ISSN 2278 – 0211 (Online)

Data Hiding in Encrypted H.264/AVC Video Stream

Shweta Patil
Student, Department of Electronics, Amrutvahini College, Sangamner, Maharashtra, India
S. S. Katariya
Associate Professor, Amrutvahini College, Sangamner, Maharashtra, India

Abstract:
Sometimes there is need to store a digital encrypted video for a security purpose. For the video encryption purpose we need to hide a data behind the video. There are many techniques to hide a data. In this paper, a scheme is proposed in which the data hiding is done in encrypted version directly which includes the following different parts i.e. H.264/AVC video encryption, after that data embedding and at last data extraction. The codeword substitution method is used for getting the better results we used the codewords of motion vector differences and the code words of the residual coefficients. After that we can again hide the additional data by the method of codeword substitution. At the receiver side we can extract the data from the encrypted version directly or else we can extract the data and the original video by using encryption key. The experimental results shows the system's efficiency and feasibility.

Keywords: *Encryption, Decryption, Data Hiding, MVD etc.*

1. Introduction

The basics of the cryptography is the encryption and decryption. Encryption is the process in which we hide the data in the host image using the encryption key. Decryption is the process in which we extract the hidden data. For extracting the hidden data we require the encryption key.

Now a day's cryptography has very importance because of the security purpose. There are many techniques for the data hiding:

1. Reversible Data Hiding
2. Irreversible Data Hiding

Encryption Algorithm are:

1. Motion Vector Differences (MVD)
2. Residual data
3. IPM

2. Literature Survey

B. Zhao, W. D. Kou, and H. Lipresent a paper which is based on the enhanced watermarking scheme and they proposed a scheme in which they increase the capacity of effective watermarking as compared to the Solankietal. SEC. Also they improved the scheme in terms of avoiding the additional overhead.

P. J. Zheng and J. W. Huang,gives the walsh-hadamard transform (WHT) implementation as well as its application for image watermarking. They used the method in which they implemented WHT with no quantization error. Also anyone can extract the watermark in encrypted domain as well as plain domain.

W. Puech, M. Chaumont, and O. Straussgives the method for reversible data hiding in encrypted images. They use the method by which we can embed any data in the image and then again we can decrypt that data. Also we get image without that hidden data. But the payload capacity is less as compared to the other techniques.

X. P. Zhangproposed method in which data hiding for the encrypted image can be done reversibly. In encryption method the uncompressed image can be embedded by stream cipher. We can decrypt the data using the encryption key and the original image can be recovered with the extracted embedded data.

W. Hong, T. S. Chen, and H. Y. Wu,gives the better results as compared to the previous paper. They proposed an improved data hiding method using side match. Using side match scheme the error rate of extracted bits can be decreased.

X. P. Zhangpropose a method in which the data hiding in encrypted images is done in separable reversible form. In this two separate phases are there. In first phase the encryption is done using encryption key. If receiver has both the encryption as well as data hiding key then hidden data and original image can be recovered.
K. D. Ma, W. M. Zhang, X. F. Zhao, N. Yu, and F. Li, eliminate the errors in the previous methods of the data hiding by vacating room after encryption. Previously after the encrypted image they vacate the room accordingly the data capacity. But due to this there are errors on data extraction. But this author suggests a method in which the data hiding in encrypted images by reserving the room before encryption so that they achieve real reversibility.

