ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

Data Hiding Techniques in Video for Data Security

Abhijeet Kotwal[1], Kishor Shedge[2]

M.E Student, Department of Computer Engineering, SVIT, Nasik, India [1]

Assistant Professor, Department of Computer Engineering, SVIT, Nasik, India[2]

ABSTRACT:In this paper propose a data hiding in video stream for secure tramission. The proposed system contains Framing Divide the Video in Frames, Data Encoding Hide data in to selected Frame, Video Encryption Rebuild the video and encrypts the video, Data decoding Extract the data from encrypted video with high secure password and Decrypt the Video.

Digital video sometimes needs to be stored and processed in an encrypted format to maintain security and privacy. For the purpose of content notation and/or tampering detection, it is necessary to perform data hiding in these encrypted videos. In this way, data hiding in encrypted domain without decryption preserves the confidentiality of the content. In addition, it is more efficient without decryption followed by data hiding and re-encryption.

KEYWORDS: Encryption, Decryption, Data hider, Data Extraction, Privacy

I. INTRODUCTION

For sending and receiving any secrete data over the network many issues like Cyber-attack, cyber hacking, stealing this data may arise. This techniques provide the security to data hiding in video/ image That techniques which prevents this attacks on such confidential data is known as Encryption, The encryption encrypt the video with original data hide in that video and transfer with secure format , that it will be very hard to understand by third party person. Data adding and data hiding systems play an important role in addressing couple of major challenges that have arisen from the widespread distribution of multimedia content over digital communication networks. In particular, these systems are enabling technologies for enforcing and protecting copyrights, authenticating and detecting tampering of multimedia signals images. This techniques mostly used in medical imaginary, military imaginary or law forensic, in which department distortion of original cover is acceptable.

II. RELATED WORK

Robust "Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution" DawenXu, Rangding Wang, and Yun Q. Shi, Fellow Digital video sometimes needs to be stored and processed in an encrypted format to maintain security and privacy. For the purpose of content notation and/or tampering detection, it is necessary to perform data hiding in these encrypted videos. In this way, data hiding in encrypted domain without decryption preserves the confidentiality of the content. [1] "Watermarking of compressed and encrypted JPEG2000 images" by A. V. Subramanyam, S. Emmanuel, and M. S. Kankanhalli, Robust watermarking of compressed and encrypted JPEG2000 images, Digital asset management systems (DAMS) generally handle media data in a compressed and encrypted form. It is sometimes necessary to watermark these compressed encrypted media items in the compressedencrypted domain itself for tamper detection or ownership declaration or copyright management purposes[2]. "An efficient security system for CABAC bin-strings of H.264/SVC," M. N. Asghar and M. Ghanbari, An efficient security system for CABAC bin-strings of H.264/SVC, we propose a complete security system for H.264/scalable video coding (SVC) video codec and present a solution for the bitrate and format compliance roblems by careful selection of entropy coder syntax elements (bin-strings) for selective encryption (SE), and the problem of managing multiple layer encryption keys for scalable video distribution. [3] "Prediction mode modulated data-hiding algorithm for H.264/AVC" by D. W. Xu, R. D. Wang, and J. C. Wang, A new real-time watermarking technique based

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

on H.264/AVC video standard is proposed. The algorithm works in the compressed domain by embedding watermark bits into quantized DCT coefficients of 4×4 blocks of the I-frame during the Context-based Adaptive Variable Length Coding (CAVLC) process. [4] Data hiding in MPEG video files using multivariate regression and flexible macro block ordering T. Shanableh. This approach hides message bits by modulating the quantization scale of a constant bitrates video. A payload of one message bit per macro block is achieved. A second order multivariate regression is used to find an association between macro blocklevel feature variables and the values of a hidden message bit. The regression model is then used by the decoder to predict the values of the hidden message bits with very high prediction accuracy. [5]

III. PROPOSED SYSTEM

Data hiding in encrypted domain without decryption preserves the confidentiality of the content. In addition, it is more efficient without decryption followed by data hiding and re-encryption. In this paper, a novel scheme of data hiding directly in the encrypted version of H.264/AVC video stream is proposed, which includes the following three parts, i.e., H.264/AVC video encryption, data embedding, and data extraction. By analyzing the property of H.264/AVC codec, the codewords of intraprediction modes, the codewords of motion vector differences, and thecodewords of residual coefficients are encrypted with stream ciphers. Then, a data hider may embed additional data in the encrypted domain by using codeword substitution technique, without knowing the original video content. In order to adapt to differentapplication scenarios, data extraction can be done either in the encrypted domain or in the decrypted domain. Furthermore, video file size is strictly preserved even afterencryption and data embedding.Experimental results have demonstrated the feasibility and efficiency of the proposed scheme.

