A Secure Video Watermarking Approach Using CRT Theorem in DCT Domain

Amir M. U. Wagdarikar, Ranjan K. Senapati and Sushmita Ekkeli

Abstract Authentication of multimedia data has gained a lot of interest in recent times. In this paper, a secure video data hiding scheme is proposed using Chinese Remainder Theorem (CRT) in the discrete cosine transform (DCT) domain. The secret binary image which is embedded in selected frames with a simple frame selection procedure helps to provide more authenticity for the host video. Modifying the high-frequency elements of the blocks of selected frames provides more imperceptibility and the information can be retained easily. This approach is robust against speckle and random noises, which makes it more suitable for real-time applications. The results obtained for the proposed approach depicts that it is robust against noise and filtering attacks and also provides better imperceptibility.

Keywords Video watermarking · DCT · CRT · Frame selection

1 Introduction

Digital data authentication has become a great challenge due to the rapid development of computer and internet technologies. A large amount of digital data is present on the web, and this data can be accessed and can be tampered by anyone through processing tools like Photoshop and video editors. The protection of authenticity of these digital files is a challenging task which can be accomplished with the use of high secure watermarking techniques [1].

A. M. U. Wagdarikar (✉) · R. K. Senapati
KL University, Vijayawada 520002, Andhra Pradesh, India
e-mail: 74.amir@gmail.com

R. K. Senapati
e-mail: ranjan.senapati@kluniversity.in

S. Ekkeli
VVPIET, Solapur, Maharastra, India
e-mail: sushmitaekkeli@gmail.com

G. Panda et al. (eds.), *Microelectronics, Electromagnetics and Telecommunications*, Lecture Notes in Electrical Engineering 521,
https://doi.org/10.1007/978-981-13-1906-8_61

Video broadcasting with utmost quality is of great interest over DVB-2 and Internet. However, most of the data which is broadcasted is not authenticated and it is distributed without any protection. To protect such type of data content invisible, the video has to be authenticated. In recent times, the digital video watermarking is becoming more popular because of its effective approach to copyright and protect this valuable data.

Today, this video watermarking will throw a demanding, challenging task for many of the researchers. Hiding the important or some data is termed as data hiding which is meant to embed some data into the host domain (any digital image, video, and sound). Plenty of research was conducted on digital image data hiding scheme, whereas the modern devices are more prone to the video content due to the increasing demand of internet services, video data hiding has got the extra potential for many business application and very low in a number of research methods were proposed to protect the video content. Due to the exhaustive nature of the video, it is very much preferable to alter the components in transform domain rather than doing it in the spatial domain. Hence, the video watermarking approaches are categorized into frame-based data hiding methods and transform domain-based schemes [2]. In this paper, one such approach is described in the transform domain.

A secure and more robust video authentication approach is proposed in this paper, which is robust against the transmission noises and attacks. The paper is organized as, Sect. 1 presents the introduction to the watermarking and its importance in the current research. Section 2 presents the related work done earlier by different researchers, Sect. 3 presents the basic concepts of DCT and CRT which are involved in the proposed framework. The procedures of key frame selection, an algorithm of embedding were also discussed. Section 4 presents the experimental results obtained with this approach and also presents the effect of attacks with various noises and filtering approaches for this framework.

2 Related Works

In recent years, many video watermarking algorithms were planned to implant vigorous watermark in videos. Scores of them center on the vigor of general signal processing and these attacks are mainly categorized as geometric attacks like rotation, scaling, and cropping. Filtering attacks like low-pass filtering, average and median filtering, and also compression attack in transform domain like JPEG compression [3, 4].

Hiding the data in the video sequences is performed either in bitstream level or the data level. In the bitstream level approach, the redundancies in the compression model are explored which is very useful for alterations leading to a good scope of hiding the data. But this type of hiding schemes is fragile and is used for authentication. In the data level, attacks are more robust so they are used for the broader range of applications.