3. System Analysis

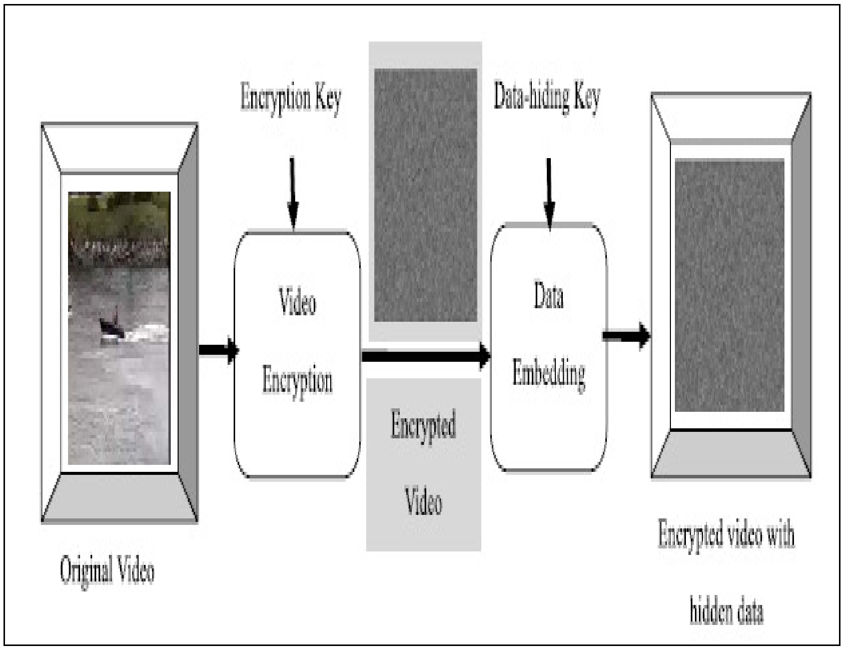


Figure 1

Following are the main steps till the video encryption process:

3.1. Original Video
At first the original video is given as the input to the system.

3.2. Video Encryption
For the requirement of the format compliance and the real time application video encryption needs a scheme that should be time efficient. But previous method was compressed whole video so they are not time efficient. In this we encrypt only selective parts of the video. For H.264/AVC the main selective 3 parts are motion vector differences (MVD), IPM and residual data. The codewords of the MVD, IPM and residual data are encrypted so we get the codewords of MVD, codewords of IPM and codewords of residual data.

