IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 2, 2020, accepted January 16, 2020, date of publication January 22, 2020, date of current version February 5, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2968740

Research on Covert Communication Security Based on Screen Content Coding

ZHE LIU[1], HE CHEN[1], AND SONGLIN SUN[2], (Senior Member, IEEE)
[1]School of Information and Electronics, Beijing Institute of Technology, Beijing 100081, China
[2]School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China

Corresponding author: Zhe Liu (liuz2020bit@163.com)

ABSTRACT Covert transmission technology is a new direction in the field of information security technology. It can protect copyright and authentication sources and integrity in an open network environment, and ensure the security of digital media content through information hiding technology. Some unique features of screen content video have promoted the further development of video coding technology, and the HEVC-SCC standard has emerged as the times require. It is of great significance and value to study the information security issues of screen content coding standards. Therefore, based on the unique characteristics of the SCC stream, this paper studies the information steganography technology, and uses the video information hiding technology to transmit private data. A video steganography scheme based on chaotic mapping in DCT domain is proposed where the proposed method applies to HEVC screen content coding. The mutation frame of the screen content sequence is judged according to the threshold value, and the location of the secret data embedding is shuffled and scrambled based on the value of the chaotic logistic map digital chaotic sequence, thereby improving the security.

INDEX TERMS Screen content coding, steganography, security, HEVC.

I. INTRODUCTION

Although information hiding technology has a shorter history than cryptography, it has also experienced a long time of development. Steganography is to hide secret information in the carrier, using the data redundancy of the carrier and the characteristics of human perception system to hide the existence of secret information. The most common carrier data are text, image, audio, video and other multimedia data. It can also be hidden in network operation or data stream for secret transmission, which is usually called covert communication. Video hiding technology: through embedding secret information in the characteristic data area of digital video by modification or replacement, information hiding is realized [1].

According to the location of information hiding, we can divide it into two categories: spatial information hiding that operates on the spatial characteristics of the carrier and temporal information hiding that operates on the temporal characteristics of the carrier. One is based on the spatial domain method of embedding the redundant data area of the carrier, in which the simplest least significant bit algorithm belongs to a kind of vulnerability information hiding [2].

When the carrier is modified and compressed, the information will be lost and cannot be reproduced. The other is the transform domain. DCT and wavelet transform are more frequent and easy to implement. By changing part of the characteristics of the carrier, the transform domain method disperses the added information to each pixel. The redundancy of vision and hearing is easy to combine with coding mode, and it can deal with general geometric / noise attacks, which makes the system more robust.

Video information hiding algorithms mainly belong to built-in embedding, and usually the information embedding process is completed by modulating transform coefficients or quantized change coefficients. This is because the combination of built-in embedding and specific compression coding has many options for embedding secret information, and the compressed video encoded stream contains a large number of transform coefficients, which can provide the number of carriers for information hiding, which has caused a lot of research Attention. There are two main types of embedding information in the transform domain: embedding in transform coefficients before quantization and embedding in transform coefficients after quantization.

The associate editor coordinating the review of this manuscript and approving it for publication was Li He.

With the loss from quantization process, the hidden information embedded may not be fully extracted. Therefore, embedding information in the quantized transform coefficients is the mainstream of video information hiding.

An information hiding technology based on the size of coding block in HEVC is proposed [3]. In order to improve the payload, the non-zero DCT coefficients are manipulated in some range to further deploy the information hiding technology based on parity. The error drift in H.264/AVC is eliminated by analyzing the error propagation phenomenon and the characteristics of 4×4 quantized DCT coefficients in the frame, and the reversible data hiding scheme is realized [4]. Based on HEVC, we select the appropriate if location of 8×8 block set, and select the coefficient close to if to embed secret data to complete reversible data hiding technology [5]. Chang *et al.* [6] proposes video steganography based on HEVC, which is derived the error formula of embedding distortion based on DCT and DST coefficient modification, and proposed the hiding algorithm based on DCT and DST coupling coefficient. The method that applying DCT to the cover image [7], scans the AC coefficient from the lowest effective value to the highest effective value in the form of zigzag, and determines the embedding position through the chaos function and the allowable maximum value to realize a steganography scheme based on the chaos mapping in DCT domain. Then a lossless data hiding scheme in JPEG image is proposed by Wang *et al.* [8]. In reference [9], based on the mapping function of genetic algorithm, the data is embedded in the cover image with 4×4 discrete wavelet transform coefficients. The frequency domain is used to improve the robustness of steganography, and the genetic algorithm and the best pixel adjustment process are used to obtain the best mapping function.

