.264-AVC stream owner can use the watermark detection and verification method to confirm the legitimacy of the watermarked stream if he/she believes that the integrity of the video stream has been purposefully altered or tampered for any reason. The watermark detection block diagram and verification procedure are shown in **Figure 4**. Entropy decoding is followed by watermark detection. Similar to how the watermark embedding works, the detection procedure uses a GOP-based strategy but in the opposite direction.

The watermark detection process iterates through each GOP. Every GOP is first partially decoded to build its frame types and structures, such as the IPCM-block if the frame being decoded is an I-frame, the I4-block and I16-block prediction modes, or alternatively the motion vectors if the current decoded frame is a P- or B-frame. Therefore, after regenerating the content-based key (K), for the GOP of interest, we can build the hashed and encrypted watermark W by invoking the authentication information creation process. After that, create the extracted watermark information W' by identifying the embedded watermark from the LSBs of the IPCM-block pixel samples. The present GOP is confirmed if the watermarks W, which was generated, and W', which was discovered, are similar. The watermarked H.264-AVC stream is certified and validated by repeating the previous operation and comparing all of the retrieved watermarks.

The fact that the motion vectors and intra prediction modes may be used to detect the hidden authentication information proves that the detection method is straightforward and quick.

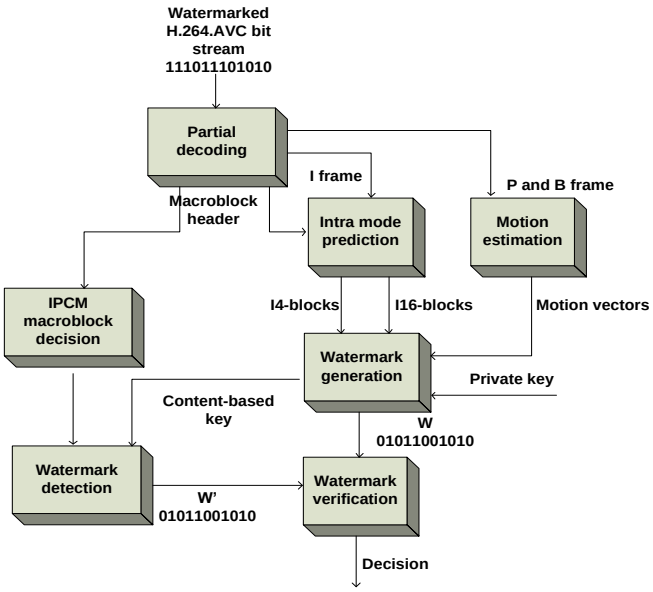


Figure 4: Block Diagram of Watermark Detection and Verification Process

4 Experimental Results and Discussions

This work successfully matched the contradictory requirements for watermarking, including indistinguishable, bit-rate management, and ideal payload capability, where a more increased payload capability means a worse visual quality and a higher bit-rate. This section contains the experimental findings that demonstrate the increased payload capacity with the least amount of compromise in visual quality and bit rate. The H.264-AVC JM14.0 of the reference program was updated to include the proposed watermarking technique (Reference Software, n.d.). **Table 2** lists the reference software's most crucial configuration settings. The other encoder parameters are left at their default values. To demonstrate the viability of the suggested approach, seventeen standard video sequences (*akiyo, stefan, grandma, mother-daughter, coast-guard, silent, bridge-close, news, carphone, container, claire, foreman, salesman, soccer, table, tempete* and *mobile*), all in QCIF (176 × 144) @7.5Hz were tested. The chosen video clips show motions with low to medium intensity and ranges from low to high spatial resolution.

Table 2: Configuration Parameters of the H.264-AVC Encoder

Profile	**Main**
Number of frames	300 (10s)
Frame rate	30fps
RD optimization	High-complexity mode
Motion estimation	Simplified UM-Hexagon-S
Group of pictures (GOP)	IBPBPBPBPBI
Entropy encoding	CABAC

For purposes of comparison with earlier works, we used the variation on bit-rate (VAR_{RATE}) and variation on *PSNR* (VAR_{PSNR}) defined in equation 2 and 3.