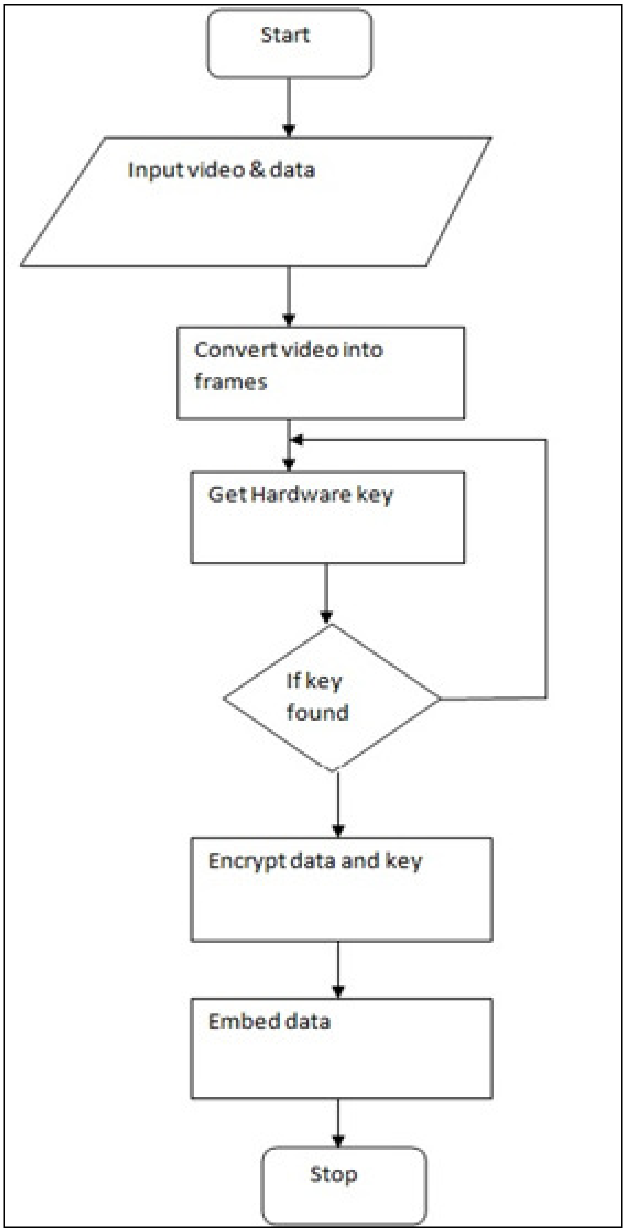


Figure 2: Encryption Algorithm

3.3. Data Embedding

Data embedding in this is done using codeword substitution. The proposed data can be embedded by substituting the eligible codewords. Codeword substitution method should satisfy the following 2 limitations: 1] After the codeword substitution this bit stream must be remaining unchanged. So that at decoder side it can be decoded by standard decoder. 2] Bit rate should remain unchanged after the codeword substitution.

3.4. Encryption Key

In the encryption scheme, the message which we have to hide is referred as plaintext. This plaintext is encrypted by encryption algorithm and generating cipher text and that can be readable only if decrypted. The pseudo-random encryption key is generated by algorithm and by using this key only decryption is possible.

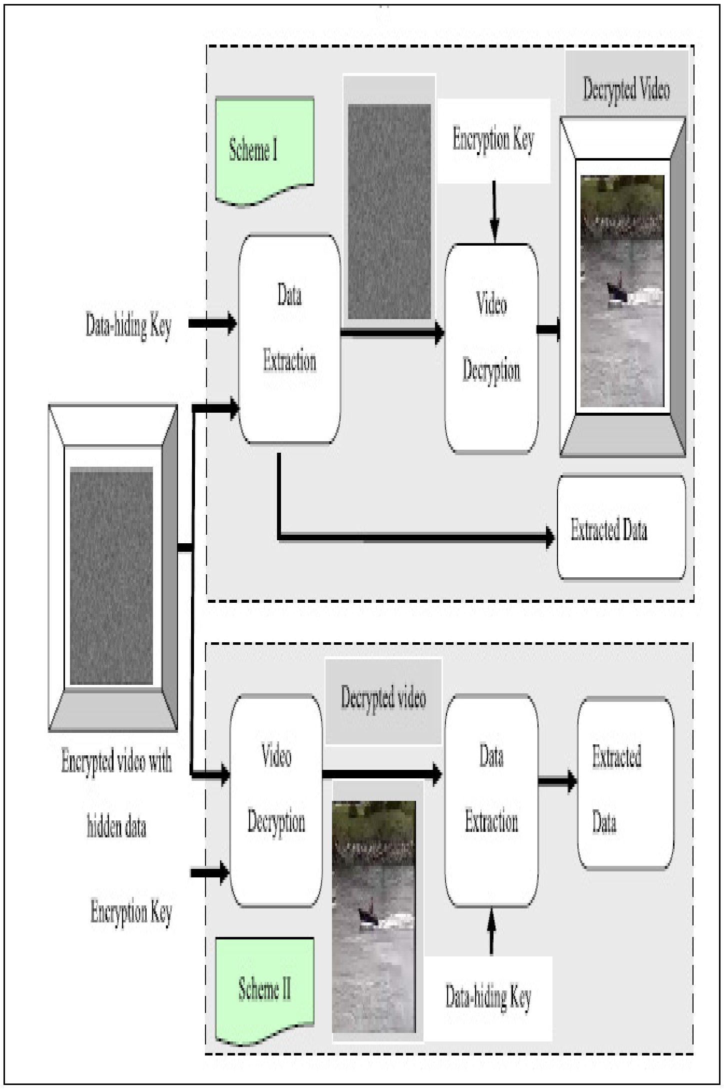


Figure 3: Block Diagram of Data encryption and decryption.