A new video steganography scheme based on random integer generation in DCT domain is proposed [10]. After data hiding, high security and good video quality can be achieved. An information embedding method of adaptive coding block size selection proposed by Tewy and Wong [3], which realized information embedding by mapping rules between coding unit and secret information, and improved embedding capacity by non-zero DCT coefficient. And an intra transform coefficient modification algorithm is proposed for HEVC [11]. By modifying the coefficients at a specific location, the resulting errors will not propagate to adjacent blocks due to intra prediction, effectively preventing the embedded errors from propagating in the frame, and reducing the impact of coefficient modification on video quality to a certain extent. The steganography method from Alamsyah *et al.* [12] is implemented by using the MSB (most significant bit) image cover bit to find the similar bit of the message. From the scheme of information hiding using quantization DCT coefficient of I frame, Ma *et al.* [13] uses compensation to limit the intra frame distortion drift. When the DCT coefficient of a 4×4 luminance block is modified, another coefficient is found to compensate at the same time. Furthermore, the paper [14] uses coefficient parity to hide data after transformation and quantization.

Recently, an algorithm for video compression has been proposed [15], based on a secret sharing scheme and an Error-Correcting Code, which the DCT blocks combines Grey Relational Analysis with a partition mode, and then use rules to hide the pretreated information in DCT coefficients. And in order to avoid obvious visual artifacts and data embedding distortion, there is an efficient cost assignment-based video data hiding scheme which considers texture and motion changes of the intra-frame with syndrome-trellis code and make improvement for quantized discrete cosine transform (QDCT) method [16]. And, by using the color mixing characteristics of different colors Peng has proposed a vectorized color modulation scheme [17] for a covert camera-screen communication (CSC) system, which may become a possible reference direction for video transmission.

At present, the most popular research of video steganography is to embed privacy data according to DCT coefficient. The main problem of this embedding algorithm is what kind of embedding strategy is used, which can not only reduce the distortion drift caused by data embedding, but also improve the robustness of video hiding system and reduce the complexity of the algorithm. Finally, video steganography can be integrated with standard codec system to improve the overall performance of the system.

II. PREVIOUS WORK

Compared with the natural sequence, the screen content sequence has many unique characteristics. Different from the natural sequence, the screen content sequence often contains a lot of scene mutations. For example, in the distance education, the quick page change of the presentation, the quick switch of the tabs when browsing the web page, etc. Because of the lack of correlation with the encoded frame, the mutation frame is often encoded in the way of intra prediction, which consumes a lot of bits and brings a large fluctuation of bits. By analyzing the characteristics of screen content sequence and natural sequence, the complexity of current frame can be obtained by using fast motion estimation. On this basis, based on the sliding window and the complexity of the image as the weight, the limited resources are allocated more reasonably to ensure that the mutation frame can obtain sufficient bits for coding.

HEVC supports the division of encoded video into several coding tree units. The CTU is divided into coding units according to the quad-tree structure, and the dimensions of four CU's in the same level must be equal. Sizes range from 64×64 to 8×8. The larger the CU is, the smoother the image is; on the contrary, the more complicated the image texture is.