Modules:

1. Video processing
2. Encryption
3. Data Embedding
4. Decryption
5. Data Extraction

VIDEO PROCESSING:

Video frames from a continuous stream are processed one (or more) at a time. We can be calculated the resolution and image size. A video processor is combination of up conversion, de-interlacing, frame rate conversion, noise reduction, artefact removal, synchronization) and edge enhancement.

These frames also contain the audio information. Here the individual frames are in video format instead of being an image because image files cannot store audio information.

Brute-force attacks have become more sophisticated, groups of expert video analysts may sit together and analyse the entire video frame by frame and may bring together the original video. Hence there is a need to increase the security further to prevent such Brute force attacks.

ENCRYPTION:

With digital video transmission, encryption methodologies are needed that can protect digital video from attacks during transmission. Due to the huge size of digital videos, they are usually transmitted in compressed formats such as MPEG, or H.264/AVC. Thus, the encryption algorithms for digital video are usually working in the compressed domain. Several encryption algorithms to secure video streaming have been proposed. Most of them tried to optimize the encryption process with respect to the encryption speed, and display process. The reversible transformation of data from the original (the plaintext) to a difficult-to-interpret format (the cipher text)as a mechanism for protecting its confidentiality, integrity and sometimes its authenticity. Encryption uses an encryption algorithm and one or more encryption keys. See encryption algorithm and cryptography.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

DATA EMBEDDING:

Although few methods have been proposed to embed data into H.264/AVC bit stream directly, however, these methods cannot be implemented in the encrypteddomain. In the encrypted bit stream ofH.264/AVC, theproposed data embedding is accomplished by substituting eligible code words of Levelsthe bit stream after code word substituting must remain syntax compliance so that it can be decoded by standard decoder. Second, to keep the bit-rate unchanged, the substituted code word should have the same size as the original code word. Third, data hiding does cause visual degradation but the impact should be kept to minimum.

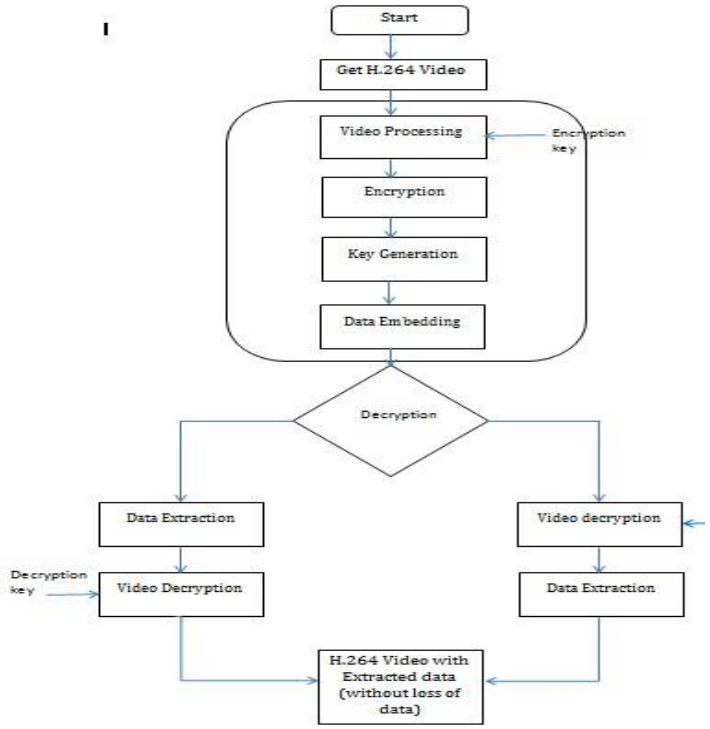


Fig. Flow Diagram

DECRYPTION:

Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords.