$$VAR_{RATE} = \frac{R\prime - R}{R} \times 100\ \%(2)$$

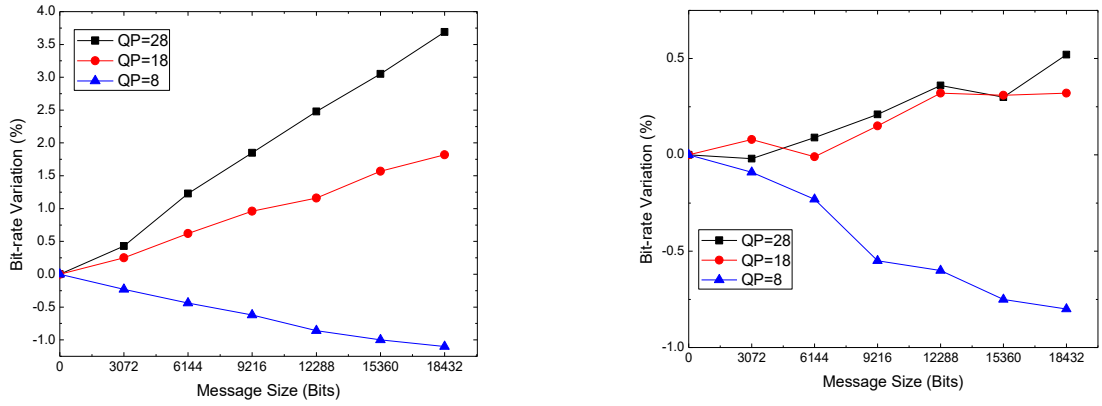
where R' is the bit-rate generated from the modified encoder and R is the bit-rate generated from the original encoder.

$$VAR_{PSNR} = \frac{(PSNR\prime_X + PSNR\prime_Y + PSNR\prime_Z) - (PSNR_X + PSNR_Y + PSNR_Z)}{3}(3)$$

where $PSNR'_X$ is the total *PSNR* of the luma (X) samples in all frames, and $PSNR'_Y$ and $PSNR'_Z$ are the total *PSNR* of the chroma (Y, Z) samples are generated from the encoder after modification, while $PSNR_X$ is the total *PSNR* of the luma (X) samples in all frames, and $PSNR_Y$ and $PSNR_Z$ are the total *PSNR* of the chroma (Y, Z) samples are generated from the original encoder.

Bit-Rate and Capacity Test

In general, the effect of introducing some IPCM-blocks on bit-rate can be minimized by allowing only few macroblocks to be generated during the encoding process with respect to the desired payload capacity. In other words, it is a tradeoff issue between the generated bit-rate and the payload capacity. We have reported some experiments to show the effect of the bit-rate expansion with respect to the payload capacity. The first set of experiments was done to show the effect of generating the IPCM-blocks with respect to the hidden message size. We ran the encoder with three common values of QP (28, 18, and 8) and for different message payloads per video sequence. Fig. 5 depicts the output of this experiment.



(a) (b)

Figure 5: Bit-Rate Variation Verses Message Size for Different QP Values for (a) Container and (b) Mobile Sequences

As can be seen, the higher *QP* value such as 28, with higher message size, has a higher bit-rate variation. For *QP* equal to 8, have another trend, where the higher message size, the lower bit-rate variation. When low *QP* is used, i.e. high-fidelity video is desired, IPCM-blocks will be more attractive than the other types of macroblocks.

As in (Kapotas & Skodras, n.d.), the payload capacity for the proposed method can be calculated based on equation 4.

$$\text{Total payload capacity} = N\_ipicture \times (\text{Luma capacity} + 2 \times \text{Chroma capacity}) \quad (4)$$

where *N_ipicture* is the number of intra coded pictures in the video stream and

$$\text{Luma capacity} = 16 \times 16 \times N_{IPCM} \times L_{bits}, \text{ and}$$

$$\text{Chroma capacity} = 8 \times 8 \times N_{IPCM} \times C_{bits},$$

where N_{IPCM} is the number of IPCM-blocks per intra coded picture, L_{bits} is the number of low bits per IPCM luma sample used for watermark embedding, and C_{bits} is the number of low bits per IPCM chroma sample used for watermark embedding.

Imperceptibility Test

A series of experiments have been carried out to assess the imperceptibility of the proposed approach. Returning to Figure 3, which shows an intra coded frame of the original and watermarked foreman sequence, we can see that there is little to no subjective difference in visual quality between the two frames. Figure 6 illustrates the connection between the message size and the PSNR change in terms of objective evaluation. We observe that, the higher payload, the lower PSNR obtained. However, this experiment shows when QP is equal to 8, the PSNR degradation is no greater than -0.1.

Table 3 displays the variation of bit rate (VAR_{RATE}), variation of *PSNR* (VAR_{PSNR}), and variation of QP for various video sequences with message size = 18432 and various values of QP (28, 18 and 8).