Each CU can be divided into smaller units (i.e. PU). Pu is used for inter frame or intra frame prediction. CU can be divided into multiple PU. The maximum size of PU can be equal to the size of CU, and the minimum size is 4×4. Because the human eye is sensitive to the noise in the smooth

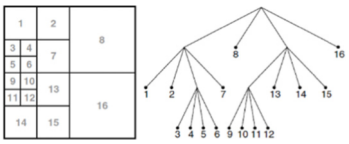

FIGURE 1. Partitioning method of coding unit CU based on quadtree.

area of the image and insensitive to the noise in the complex area of the texture, it is easier to hide more information and achieve invisibility in the complex area of the texture. Therefore, the luminance block with higher texture complexity is selected as the secret information hiding area.

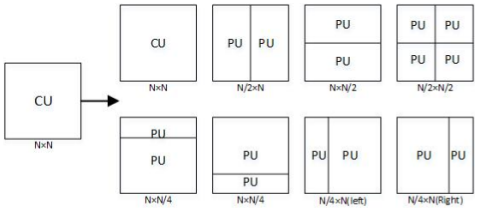

FIGURE 2. Partitioning method of prediction unit PU based on HEVC.

In HEVC standard, luminance data and chrominance data are represented by transform block, and transform coefficients are expressed by encoding the position information and amplitude information of non-zero coefficients. Before entropy coding, the encoder arranges the two-dimensional quantized transform coefficients into one-dimensional sequence. HEVC supports three scanning modes: zig-zag scanning, horizontal scanning and vertical scanning. In the process of steganography, zig-zag transformation can not only play the role of encryption, but also adjust the internal position of the information in the steganography area of the carrier to improve the consistency with the secret information, so as to improve the robustness of the steganography algorithm.

Video sequence is composed of one image, each image can be divided into sub blocks of different sizes, so video processing is based on blocks. There are many motion characteristics in the video. In order to adapt to this characteristic, the luminance block and the chroma block are divided into 8 $\times$ 8 sub blocks, and then the sub blocks are DCT transformed and quantized. According to different motion scenes, video can choose 16 $\times$ 16 or 8 $\times$ 8 sub blocks for DCT transformation. According to HVS theory of human eye, human eye is not sensitive to the details of image, and it is difficult for human eye to recognize the transformation of some details. Therefore, 8 $\times$ 8 sub block is chosen as the steganography area of information.

III. PROPOSED METHOD

Steganography can easily cause video image distortion. In order to reduce the distortion of the video image, the secret information can be hidden in the least significant bit, which can minimize the distortion of the video image. This algorithm is to embed the secret information on the least significant bit of the DCT discrete cosine coefficient.

A. STEP OF EMBEDDING

Step A: Preprocessing operation

Many screen content videos are sampled and captured in RGB color space. Different color components in the RGB color space often have a strong correlation. Applying the color space conversion method can effectively remove the redundancy between the color components and improve the coding efficiency. Therefore, the conversion method of HEVC-SCC to convert RGB space to l, α, β color space is adopted.

$$\begin{bmatrix} L \\ M \\ S \end{bmatrix} = \begin{bmatrix} 0.3811 & 0.5783 & 0.0402 \\ 0.1967 & 0.7244 & 0.0782 \\ 0.0241 & 0.1288 & 0.8444 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \quad (1)$$

where $\mathrm{L}' = \log L$, $\mathrm{M}' = \log M$, and $\mathrm{S}' = \log S$.

$$\begin{bmatrix} l \\ \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} 1/\sqrt{3} & 0 & 0 \\ 0 & 1/\sqrt{6} & 0 \\ 0 & 0 & 1/\sqrt{2} \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & -2 \\ 1 & -1 & 0 \end{bmatrix} \begin{bmatrix} L' \\ M' \\ S' \end{bmatrix} \quad (2)$$

The advantage of l, α, β color space is that it can eliminate the strong correlation of color space. When a certain component is modified, it does not worry that other components will also change accordingly, which is convenient for information steganography.