In Kim et al. [5], embed watermark bits are embedded in the frequency domain as pseudo-random sequences. In Langelaar et al. [6], hide watermarks by removing or retaining chosen DCT coefficients. In Kapotas et al. [7], explored the redundant blocks for the selection of H.264 encoding. In Wong et al. [8], tried to alter the quantization matrix of the DCT coefficients in bitstream level. In Sarkar et al. [9], proposed an application of quantization index modulation to alter the low-frequency coefficients which are very suitable for hiding a large amount of data. In Liu et al. [10], proposed a 3D DWT domain-based data hiding scheme where the LL subband is used for data hiding with the use of BCH codes to increase error correction capability.

3 Proposed Frameworks

3.1 Frame Selection Procedure

An Mp4 video file is taken as an input video file whose frame rate is 25 frames per second. Let “nf” be the number of frames in the video sequence. This frame selection algorithm is based on the calculation of entropy of each individual frame and the frames with minimum, maximum, and mean values are indexed and selected for embedding process. Figure 1 is the building block of the video sequence, and it can be observed that “nf” number of frames is present in a single shot. In this analysis, only three frames are selected for embedding the data. The entropy of the frame is calculated as

$$E_f = -\sum_{i=1}\sum_{j=1} p(i, j)\log\left(p(i, j)\right)$$

where p(i, j) is the probability and “f” is the number of frames. Frames are selected which have max(E_f), min(E_f), and mean(E_f) values.

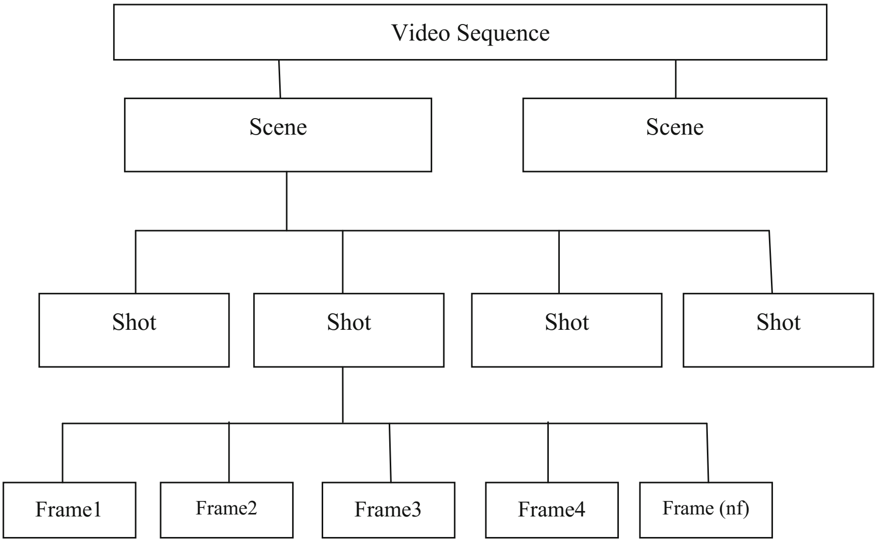

Fig. 1 Building block of the video sequence

3.2 Chinese Remainder Theorem

So far, many researchers have used this theorem in watermarking methods, and its main intention is to provide security by selecting a set of relatively prime numbers. Let the "r" be the integers represented as $\mu = \{M_1, M_2, \ldots, M_r\}$, so that two M_i are relatively prime.

$$Z = R_i (\text{mod } R_i)$$

where "R" is called residue and the solution for "Z" is obtained as

$$Z = \left(\sum_{i=1}^{r} R_i \frac{M}{M_i} K_i \right).$$

For example, let $M_1 = 6$ and $M_2 = 11$, $k_1 = 5$ and $k_2 = 2$, and $R_1 = 4$ and $R_2 = 8$. $M = M_1 * M_2 = 66$. Then, Z = (4 * 66/6 * 5 + 8 * 66/11 * 2) (mod 66) = 52.

And, the inverse can be obtained as 52 = R_1 (mod 6) then, $R_1 = 4$ and similarly, it can be calculated that $R_2 = 8$ [11].