Table 3: Bit-Rate and PSNR Variation for Different QP Values with Message Size = 18432

Video sequence	VAR_{RATE} (%)			VAR_{PSNR} (dB)		
	QP = 28	***QP = 18***	***QP = 8***	***QP = 28***	***QP = 18***	***QP = 8***
akiyo	3.12	2.60	1.08	- 0.02	-0.1	-0.24
stefan	0.69	0.49	-4.04	-0.01	-0.05	-0.13
mother-daughter	3.42	1.93	0.78	-0.04	-0.11	-0.29
coast-guard	1.59	0.73	-2.25	-0.06	-0.14	-0.29

Based on bit-rate variation (VAR_{RATE}) and PSNR variation (VAR_{PSNR}), performance evaluations of the approaches in (Kapotas & Skodras, n.d.) and (Hu et al., n.d.)have been done. We used four 199-frame-long QCIF videos (*bridge-close*, *granny*, *news*, and *silent*). Using the H.264 Main profile setup (RDO = On, Entropy encoding = CABAC, QP = 28, and 30 fps), the tests were conducted.

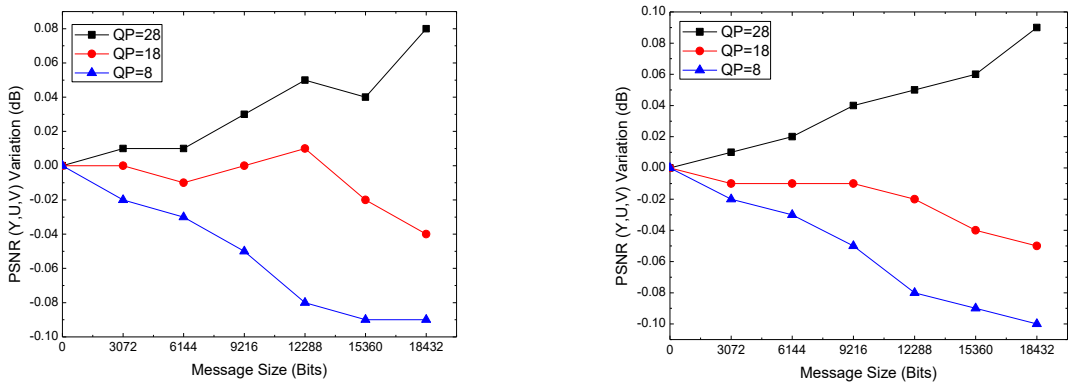


Figure 6: PSNR Variation (VARPSNR) Verses Message Size for Different QP Values for (a) Container and (b) Mobile Sequences

Table 4: Performance Comparison with the Methods in (Kapotas & Skodras, n.d.) and (Hu et al., n.d.)

Video sequence	**Maximum payload Cp (bits)**			**VARRATE (%)**			**VARPSNR (dB)**		
	Proposed method	**Method in** (Kapotas & Skodras, n.d.)	**Method in** (Hu et al., n.d.)	**Proposed method**	**Method in** (Kapotas & Skodras, n.d.)	**Method in** (Hu et al., n.d.)	**Proposed method**	**Method in** (Kapotas & Skodras, n.d.)	**Method in** (Hu et al., n.d.)
grandma	18432	15360	12352	3.01	2.93	3.72	-0.02	-0.01	-0.08
silent	18432	18432	17368	3.38	3.59	4.14	-0.01	0.02	-0.04
bridge-close	18432	15360	11748	2.0	1.15	2.90	-0.02	0.01	-0.04
news	18432	18432	9972	3.21	3.80	3.23	-0.01	-0.01	-0.01
(Average)	**18432**	**16896**	**12860**	**2.9**	**2.87**	**13.99**	**-0.015**	**0.003**	**-0.043**

Table 4 presented the performance comparison results with the method of (Kapotas & Skodras, n.d.) and (Hu et al., n.d.). The results show that the proposed method has achieved a higher hiding capacity. For the variation of bit-rate (VAR_{RATE}), our method outperforms method (Hu et al., n.d.) and very close to method (Kapotas & Skodras, n.d.). Regarding the variation of *PSNR* (VAR_{PSNR}) compared to (Kapotas & Skodras, n.d.) and (Hu et al., n.d.), our method is superior.

There has been an additional comparison with the DCT-based approaches (Wolfgang et al., 1999), (Noorkami & Mersereau, 2007), and (Noorkami & Mersereau, 2008). We utilize the watermark cost (δ), defined in (Noorkami & Mersereau, 2008) as the increase in the number of bits necessary to encode the watermarked video per watermark bit, in order to ensure a fair comparison because the bit-rate depends on the embedded capacity:

$$\delta = \frac{R' - R}{Cp} \quad (5)$$

where *Cp* is the payload capacity. To evaluate the performance of the proposed method, eight QCIF videos were used. The tests were performed using the H.264 Main profile configuration (*RDO* = On, Entropy encoding = CABAC, *QP* = 28, frame rate 30 fps, and GOP structure "IBPBPBI"). **Table 5** shows the comparison of the watermark cost δ of different video sequences in the proposed watermarking method with the methods presented in (Wolfgang et al., 1999), (Noorkami & Mersereau, 2007), and (Noorkami & Mersereau, 2008). We can see that our proposed method is superior in terms of δ. Our results show that the proposed watermarking method can prevent the bit-rate increase for all of the used video sequences.