Step B: Video frame pre-judgment

Based on the video characteristics of SCC, judging the abrupt frame by threshold.

$$Threshold = \frac{\sum_{k=1}^{N} (N - K + 1) \cdot C_{i-k}}{\sum_{j=1}^{N} j}, \quad i \geq N \quad (3)$$

If $C_i > 50 | C_i > 5 \times Threshold, f(k) \geq 2$, it is judged as an abrupt frame; if $C_i < 0.1, f(k) < 2$, it is judged as a non-abrupt frame. The frame next to the first abrupt change is selected to embed the data. For different information or data that needs to be hidden, one or more consecutive frames can be selected to hide confidential data.

Step C: DCT coefficient generation

Next, the DCT coefficients of the sub-images are estimated, and the 8 least significant DCT coefficients are replaced with thresholds. The threshold value is 0 or 1, depending on the confidential information to be hidden, and the position of the confidential information depends on the generated random integer. After confirming the frame to be embedded in the data, the video frame is divided into 8×8 sub-images, f_w represents the frame to be embedded with the secret data, and image S (x, y) can also be expressed as $S_l(x, y)$, $S_\alpha(x, y)$, $S_\beta(x, y)$, where $S_l(x, y)$, $S_\alpha(x, y)$, $S_\beta(x, y)$ represent l, α, β three colors component.

C-1: Initialize the l-component of frame and divide it into 8×8 non-overlapping sub-image blocks with a number of $\frac{W \times H}{64}$, where W and H represent the size of the video frame, and $s(x, y)$ represents the sub-image blocks.

C-2: Obtain the DCT coefficients of the sub-image blocks, and record the DCT values as $C_s(U, V)$, where $s(x, y)$ is the image matrix of $W \times H$.

$$C_s(U,V) = \frac{2}{\sqrt{WH}} C(U) C(V) \sum_{x=0}^{W-1} \sum_{y=0}^{H-1} s(x,y) \times cos\frac{(2x+1)U\pi}{2W} cos\frac{(2y+1)V\pi}{2H} \quad (4)$$

where the parameters meet the conditions $x, u = 0, 1, \ldots, W-1$ and $y, v = 0, 1, \ldots, N-1$. So considering the situation,

When

$$U, V = 0,$$
$$C_s(U,V) = \sqrt{\frac{1}{8}} \sum_{x=0}^{7} \sum_{y=0}^{7} s(x,y) cos\frac{(2x+1)U\pi}{2W} cos\frac{(2y+1)V\pi}{2H};$$

When

$$U, V \neq 0,$$
$$C_s(U,V) = \frac{1}{2} \sum_{x=0}^{7} \sum_{y=0}^{7} s(x,y) cos\frac{(2x+1)U\pi}{2W} cos\frac{(2y+1)V\pi}{2H}.$$

Repeat the same operation for $S_\alpha(x, y), S_\beta(x, y)$ components.

The transform block of size 8×8 has a total of 64 coefficients. For the transform coefficients, the low-frequency coefficients in the upper left corner represent the basic contour information of the image, and the image details are represented by the high-frequency coefficients in the lower right corner. The impact of the modification on image quality is relatively slight, and it is more difficult to see the difference visually.

Step D: Improve security by generating random sequences of integers

Because the chaotic sequence has good convenience, determining the embedding position of the secret image information based on chaotic mapping can realize the random distribution of steganography. At the same time, it has strong sensitivity to initial values, and requires precise keys when extracting secret information, which effectively ensuring information security.