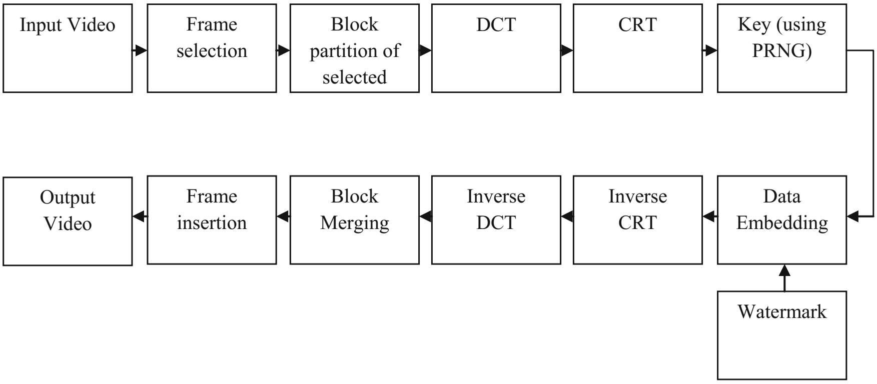

Fig. 2 Proposed framework block diagram

3.3 Proposed Algorithm

The proposed framework of embedding the data into video sequence is based on CRT in DCT domain. This approach is robust against noise attacks, and three different types of noises like speckle noise, Gaussian, and salt-and-pepper noises were validated with different video streams. The results are tabulated in the next section. Figure 2 shows a basic block diagram of the proposed algorithm.

Algorithm 1. Select the MP4 video file.
2. Select video frames from a video based on frame selection criteria
3. Divide the frame into blocks and apply DCT on every block
4. Using PRNG, generate a decimal and based on their rank select, the respective intensity level. Blocks are selected based on their ranking criteria
5. Select, pairwise relatively prime numbers such as $M_1 = 6$ and $M_2 = 11$.
6. In order to embed bit “1”, then condition is $R_1 \geq R_2$
7. In order to embed bit “0”, then condition is $R_1 \leq R_2$
8. Repeat the procedure from 5 to 8, until all the blocks are embedded with watermark bits.

4 Experimental Results

The proposed approach is tested and evaluated with different video sequences available at [12]. One of the key important features of this approach is to locate the position to embed the data in the cover frame data since 8 × 8 block size is used for

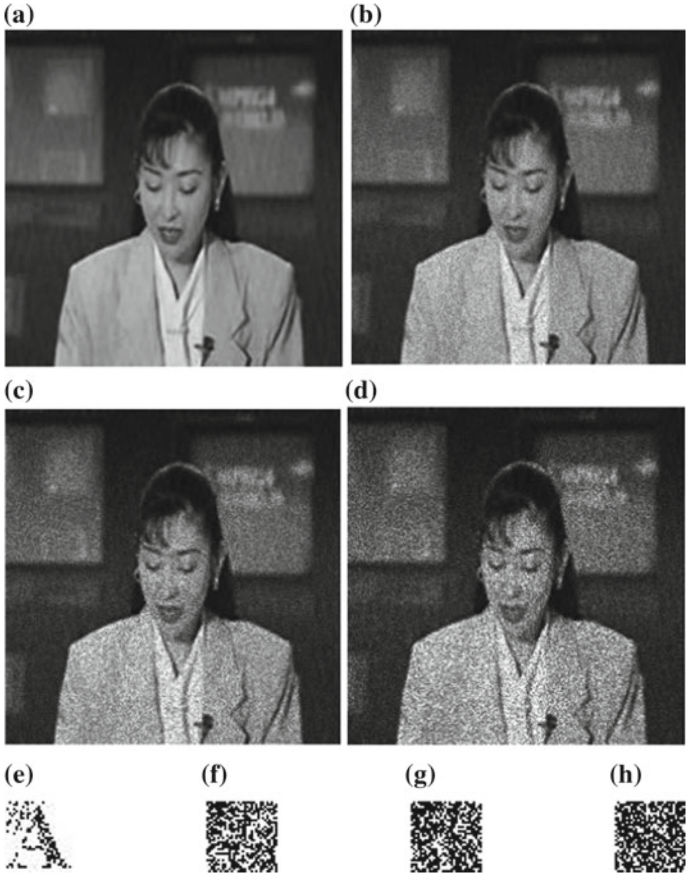

Fig. 3 **a** Without speckle noise, **b** with speckle noise of value 0.01, **c** with speckle noise of value 0.02, **d** with speckle noise of value 0.03, **e–h** extracted watermarks