DATA EXTRACTION:

Embedding and extraction of the data are performed in encrypted domain. However, in some cases, users want to decrypt the video first and extract the hidden data from the decrypted video. For example, an authorized user, which owned the encryption key, received the encrypted video with hidden data. The received video can be decrypted using the encryption key. That is, the decrypted video still includes the hidden data, which can be used to trace the source of the data. Data extraction in decrypted domain is suitable for this the received encrypted video with hidden data is first pass through the decryption module. The whole process of decryption and data extraction is performing.

.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

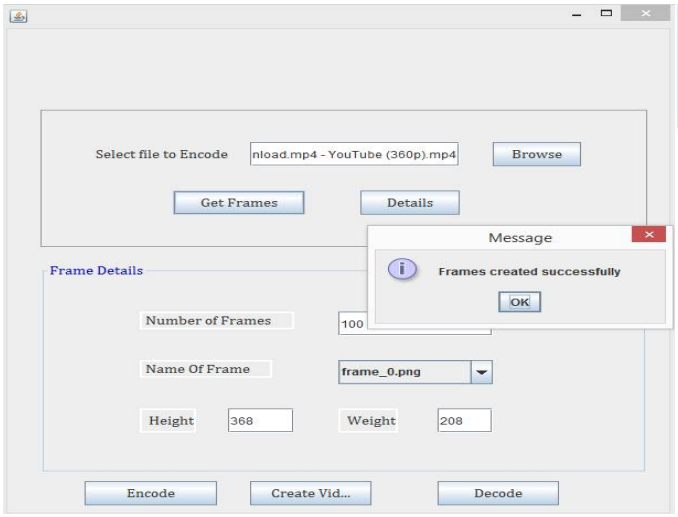
International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

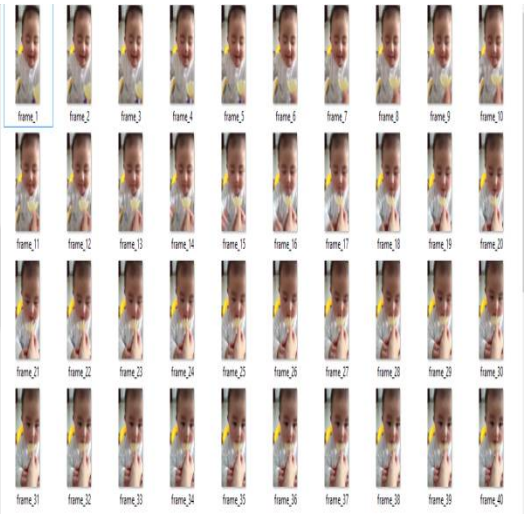
Vol. 5, Issue 11, November 2016

IV. EXPERIMENTAL RESULTS

Input: Select the input file (Video)
Framing: Divide the image in different frames.