Using the improved two-dimensional time-varying discrete-time space-time system to generate the logistic mapping digital chaotic sequence, a new pseudo-random key stream sequence is generated based on the initial key. Substitute x_k and y_k as initial values into the formula to obtain a pseudo-random sequence as the initial sequence.

$$x_{n+1} = \lambda x_n (1 - x_n) \quad (5)$$

where the parameter x_0 is the initial value, the branch parameter is λ which the value is between 0 and 4.

$$x_{n+1,n} = \frac{1 + (-1)^m}{2} \left(y_{m,n} + x_{m,n}\right) + x_{m,n+1} \ mod\ 256 \quad (6)$$
$$y_{m+1,n} = a_m y_{m,n} + b_m y_{m,n} + y_{m,n+1} \ mod\ 256 \quad (7)$$

Select the three significant digits after the decimal point of the real-valued chaotic sequence x_k to obtain the integer sequence $y_k = \{y_0, y_1, y_2, \ldots, y_{N-1}\}$, and the size of the hidden image $M(x, y)$ is $N = u \times v$.

Step E: Embedded data algorithms

E-1: The pixel matrix P of the secret image $M(x, y)$ is hidden in the DCT coefficients of the sub-image block, and the pixel P is converted into an 8-bit binary number sequence, expressed as $q_s = \{q_7, q_6, q_5, q_4, q_3, q_2, q_1, q_0\}$. In addition, the random integer sequence y_k becomes a random binary integer sequence, and the binary bits are hidden in the DCT coefficients $C_s(U, V)$ of the sub-image.

E-2: Perform an XOR operation with q and the random number sequence converted to binary to obtain the binary sequence $q_b = \{q'_0, q'_1, q'_2, q'_3, q'_4, q'_5, q'_6, q'_7\}$ to hide in the least significant DCT coefficients in a certain order. Scan each DCT block in two different zigzag forms from the low significant DCT-coefficient to the most significant DCT-coefficient. The selection of the embedding position is based on the value of the random integer sequence modulo the data.

$$Y_k = [y_k \ mod\ 2] \quad (8)$$

Firstly, when the case of $Y_k = 0$, the first shuffling of data method is given by: $C_{63} - C_{55} - C_{62} - C_{61} - C_{54} - C_{47} - C_{39} - C_{46} - C_{53}$, which shuffle the positions to embed the binary number sequence $\{q'_0, q'_1, q'_2, q'_3, q'_4, q'_5, q'_6, q'_7\}$;

Secondly, when the case of $Y_k = 1$, the second shuffling of data method is adopted which is $C_{63} - C_{62} - C_{55} - C_{47} - C_{54} - C_{61} - C_{60} - C_{53} - C_{46}$.

The partial coefficients of the selected embedded information are set to zero and recorded as $C_z(i, j)$, IDCT operation is applied to each $C_z(U, V)$, and then DCT operation is performed to obtain $D_z(i, j)$. Finally, the situation is discussed based on the value of the secret information q to determine whether $D_z(i, j)$ is subtracted or added to the variable delta and then embedded in the corresponding position in the previous step.

$$delta = \sum_{i=1}^{8} \sum_{j=1}^{8} |D_z(i,j)| \times \Delta / 100 \quad (9)$$

where Δ is a value between 0.1 and 2. When q_s is 0, the embedded DCT subgraph $E_z(i, j) = D_z(i, j) - delta$; when q_s is 1, $E_z(i, j) = D_z(i, j) + delta$.

The inverse IDCT transform is applied to the sub-image coefficients $E_z(i, j)$ of the embedded information to generate

C_0	C_1	C_2	C_3	C_4	C_5	C_6	C_7
C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}	C_{14}	C_{15}
C_{16}	C_{17}	C_{18}	C_{19}	C_{20}	C_{21}	C_{22}	C_{23}
C_{24}	C_{25}	C_{26}	C_{27}	C_{28}	C_{29}	C_{30}	C_{31}
C_{32}	C_{33}	C_{34}	C_{35}	C_{36}	C_{37}	C_{38}	C_{39}
C_{40}	C_{41}	C_{42}	C_{43}	C_{44}	C_{45}	C_{46}	C_{47}
C_{48}	C_{49}	C_{50}	C_{51}	C_{52}	C_{53}	C_{54}	C_{55}
C_{56}	C_{57}	C_{58}	C_{59}	C_{60}	C_{61}	C_{62}	C_{63}

FIGURE 3. DCT coefficient for the 8 × 8 sub image.

steganographic video frames, and the above steps are repeated for all sub-images that can generate steganographic video.