3.5. Data Extraction

Data extraction is done by two ways. Data can be extracted either in decrypted or encrypted domain. Based on this there are two schemes: scheme-I and scheme-II.

Scheme-I: Extraction in encrypted domain:

In this scheme, directly we can extract the hidden data if we have data hiding key. And if we want the original video then video can be extracted using video encryption key.

Scheme –II: Extraction in decrypted domain:

In this first we have to decrypt the video first and after that only data can be extracted from that decrypted video. For this first we have to required encryption key and then data hiding key to extract the hidden data.

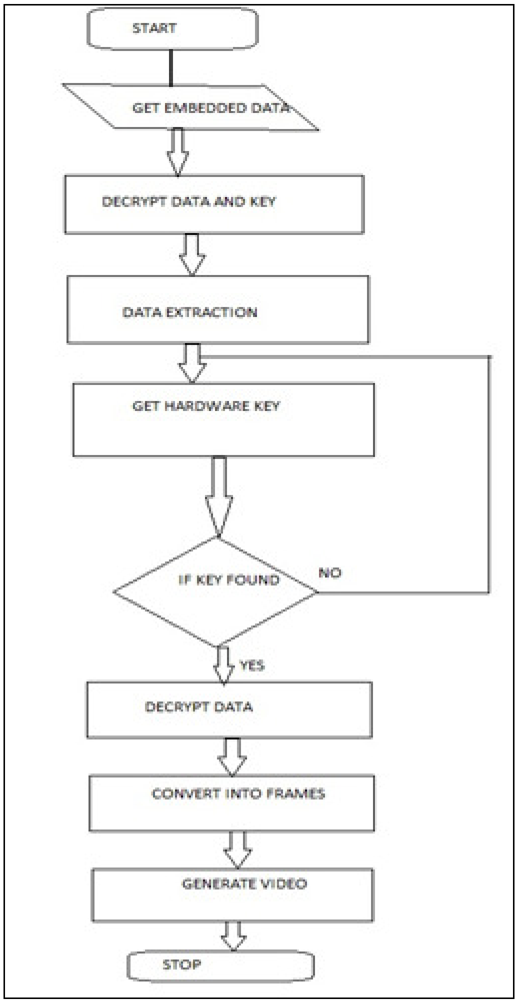


Figure 4: Decryption Algorithm

3.6. Decryption key

Decryption is the opposite process of encryption. For the secrete key encryption we required both encryption as well as decryption key. Private key encryption requires only encryption key.