Table 5. Comparison of the δ of the Proposed Watermarking Method with Method (Wolfgang et al., 1999), (Noorkami & Mersereau, 2007) and (Noorkami & Mersereau, 2008) when Watermark is Embedded in I-Frames

Video sequence	**Number of frames**	**Watermark cost (δ)**			
		Method in (Wolfgang et al., 1999)	**Method in** (Noorkami & Mersereau, 2007)	**Method in** (Noorkami & Mersereau, 2008)	**Proposed approach**
carphone	150	2.75E+00	2.76E+00	1.54E+00	3.80×10-4
claire	200	4.53E+00	4.77E+00	2.41E+00	3.49×10-4
mobile	100	2.15E+00	2.33E+00	1.06E+00	4.64×10-4
mother	100	4.01E+00	3.87E+00	2.48E+00	5.74×10-4
salesman	150	1.95E+00	1.92E+00	1.10E+00	3.54×10-4
soccer	60	2.54E+00	2.50E+00	1.58E+00	1.02×10-3
table	100	1.60E+00	1.90E+00	8.20E-01	5.75×10-4
tempete	60	2.29E+00	2.08E+00	1.35E+00	7.58×10-4
(Average)	--	**2.72**	**2.76**	**1.54**	**5.59×10-4**

The VQM (Video Quality Measure) (National, n.d.) is also used because PSNR and other image quality metrics do not take into account the temporal activity of the encoded streams. The VQM falls between zero and one, where one denotes the greatest impairment and zero denotes the absence of any distortions. Our proposed method was put up against those in (Wolfgang et al., 1999), (Noorkami & Mersereau, 2007), and (Noorkami & Mersereau, 2008) using VQM. The VQM for various techniques when only I-frames are watermarked is shown in

Table 6. As the obtained average VQM of the suggested technique is around 3 times lower than the other techniques, it is obvious that our method beats them. This indicates that our solution preserves the watermarked video streams' perceived quality.

Table 6: When a Watermark is Placed in an I-Frame, VQM for the Suggested Method of Watermarking as well as the Procedures in (Wolfgang et al., 1999), (Noorkami & Mersereau, 2007), and (Noorkami & Mersereau, 2008)

Video sequence	**Number of frames**	***VQM***			
		Method in (Wolfgang et al., 1999)	**Method in** (Noorkami & Mersereau, 2007)	**Method in** (Noorkami & Mersereau, 2008)	**Proposed approach**
carphone	150	1E-01	1E-01	1E-01	3E-02
claire	200	1E-01	1E-01	1E-01	2E-02
mobile	100	5E-02	5E-02	6E-02	2E-02
mother	100	2E-01	2E-01	1E-01	3E-02
salesman	150	1E-01	1E-01	2E-01	3E-02
soccer	60	8E-02	8E-02	9E-02	3E-02
table	100	2E-01	2E-01	2E-01	4E-02
tempete	60	8E-02	7E-02	8E-02	2E-02
(Average)	**--**	**1E-01**	**1E-01**	**1E-01**	**3E-02**

Fragility Test

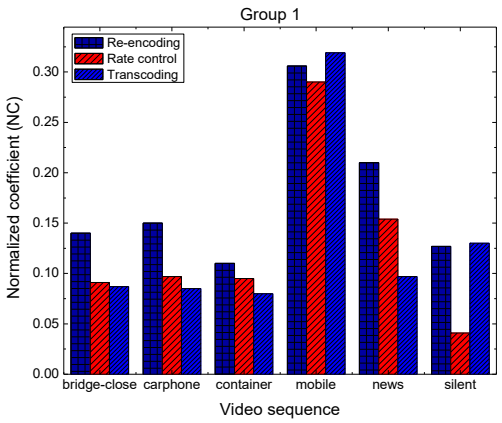
This paper's goal, as stated previously, is to suggest a hard authentication mechanism that can identify both purposeful and unintentional attacks. An attacker would ideally try to target the watermarked videotape streamlet in a fragile watermarking such that the watermark is completely removed while, at the same time, there is no obvious quality reduction in the video. The watermarked streams of [foreman, bridge-close, carphone, container, mobile, and silent] video sequences were submitted to three groups of simulated attacks in order to assess the vulnerability of the proposed approach against such attacks. Group 1: Attacks that focus on content preservation include transcoding, rate control, and re-encoding. Group 2: This category consists of common signal processing attacks such as cropping, median filtering, rotation attacks, and gaussian blurring. Category 3 includes conventional GOP-based and Frame-based assaults. Although the simulated attacks from Groups 1, 2, and 3 are, respectively, weak, medium, and strong.