B. STEP OF EXTRACTION

The extraction of secret information is the reverse process of information embedding.

First step, the hidden information images are sequentially extracted, and the carrier frame is also subdivided into non-overlapping blocks. Furthermore, the DCT coefficient of the sub-image is calculated and represented as $C_e\,(i, j)$.

Second step, similar to the operation of generating a random sequence in the embedding operation, a pseudo-random integer Y_k needs to be obtained during extraction. Calculate y_k using the formula $y_k mod 2$ and determine where the DCT coefficients are scrambled.

Third step, based on the scrambling method during embedding, those DCT coefficients that are hidden to zero need to be reset their positions, and the reset coefficients are $Z_e\,(i, j)$.

Fourth step, IDCT is applied on $Z_e\,(i, j)$ and then on DCT to obtain $D_e\,(i, j)$.

Fifth step, hidden bit information extraction. When the subtraction between the DCT coefficient of the sub-image and $D_e\,(i, j)$ in the previous step is greater than 0, the hidden information bit is judged to be 1; otherwise, it is 0.

Sixth step, the sequence $\{q_7, q_6, q_5, q_4, q_3, q_2, q_1, q_0\}$ derives from the XOR operation of the obtained bit information and the random sequence. The pixels are reconstructed through decimal conversion, and the operation is repeated to reconstruct the hidden image.

IV. EXPERIMENT RESULTS

Invisibility is a vital performance indicator in information hiding algorithms. This section uses simulation experiments to analyze the invisibility of the information hiding algorithm implemented in this chapter, including subjective quality and objective quality.

(1) Subjective quality: verify the results of information hiding on the test video sequences suggested by SCC such as SlideShow, Web_browsing, Map, etc., then select the photo of Lena as the data to be hidden, and compare the quality of the original frame with the embedded video frame.

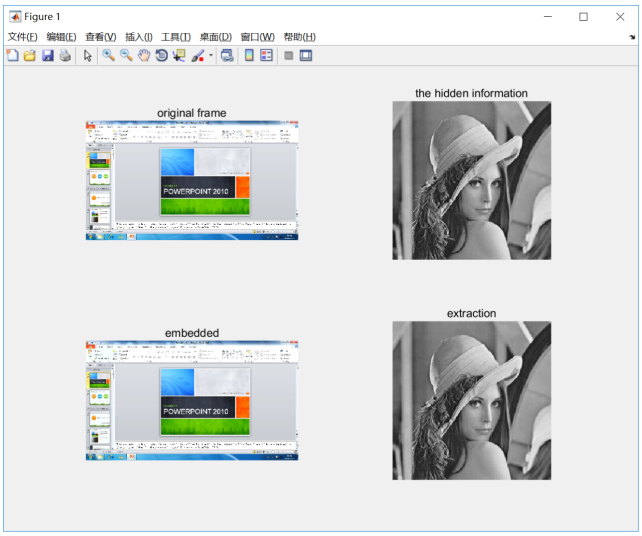

FIGURE 4. Visual subjective quality of embedding and extraction.

(2) Objective quality: In order to measure the performance of the algorithm in a quantitative way, objectively evaluate the embedded algorithm using PSNR, SSIM before and after changes, and analyze bit rate change. PSNR represents the fidelity of the dense video relative to the original video and the value ranges from zero to positive infinity. The larger the value, the smaller the distortion introduced by the embedded information. SSIM is a measure of the similarity between two images. Its value can better reflect the subjective perception of the human eye which ranges from 0 to 1. The higher the value, the higher the consistency with the original video.

TABLE 1. Objective quality.