4. Work Done

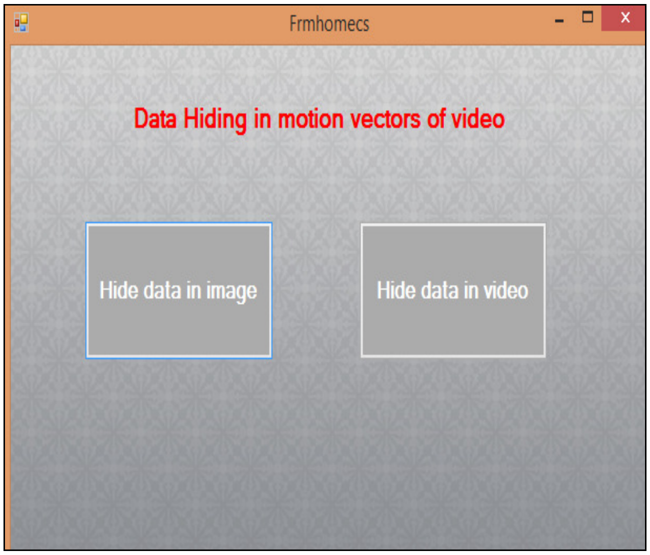
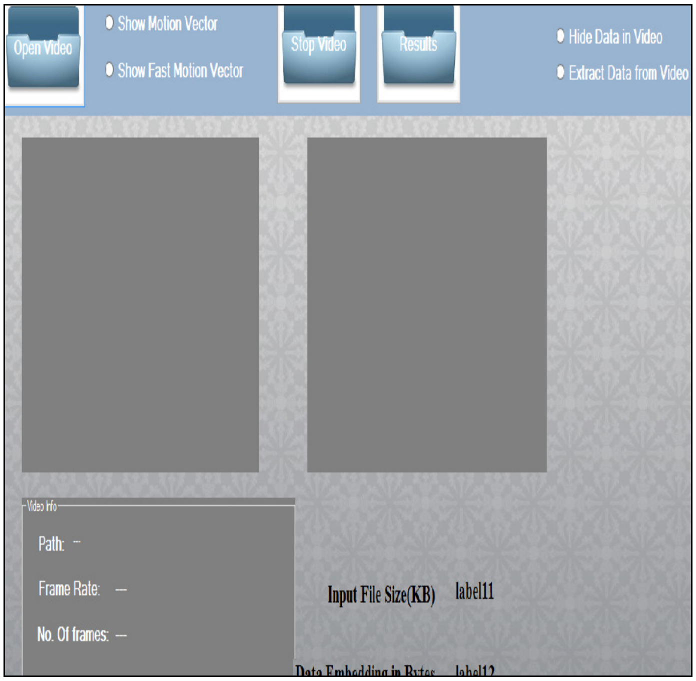


Figure 5: GUI of the data hiding model

After clicking on the hide data in video button we get the following window.



Path: --

Frame Rate: ---

No. Of frames: ---

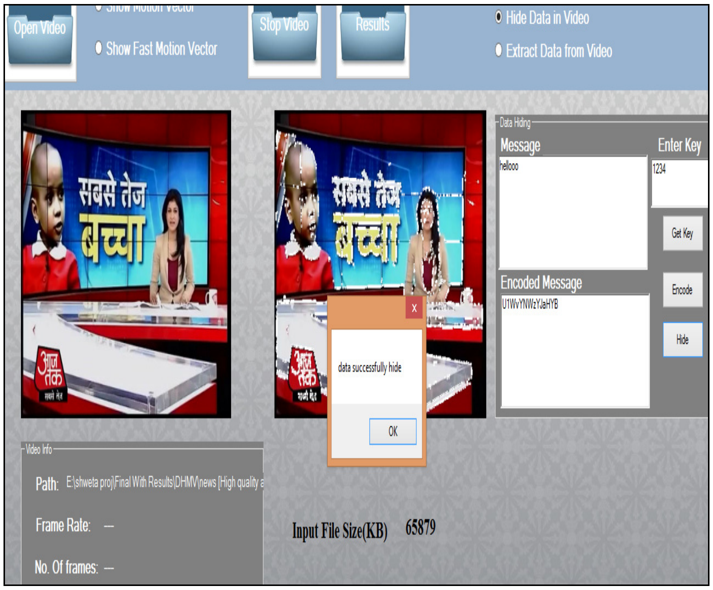
Input File Size(KB) label11

Data Embedding in Bytes label12

Figure 6: For data hide in video.

After clicking on the open video, we have to choose the video in which we have to hide data. This video is open in the first blank box. If we have to see the motion vectors of the video then click on the show motion vector button. We can see this video on second blank box. After seeing this we find the places in which we can hide the data so that the clarity of the original video will not lost.

Then click on the button hide data in video. After clicking on this we get the following window.