DCT decomposition and a total of 64 DCT coefficients are obtained. This contains DC and AC components as it is known from [13] that DC components have most of the energy and information of the block, so the AC coefficients are selected for data hiding in a zigzag manner. Figures 3, 4, and 5 shows the result for $M_1 = 6$ and $M_2 = 7$,

The experiment results show that the present approach is robust under noise and filtering attacks with a PSNR varying from 28 to 22 at 0.01 noise density and also 48.31, 49.21 for median and Wiener filtering attacks which is shown in Tables 1 and 2.

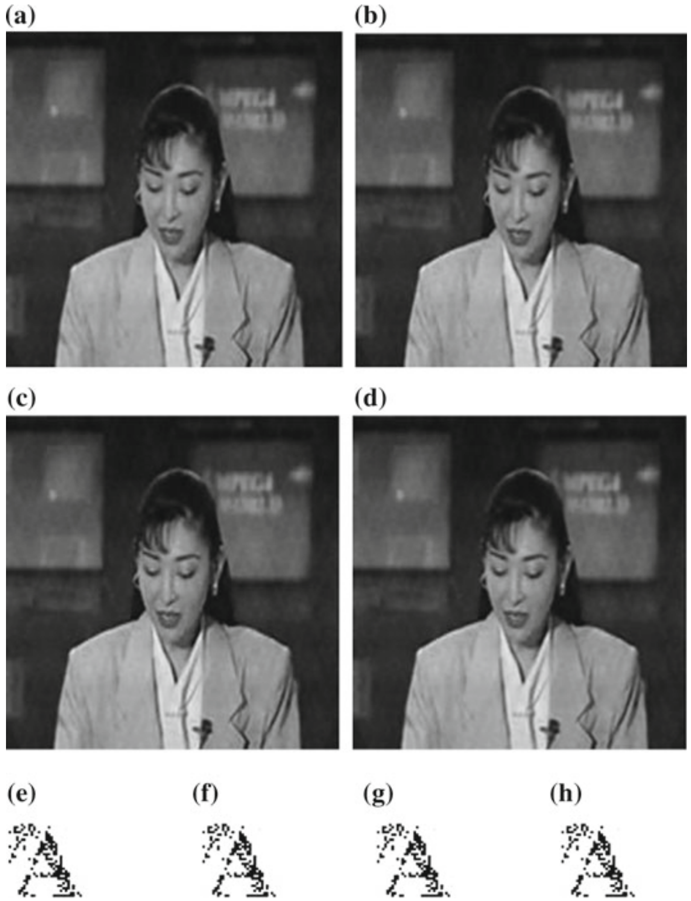

Fig. 4 **a** Without salt and noise, **b** with noise density 0.01, **c** with noise density 0.02, **d** with noise density 0.03, **e**–**h** extracted watermarks

This result also presents the evidence of imperceptibility with normalization coefficient not falling less than 0.8 which is a good achievement. Performance analysis of the proposed approach in terms of PSNR and NC for various noises is shown in Fig. 6.