Sequence	QP	Bitrate	Original		With proposed method	
			PSNR	SSIM	PSNR	SSIM
Console	27	33387.38	40.48	0.978	40.35	0.977
	32	22739.21	35.58	0.987	35.27	0.982
Desktop	27	15733.29	40.36	0.992	39.37	0.988
	32	11024.11	35.33	0.993	35.24	0.991
Map	27	1953.23	40.55	0.989	40.54	0.982
	32	1184.89	36.53	0.991	36.45	0.986
Programming	27	7145.65	39.95	0.939	39.92	0.932
	32	4038.77	35.91	0.954	35.62	0.951
Robot	27	2277.88	37.63	0.994	37.58	0.990
	32	789.82	35.29	0.996	34.18	0.992
SlideShow	27	779.66	44.98	0.988	44.63	0.984
	32	470.94	41.36	0.991	41.25	0.989
Web_browsing	27	1182.16	40.79	0.879	40.18	0.876
	32	687.22	35.76	0.899	35.54	0.894
WordEdit	27	5038.38	39.86	0.993	39.76	0.991
	32	3146.61	35.28	0.994	34.94	0.987

Seen from the PSNR and SSIM values of the original compressed video, it can be analyzed that the comparative result between original video and embedded video: the maximum

PSNR drop is 2dB, the minimum is less than 1dB, and the SSIM value drops even less than 0.01. The structure and pixel values of the image have not changed much.

$$\omega = \frac{B - B_O}{B_O} \times 100\% \tag{10}$$

B is the bit rate after embedding and B_O indicates the original bit rate. Before and after the information is embedded, there is no significant bit rate change of the video coding which means that small bit rate increment does not put additional pressure on the video transmission bandwidth.

V. CONCLUSION

At present, there are few researches on video information hiding algorithms based on HEVC screen content coding. This paper proposes a new video steganography technology based on DCT domain and chaotic sequences for SCC. By referring the prejudgment of the screen content sequence encoding and detecting the abrupt frames based on the complexity analysis, the scene changes of the video frames are identified. The carrier frame is divided into 8×8 sub-images, and the purpose of improving security is achieved by scrambling hidden data of some least significant bit coefficients in the DCT transform coefficients. Experiments have shown that there is no significant difference in subjective visual perception after data hiding, ensuring that the video has good quality.