Message: hellooo

Enter Key: 1234

Encoded Message: U1WvYNWzYJaHYB

data successfully hide

Path: E:\shweta proj\Final With Results\DHMV\news [High quality a

Frame Rate: ---

No. Of frames: ---

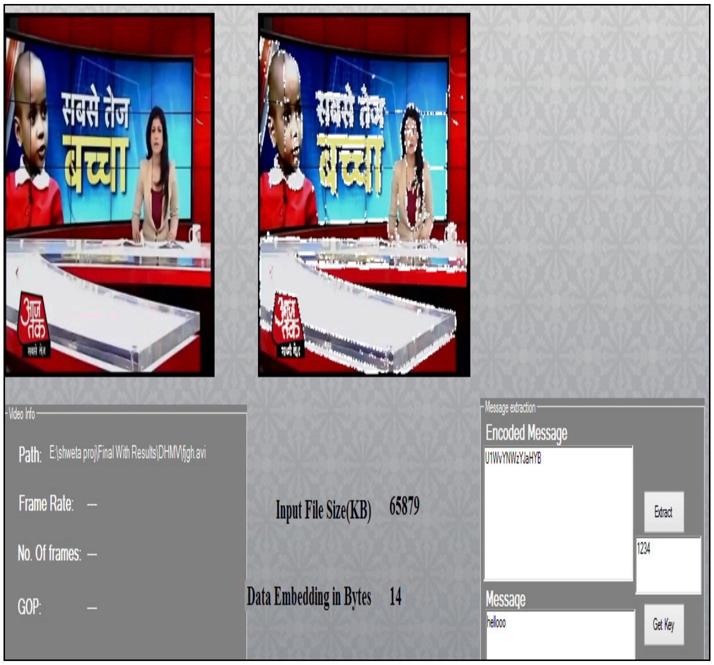
Input File Size(KB) 65879

Figure 7

We get the window as shown above. In that the secrete message which we have to hide is type in message box.

Then enter the encryption key in enter key box.

The click on the encode button will get the encoded message. Click on the hide button so that this message will hide and will get the small window showing the data successfully hide.



Path: E:\shweta proj\Final With Results\DHMV\fjgh.avi

Frame Rate: ---

No. Of frames: ---

GOP: ---

Input File Size(KB) 65879

Data Embedding in Bytes 14

Encoded Message: U1WvYNWzYJaHYB

1234

Message: hellooo

Figure 8

Above window showing the data extraction method.
Click on the data extraction button after that will get the above window and in that open the video in which we hide the data already.
Then click on the extract button so we get the encoded message and after that enter the encryption key.
If the encryption key is right then we get the secrete data successfully.

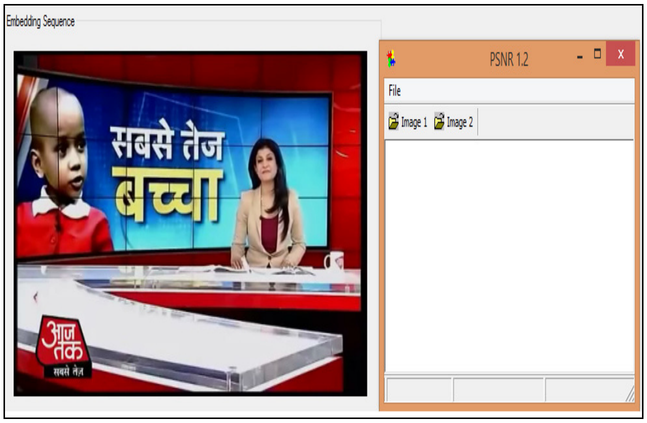


Figure 9

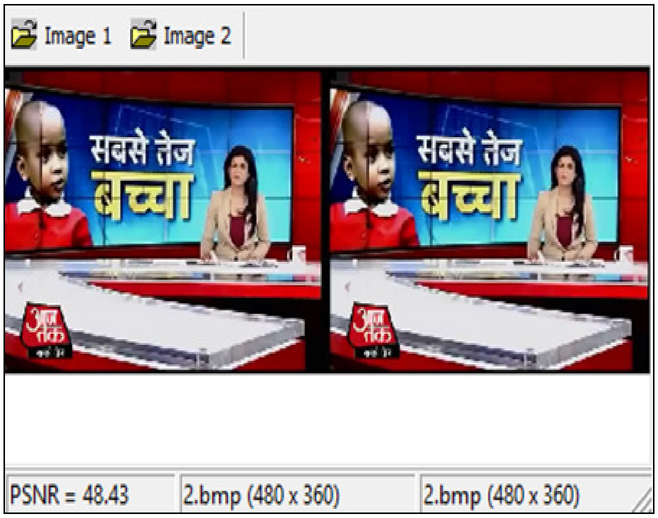
If click on the results button then we get the above window. In that if we open the original video and after that if we open the video in which data is hide then we get the frames of two different videos. Open that frames in the window shown above and we get the PSNR values result as shown in the below.