Table 7 displays how the vulnerable watermark performed during the simulated assaults for the sequence including the assaulted foreman. We can see from the identified watermarks following the simulated attacks that the suggested method is extremely sensitive to both modest pixel changes and powerful attacks. As a result, the technique effectively authenticates the consistency of watermarked H.264 streams.

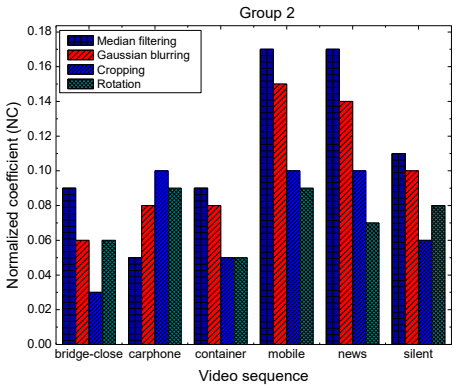
Table 7: Fragility Against three Groups of Attacks for the Watermarked Foreman in the Proposed Method

Group No.	**Type of Attack**	***NC***	***VAR*$_{PSNR}$ (dB)**
G.1	Re-encoding	0.33	0.02
	Rate-control	0.12	-0.14
	Transcoding (QP = 32)	0.11	-3.45
G.2	Median filtering (3 × 3)	0.04	-4.51
	Gaussian blurring (2.5 × 2.5)	0.06	-4.60

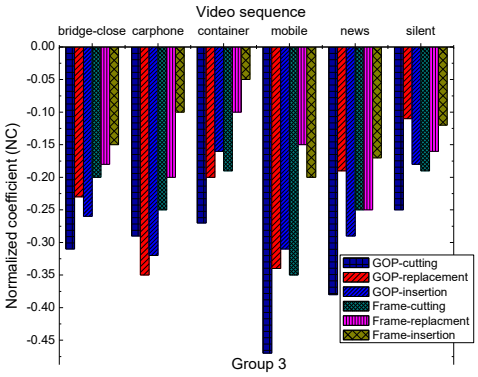
	Cropping (170 ×140)	0.03	-3.16
	Rotation (1°)	0.01	-3.42
G.3	GOP-cutting (GOP No. = 3, 5, 8)	-0.33	-6.41
	GOP-replacement (GOP No. 4 with 5)	-0.28	-6.88
	GOP-insertion (GOP No. = 2, 5)	-0.31	-4.64
	Frame-cutting (GOP. No. 1 [2 to 9], GOP No. 2 [11 to 13], GOP No. 5 [51 to 55])	-0.46	-6.52
	Frame-replacement (Frame No. 10 with 11)	-0.15	-3.57
	Frame-insertion (Frame No. = 21, 32, 55)	-0.13	-2.96



(a)



(b)



(c)

Figure 7: Fragility Against Thirteen Common Video Attacks

The Normalized Correlation Coefficient (NC) for the video sequences [*bridge-close*, *carphone*, *container*, *mobile*, *news*, and *silence*] under the aforementioned attacks is displayed in **Figure 7**. As can be observed, the detected (NC) values were extremely low, demonstrating the proposed approach's strong sensitivity to the thirteen simulated attacks. The achieved results proofs effectiveness of the proposed scheme to validate the authenticity of any H.264-AVC stream that has a watermark.

The IPCM-block, motion vectors, intra-prediction modes, and the content-based key (K), which causes the embedded watermark to collapse under any manipulations, were all used to boost the effectiveness of the suggested method. We conclude that the suggested method is capable of detecting any form of spatial or temporal manipulations based on the findings shown in **Table 7** and **Figure 7**.

Complexity Test

For the H.264-AVC codec, the intra prediction process typically takes little time and costs less than 10% of the computational load (Peter et al., n.d.). The present encoder would not have any additional overhead if a strategy that takes advantage of the intra/inter prediction modes already chosen by the Rate-Distortion Optimization (RDO) process were used. The suggested method has a low computational complexity because the main activities, including the synthesis of authentication information, embedding of the watermark, and finally detection and verification of the watermark, are all constituted of straightforward basic mathematical operations. Our tests revealed that the suggested strategy did not significantly slow down the aforementioned operations. In contrast, there is hardly any delay in the embedding and detection of the watermark.