REFERENCES

[1] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, "Digital image steganography: Survey and analysis of current method," *Signal Process.*, vol. 90, pp. 727–752, Mar. 2010, doi: 10.1016/j.sigpro.2009.08.010.
[2] C.-K. Chan and L. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognit.*, vol. 37, no. 3, pp. 469–474, Mar. 2004.
[3] Y. Tew and K. S. Wong, "Information hiding in HEVC standard using adaptive coding block size decision," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Oct. 2014, pp. 5502–5506, doi: 10.1109/ICIP.2014.7026113.
[4] W. Huo and Y. Zhu, "A reversible watermarking algorithm with error-drift elimination in H.264/AVC stream," in *Proc. Int. Conf. Consum. Electron., Commun. Netw. (CECNet)*, Apr. 2011, pp. 2893–2896.
[5] F. Gui and H. Xue, "A reversible data hiding scheme for HEVC," in *Proc. 10th Int. Symp. Comput. Intell. Design (ISCID)*, Hangzhou, China, Dec. 2017, pp. 34–37.
[6] P.-C. Chang, K.-L. Chung, J.-J. Chen, C.-H. Lin, and T.-J. Lin, "An error propagation free data hiding algorithm in HEVC intra-coded frames," in *Proc. Asia–Pacific Signal Inf. Process. Assoc. Annu. Summit Conf.*, Kaohsiung, Taiwan, Oct./Nov. 2013, pp. 1–9.
[7] M. Saidi, H. Hermassi, R. Rhouma, and S. Belghith, "A new adaptive image steganography scheme based on DCT and chaotic map," *Multimedia Tools Appl.*, vol. 76, no. 11, pp. 13493–13510, Jun. 2017.
[8] K. Wang, Z.-M. Lu, and Y.-J. Hu, "A high capacity lossless data hiding scheme for JPEG images," *J. Syst. Softw.*, vol. 86, no. 7, pp. 1965–1975, 2013.
[9] G. Elham, S. Jamshid, and F. Nima, "High capacity image steganography using wavelet transform and genetic algorithm," in *Proc. Multi Conf. Eng. Comput. Scientists*, vol. 1, 2011.
[10] M. Suresh and I. Shatheesh Sam, "High secure video steganography based on shuffling of data on least significant DCT coefficients," in *Proc. 2nd Int. Conf. Intell. Comput. Control Syst. (ICICCS)*, Madurai, India, Jun. 2018, pp. 877–882.
[11] P.-C. Chang, K.-L. Chung, J.-J. Chen, C.-H. Lin, and T.-J. Lin, "A DCT/DST-based error propagation-free data hiding algorithm for HEVC intra-coded frames," *J. Vis. Commun. Image Represent.*, vol. 25, no. 2, pp. 239–253, 2014.
[12] I. Alamsyah, M. A. Muslim, and B. Prasetiyo, "Data hiding security using bit matching-based steganography and cryptography without change the stego image quality," *J. Theor. Appl. Inf. Technol.*, vol. 82, no. 1, pp. 106–112, 2015.
[13] X. Ma, Z. Li, H. Tu, and B. Zhang, "A data hiding algorithm for H.264/AVC video streams without intra-frame distortion drift," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 20, no. 10, pp. 1320–1330, Oct. 2010.
[14] Y. Li, H.-X. Chen, and Y. Zhao, "A new method of data hiding based on H.264 encoded video sequences," in *Proc. Int. Conf. Signal Process.*, Oct. 2010, pp. 1833–1836, doi: 10.1109/ICOSP.2010.5656918.
[15] Y. Zhang, M. Zhang, X. Yang, D. Guo, and L. Liu, "Novel video steganography algorithm based on secret sharing and error-correcting code for H.264/AVC," *Tinshhua Sci. Technol.*, vol. 22, no. 2, pp. 198–209, Apr. 2017.
[16] Y. Chen, H. Wang, H.-Z. Wu, Z. Wu, T. Li, and A. Malik, "Adaptive video data hiding through cost assignment and STCs," *IEEE Trans. Depend. Sec. Comput.*, to be published.
[17] C. Peng and Z. Xu, "Vectorized color modulation for covert camera-screen communication," in *Proc. ICC-IEEE Int. Conf. Commun. (ICC)*, Shanghai, China, May 2019, pp. 1–6.

ZHE LIU received the B.S. degree from China People's Police University, in 1996, and the M.A. degree from Peking University, in 2000. He is currently pursuing the Ph.D. degree with the Beijing Institute of Technology.

HE CHEN was born in Shenyang, in 1970. She received the Ph.D. degree in electronic engineering from the Harbin Institute of Technology, in 1998. She is currently a Professor with the Beijing Institute of Technology. Her main interests are in the areas of real-time image and signal processing, system-on-chip design, and VLSI architectures for neural networks.

SONGLIN SUN (Senior Member, IEEE) received the B.S. degree in radio technology and the M.S. degree in signal and information processing from Shandong University, in June 1997 and January 2000, respectively, and the Ph.D. degree in communication and information system from the Beijing University of Posts and Telecommunications, in September 2003. He is currently an Associate Professor with the School of Information and Communication Engineering, Beijing University of Posts and Telecommunications. His research interests include signal processing in adaptive filter design, signal estimation in fading channel wireless communication in massive MIMO, cognitive radio, 4G/5G network technology in heterogeneous networks, SDN video codec and multimedia transmission in H.265/HEVC inter coding, and joint source-channel coding. He received the Chinese Industry-University-Research (IUR) Innovation Award, Ministry of Science and Technology China, in November 2014.