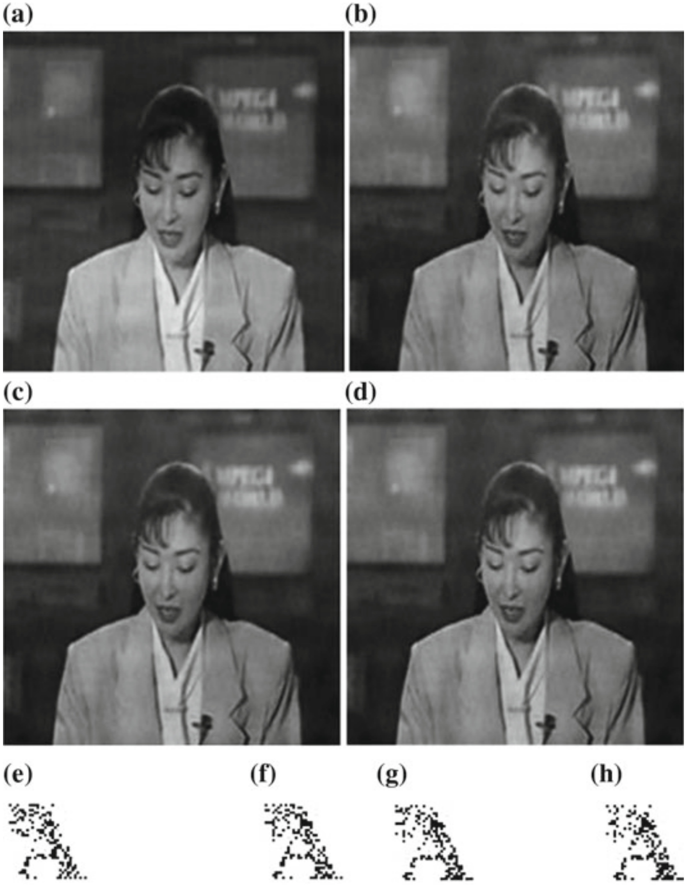

Fig. 5 **a** Without Gaussian, **b** with noise density 0.01, **c** with noise density 0.02, **d** with noise density 0.03, **e**–**h** extracted watermarks

Table 1 Analysis of the proposed approach under salt-and-pepper noise attack

Noise density	PSNR	NC	Tamper
0	46.42546	0.901515	4.296875
0.01	24.27089	0.77984	9.66796875
0.02	19.5756	0.501727	18.1640625
0.03	16.61077	0.296028	24.8046875
0.04	14.43571	0.156337	29.39453125
0.05	12.77404	0.062267	34.5703125
0.06	11.40886	0.073675	35.546875
0.07	10.28177	0.024982	39.35546875
0.08	9.361016	0.00725	40.625
0.09	8.571215	0.016177	42.08984375
0.1	7.893218	0.033758	39.94140625

Table 2 Under filtering attacks

Filtering	PSNR	NC	Tamper
Median filtering	48.31	0.83	8.88
Wiener filtering	49.42	0.89	5.37