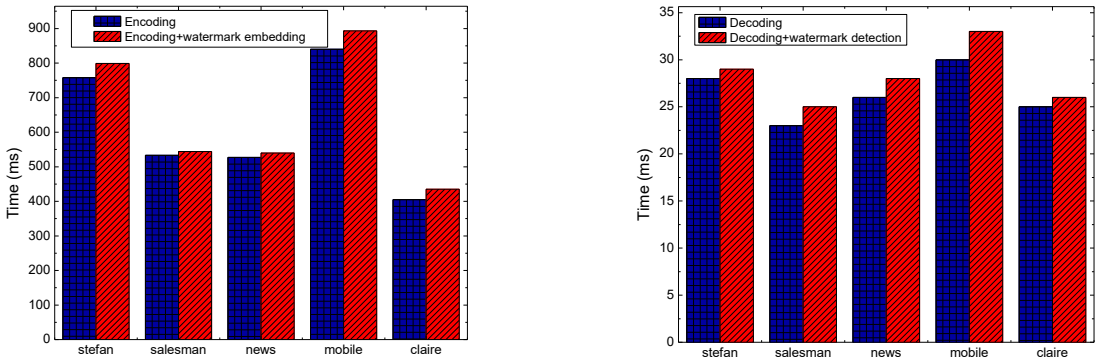


Figure 8: Comparison of Time Overhead for Watermark Embedding and Watermark Detection and Verification

Figure. 8 illustrates the average delays in milliseconds (ms) incurred by the watermark embedding and detection and verification (300 frames). As it is seen, the maximum overhead cost found in the watermark embedding process is no more than (53 ms) in the case of mobile sequence. Similarly, the maximum overhead cost observed in the watermark detection and verification process is no more than (3 ms) in the case of mobile sequence, which almost negligible. Therefore, we conclude that the proposed method can be applied practically in watermarking H.264 streams in real-time.

5 Conclusions

This paper proposed a blind GOP-based fragile watermarking and low intricacy, approach for authenticating H.264-AVC video. The shortcomings of the preceding watermarking methods were examined and rectified. The three main H.264-AVC components that are utilized in this method are motion vectors, IPCM-blocks, and intra-mode prediction.

There is no additional overhead because the watermark's embedding occurs during the information compression process. The intra-prediction modes of I.4-blocks and I.16-blocks, along with the motion vectors, make up the features of the self-authentication data after they have been permuted, hashed, zigzag ordered, and encrypted with a content-based key. The secret information is subsequently included in the luma and chroma samples of each intra-predicted I-frame and GOP in the resulting IPCM-block in the H.264-AVC stream. Without needing the original video stream, concealed data can be found by partly decoding the watermarked H.264 stream.

Results from experiments on some examples of video sequences demonstrate that the approach has a heightened payload capability while having no impact on coding effectiveness or perceptual quality. The proposed system can reportedly identify spatial and material manipulation because the simulated fragility tests show remarkable sensitivity to purposeful and inadvertent attacks. Our ongoing research will focus on creating a new, reliable system that uses the latest H.264-AVC standard features.

Author Contributions: Conceptualization, Mahmoud E. Farfoura, and Hani Omar; methodology, Mahmoud E. Farfoura and Mohammad Alshinwan; validation, Yazn Alshamaila, Nader Abdel Karim; , and Osama A. Khashan; formal analysis, Mahmoud E. Farfoura and Hsiao-Ting Tseng; writing—original Mahmoud E. Farfoura, Mohammad Alshinwan, and Hani Omar; writing—review and editing, Yazn Alshamaila, Osama A. Khashan, Nader Abdel Karim, and Hsiao-Ting Tseng. All authors have read and agreed to the published version of the manuscript.

Funding: N/A.

Declarations

Ethical Approval and Consent to Participate

The research in this paper does not involve animal experiments and does not harm humans and the environment.

Competing for Interests

The authors declare no competing interests.

References

[1] Abualigah, L.M., Khader, A.T., Al-Betar, M.A., & Alomari, O.A. (2017). Text feature selection with a robust weight scheme and dynamic dimension reduction to text document clustering. *Expert Systems with Applications*, *84*, 24–36.

[2] Ahmad, I., Wei, X., Sun, Y., & Zhang, Y.-Q. (2005). Video transcoding: an overview of various techniques and research issues. *IEEE Transactions on Multimedia*, *7*(5), 793–804.

[3] Baba, S.E.I., Krikor, L.Z., Arif, T., & Shaaban, Z. (2010). Watermarking of digital images in frequency domain. *International Journal of Automation and Computing*, *7*, 17–22.

[4] Barni, M, Bartolini, F., Caldelli, R., Rosa, A. De, & Piva, A. (2000). A Robust Watermarking Approach for Raw Video. *Proceedings*, *10*, 1–2.

[5] Barni, Mauro, Bartolini, F., & Checcacci, N. (2005). Watermarking of MPEG-4 video objects. *IEEE Transactions on Multimedia*, *7*(1), 23–32.