5. Results

PSNR VALUES		
Video name	Results Obtained	Existing Result
Table	48.25	38.44
Mobile	47.37	38.45
Hall	47.32	40.32
News	48.22	40.82

Table 1: Results based on the PSNR value

As shown in following figure the PSNR value calculation of frame of the original video and the frame of the encrypted video are calculated and the result table is made by calculating as shown in figure



PSNR = 48.43 | 2.bmp (480 x 360) | 2.bmp (480 x 360)

Figure 10

6. Future Scope

We try to improve the PSNR value for any videos. Also we plan to improve the accuracy of this system.

7. Conclusion

Data Hiding is a new topic drawing attention because of the privacy-preserving requirements from cloud data management.

The algorithm can preserve the bit-rate exactly even after encryption and data embedding, and is simple to implement as it is directly performed in the compressed and encrypted domain. The average time required for hiding the data is less. The PSNR value of this system is improved as compared to existing system

8. References

i. B. Zhao, W. D. Kou, and H. Li, “Effective watermarking scheme in the encrypted domain for buyer-seller watermarking protocol,” Inf. Sci.,vol. 180, no. 23, pp. 4672–4684, 2010.

ii. P. J. Zheng and J. W. Huang, “Walsh-Hadamard transform in the homomorphic encrypted domain and its application in image watermarking,”in Proc. 14th Inf. Hiding Conf., Berkeley, CA, USA, 2012, pp. 1–15.

iii. W. Puech, M. Chaumont, and O. Strauss, “A reversible data hiding method for encrypted images,” Proc. SPIE, vol. 6819,pp. 68191E-1–68191E-9, Jan. 2008.

iv. X. P. Zhang, “Reversible data hiding in encrypted image,” IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

v. W. Hong, T. S. Chen, and H. Y. Wu, “An improved reversible data hiding in encrypted images using side match,” IEEE Signal Process.Lett., vol. 19, no. 4, pp. 199–202, Apr. 2012.

vi. X. P. Zhang, “Separable reversible data hiding in encrypted image,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 2,pp. 826–832, Apr. 2012.

vii. K. D. Ma, W. M. Zhang, X. F. Zhao, N. Yu, and F. Li, “Reversible data hiding in encrypted images by reserving room before encryption,” IEEETrans. Inf. Forensics Security, vol. 8, no. 3, pp. 553–562, Mar. 2013.

viii. A. V. Subramanyam, S. Emmanuel, and M. S. Kankanhalli, “Robust watermarking of compressed and encrypted JPEG2000 images,” IEEETrans. Multimedia, vol. 14, no. 3, pp. 703–716, Jun. 2012.

ix. S. G. Lian, Z. X. Liu, and Z. Ren, “Commutative encryption and watermarking in video compression,” IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 6, pp. 774–778, Jun. 2007.

x. S. W. Park and S. U. Shin, “Combined scheme of encryption and watermarking in H.264/scalable video coding (SVC),” New Directions Intell. Interact. Multimedia, vol. 142, no. 1, pp. 351–361, 2008.

xi. T. Wiegand, G. J. Sullivan, G. Bjontegaard, and A. Luthra, “Overview Of the H.264/AVC video coding standard,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 7, pp. 560–576, Jul. 2003.