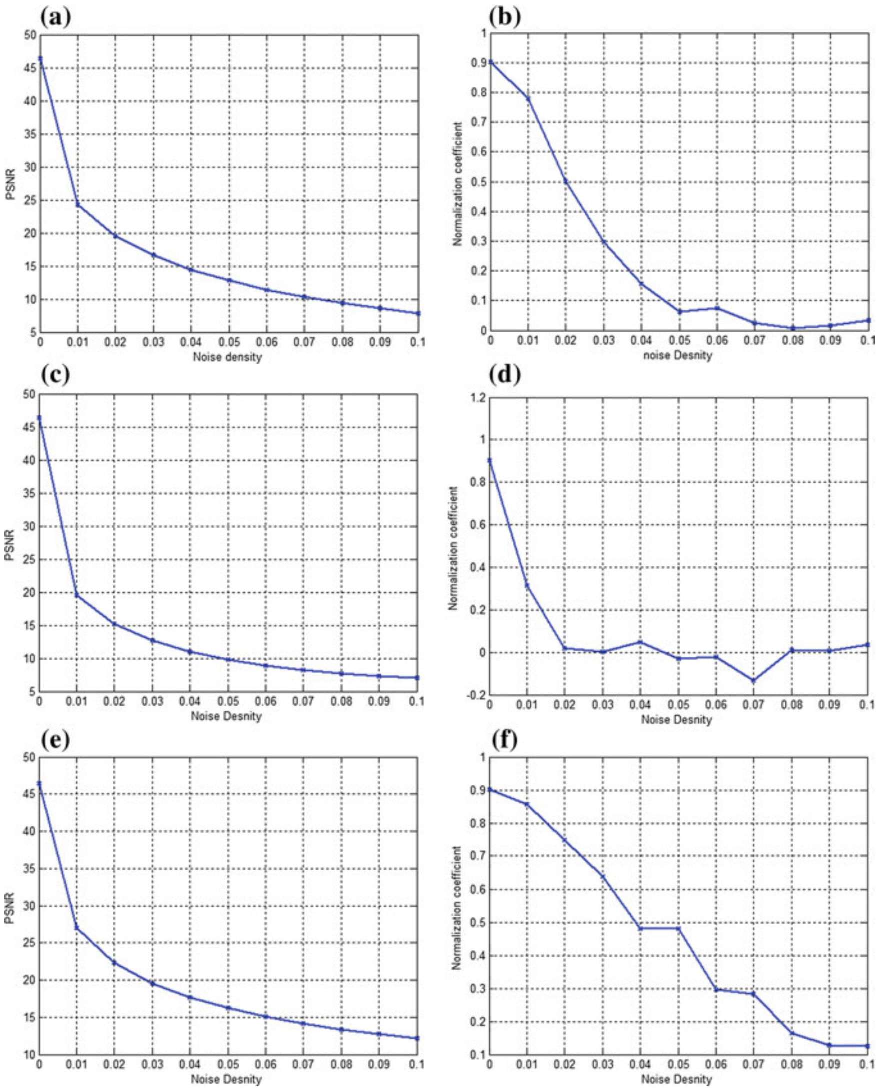

Fig. 6 Performance analysis of the proposed approach in terms of PSNR and NC **a** and **b** for salt and pepper, **c** and **d** for Gaussian noise, **e** and **f** for speckle noise

5 Conclusions

Simpler and secure robust video watermarking approach is proposed in this paper, this approach provides more security with the use of CRT and it is more imperceptible and robust due to the modification of the AC components of DCT coefficients. Presently, this work is performed on grayscale video and further, this extended under different color transformations with more secure features. From the experimental analysis, it is evident that this approach is not only robust but also can be used for high-quality digital video transmission as the NC values are quite satisfactory.

References

1. Podilchuk I, Delp EJ (2001) Digital watermarking: algorithms and applications. IEEE Signal Process Mag 18(4):33–46
2. Lin ET, Eskicioglu AM, Lagendijk RL, Delp EJ (2005) Advances in digital video content protection. Proc IEEE (Special Issue on Advances in Video Coding and Delivery) 93(1):171–183
3. Hartung F, Girod B (1997) Fast public-key water-marking of compressed video. In: Proceedings of IEEE international conference on image processing, vol 1, Oct 1997, pp 528–531
4. Langelaar GC, Lagendijk RL, Biemond J (1999) Watermarking by DCT coefficient removal: a statistical approach to optimal parameter settings. In: Proceeding of SPIE symposium of security and watermarking of multimedia contents, pp 2–13
5. Kim WG et al (1999) An image watermarking scheme with hidden signatures. In: Proceedings of IEEE international conference on image processing, vol 2, Oct 1999, pp 205–210
6. Langelaar GC, Lagendijk RL, Biemond J (1999) Watermarking by DCT coefficient removal: a statistical approach to optimal parameter settings. In Proceedings of SPIE symposium of security and watermarking of multimedia contents, pp 2–13
7. Kapotas SK, Varsaki EE, Skodras AN (2007) Data hiding in H-264 encoded video sequences. In: Proceedings of the IEEE 9th workshop multimedia signal processing, Oct 2007
8. Wong K, Tanaka K, Takagi K, Nakajima Y (2009) Complete video quality-preserving data hiding. IEEE Trans Circuits Syst Video Technol 19(10):1499–1512
9. Sarkar A, Madhow U, Chandrasekaran S, Manjunath BS (2007) Adaptive MPEG-2 video data hiding scheme. In: Proceedings of the 9th SPIE security steganography watermarking multimedia contents, pp 373–376
10. Liu H, Huang J, Shi YQ (2005) DWT-based video data hiding robust to MPEG compression and frame loss. Int J Image Graph 5(1):111–134
11. Patra JC, Karthik A, Bornand C (2010) A novel CRT-based watermarking technique for authentication of multimedia contents. Digital Signal Process 442–453
12. http://trace.eas.asu.edu/
13. Rao KR, Hwang JJ (1996) Techniques and standards of image, video and audio coding. Prentice Hall