[6] Cappellini, V., F. Bartolini R. Caldelli, A.D.R.A.P., & Bami, A. (2001). Robust frame-based watermarking for digital video. *Proceedings*, *12*.

[7] Chen, B., & Wornell, G.W. (n.d.). (2001). Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding. *IEEE Transaction on Information Theory*, *47*(4), 1423-1443.

[8] Cox, I., Kilian, J., Leighton, F.T., & Shamoon, T. (n.d.). (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, *6*(12), 1673-1687.

[9] Dai, Y.W., Wang, Z.Q., Ye, D.P., & Zou, C. F. (n.d.). (2007). A new adaptive watermarking for real-time MPEG videos. *Applied Mathematics and Computation*, *2*(185), 907--918.

[10] Furht, B., & Marques, O. (2003). *Handbook of Video Databases: Design and Applications*. CRC Press.

[11] Golikeri, A., Nasiopoulos, P., & Wang, Z.J. (2007). Robust digital video watermarking scheme for H.264 advanced video coding standard. *Journal of Electronic Imaging*, *16*, 4.

[12] Gonzalez, R.C., Woods, R.E., & Processing, D.I. (n.d.). (2008). *3rd Edn., Prentice-Hall, Englewood Cliffs*.

[13] Horowitz, M., Joch, A., Kossentini, F., & Hallapuro, A. (2003). H. 264/AVC baseline profile decoder complexity analysis. *IEEE Transactions on Circuits and Systems for Video Technology*, *13*(7), 704–716.

[14] Hu, Y., Zhang, C.T., & Su, Y.T. (n.d.). (2007). Information hiding based on intra prediction modes for H.264-AVC. *IEEE International Conference on Multimedia and Expo (ICME 2007), Beijing, China, 1231--1234*.

[15] ISO, I.T. (2003). *IEC 14496-10 ITU-T Rec. H. 264,"Advanced video coding," ISO*.

[16] Kapotas, S.K., & Skodras, A.N. (n.d.). (2009). Real time data hiding by exploiting the IPCM macroblocks in H.264-AVC streams. *Journal of Real-Time Image Processing, 4(1), 33--41*.

[17] Khashan, O.A., Khafajah, N.M., Alomoush, W., Alshinwan, M., Alamri, S., Atawneh, S., & Alsmadi, M.K. (2023). Dynamic Multimedia Encryption Using a Parallel File System Based on Multi-Core Processors. *Cryptography*, *7*(1), 1-17.

[18] Kim, S.M., Kim, S.B., Hong, Y., & Won, C.S. (n.d.). (2007). Data hiding on H.264-AVC compressed video. *International Conference on Image Analysis and Recognition (ICIAR 2007), Montreal, Canada, LNCS, 4633, 698--707*.

[19] Krikor, L., Baba, S., Arif, T., & Shaaban, Z. (2009). Image encryption using DCT and stream cipher. *European Journal of Scientific Research*, *32*(1), 47–57.

[20] Liu, C.H., & Chen, O.T.C. (2008). Data hiding in inter and intra prediction modes of H.264-AVC. In I. International (Ed.), *Symposium on Circuits and Systems (ISCAS 2008), Seattle*, 3025–3028. Washington.

[21] Laouamer, L., Euchi, J., Zidi, S., & Mihoub, A. (2020). Image-to-Tree to Select Significant Blocks for Image Watermarking. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 11*(1), 81-115.

[22] Mauro, B., & Franco, B. (2004). *Watermarking Systems Engineering (Signal Processing and Communications, 21)*. CRC Press, Inc.

[23] National, A. (n.d.). (2003). *Standard for Telecommunications-Digital Transport of One-Way Video Signals-Parameters for Objective Performance Assessment, Standard*.

[24] Noorkami, M., & Mersereau, R.M. (2007). A framework for robust watermarking of H.264-encoded video with controllable detection performance. *IEEE Transaction on Information*, *2*(1), 14–23.

[25] Noorkami, M., & Mersereau, R.M. (2008). Digital video watermarking in P-frames with controlled video bit-rate increase. *IEEE Transaction on Information*, *3*(3), 441–455.

[26] Peter, L., Detlev, M., Matthias, N., Fernando, P., Thomas, S., & Thomas, W. (n.d.). (2004). Video coding with H.264-AVC: tools, performance, and complexity. *IEEE Circuits and Systems Magazine, 3*, 7- 28.

[27] Proefrock, D., Richter, H., Schlauweg, M., & Mueller, E. (n.d.). (2005). H.264-AVC video authentication using skipped macroblocks for an erasable watermark. *Proceedings of SPIE, 5960*, 1480-1489.

[28] Qiu, G., Marziliano, P., Ho, A.T.S., He, D., & Sun, Q. (n.d.). (2006). A hybrid watermarking scheme for H.264-AVC video. *Proceedings of the 17th Inter-national Conference on Pattern Recognition (ICPR 2004), 4*, 2353--2356.

[29] Reference Software, J.M. (n.d.). J. *V.T.*, *Version*, *14*.

[30] Richardson, I.E. (n.d.). *H.264 and MPEG-4 Video Compression, Wiley*. *2004*.

[31] Schneier, B., Cryptography, A., Wiley, J., & York, N. (1996). *No Title*.

[32] Shkoukani, M., Altamimi, A.M., & Qattous, H. (2019). An Experimental Study to Evaluate the Integration of Various Security Approaches to Secure Transferable Data. *International Journal of Simulation--Systems, Science \& Technology*, *20*(1).

[33] Wolfgang, R.B., Podilchuk, C.I., & Delp, E.J. (1999). Perceptual watermarks for digital images and video. *Proceedings of the IEEE*, *87*(7), 1108–1126.

[34] Yang, G., Li, J., He, Y., & Kang, Z. (n.d.). (2010). An information hiding algorithm based on intra-prediction modes and matrix coding for H.264-AVC video stream. *International Journal*

of Electronics and Communications.

[35] Zhu, B.B., Swanson, M.D., & Tewfik, A.H. (2004). When seeing isn't believing [multimedia authentication technologies]. *IEEE Signal Processing Magazine, 21*(2), 40–49.

Authors' Biography

Dr. Mahmoud Farfoura, an enthusiastic PhD holder and dedicated professional with practical experience across various areas of Software Engineering, Information Security and Data Science for more than 23 years in well-known local organization in Jordan. Dr. Farfoura led many IT and software development projects for local clients in Jordan. Currently, he is an Assistant Professor at Applied science private university, in Jordan. His research interests in Information Security, Artificial Intelligence, and Machine learning

Osama Ahmed Khashan received his PhD in computer science from the National University of Malaysia, Malaysia in 2014, and his MSc in information technology from Utara University Malaysia, Malaysia in 2008. With a diverse academic background, he has hold positions at several universities in Saudi Arabia and Malaysia. Currently, he is working as Associate Professor/Associate Researcher at the Research and Innovation Centers, Rabdan Academy, Abu Dhabi, United Arab Emirates. His research interests include information security, cyber security, cryptography, Blockchain technology, cloud computing, and image processing.

Yazan Alshamaileh is an Associate Professor, imparts his knowledge at the prestigious King Abdullah II School for Information Technology, situated within the esteemed University of Jordan. His academic background encompasses a BSc in Computer Information Systems from Mu'tah University in Jordan, an MSc in Business Information Technology from Northumbria University in England, and a Ph.D. in e-Business from the University of Newcastle in the UK.

Dr. Hani Omar born in Kuwait 1978 and raised in Kuwait and Jordan. He got his B.Sc. in Computer Science from Mutah University- Jordan in 2001, and M.Sc. in Computer Science-Jordan in 2008. While pursuing his M.Sc., he was working in University of Jordan as instructor (2003-2008). He had got his Ph.D. in Information Management from National Chiao Tung University in 2015.

Dr. Nader Abdel Karim is an accomplished professional in the fields of user authentication, cybersecurity, Human-Computer Interaction (HCI), and E-learning. He obtained his Ph.D. in 2017 from the National University of Malaysia, focusing on the development of a novel user authentication method called User Interface Preferences for Account Recovery (UIPA). Dr. Nader joined the Faculty of Artificial Intelligence at Al-Balqa Applied University in 2022, where he contributes his extensive expertise to the advancement of the field. His research interests include preference-based authentication and virtual privacy techniques. Dr. Nader's dedication to ongoing learning and collaboration ensures that he remains at the forefront of advancements in his field, making him a valuable asset to academia and the university community.

Dr. Hsiao-Ting Tseng is an Assistant Professor at Department of Information Management at National Central University, Taoyuan, Taiwan and Guest Editor of several journal Special Issues. She has also been awarded the Best Paper Award of several IEEE Conferences and the Young Scholar Fellowship (The Einstein Program) of the Ministry of Science and Technology of Taiwan. Her research focuses mainly on the application and impact of big data, AI and Metaverse on the social networking and economic development.

Dr. Mohammed AlShinwan received a Ph.D. degree from the School of Computer Engineering at Inje University, Gimhae, Republic of Korea, in 2017. He was an Assistant Professor at the Department of Computer and Information Sciences, Amman Arab University, Jordan. Currently, he is an Associate professor at an Applied science private university, in Jordan. His research interests in computer networks, Mobile networks, information security, AI, and optimization methods.