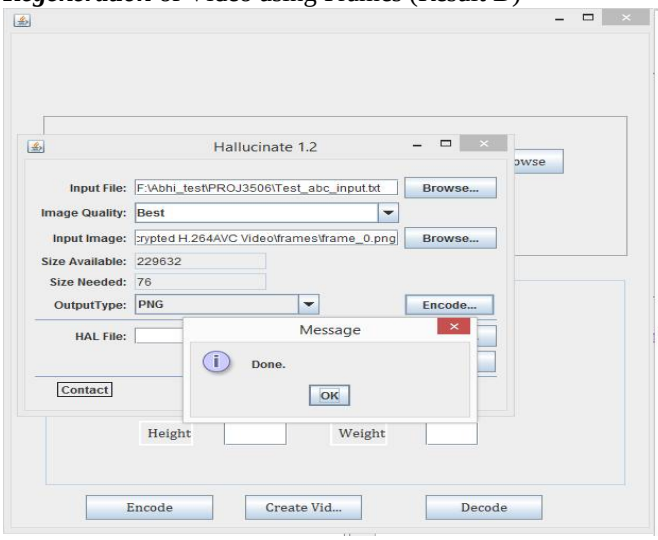
Result A .Input Video



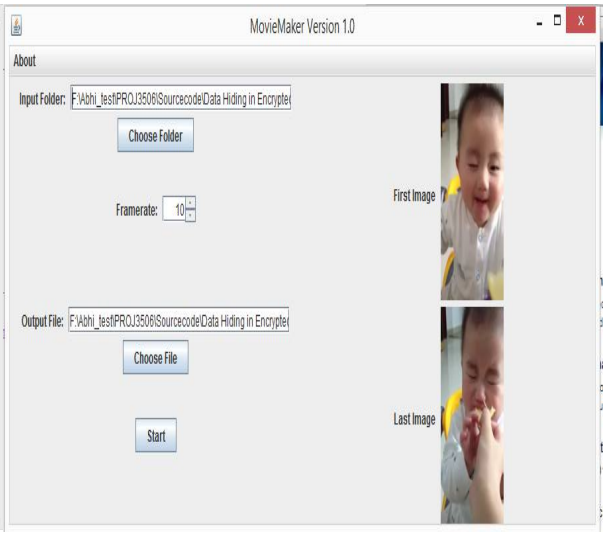
Result B. Frames

In first step we select the one video as aninput,after click on Get Frames , the framing operation divide the input video into different -different images. The frame is used to hide the data. In Frames we easily hide the data hence we make the frames.(refer fig A & B)

Data Encoding: Hide the data in to one frames (Result C)
Regeneration of Video using Frames (Result D)



Result C. Encode the Message



Result D .Create Video after Encoding Message in Frames

After making Frames we encode the message in to the selected frames. Encode the message module is used to hide the data in selected frames. We select the frames from folder then select the image Quality and then click on Encode.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

The Video making module rebuild the video after encode the data in to the frames , Making the video by selecting first frame and last frame.

Encryption: Encrypt the Video Using Secure password.

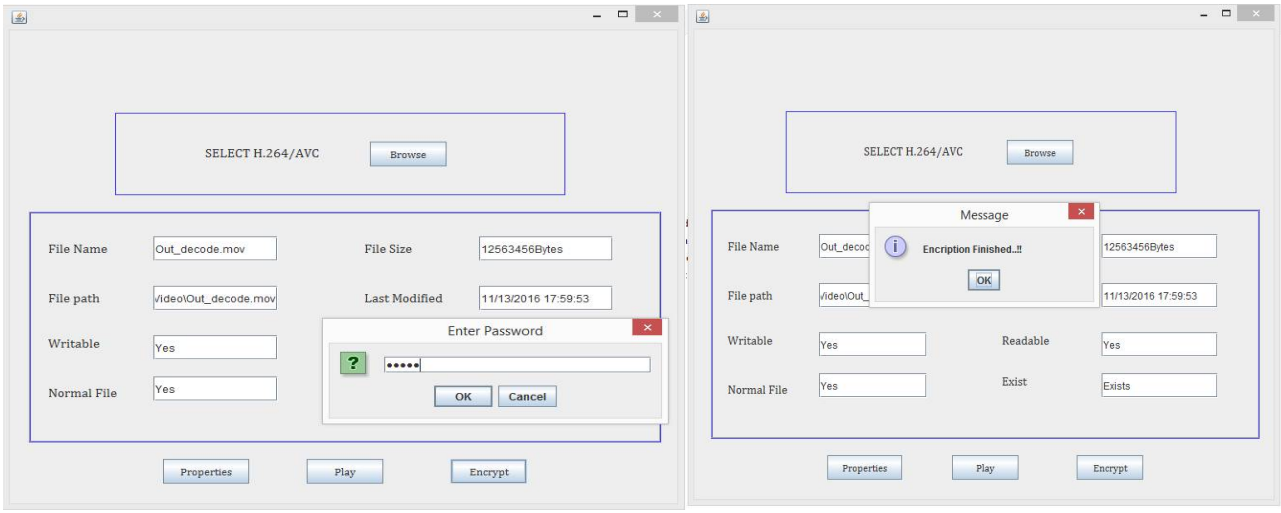
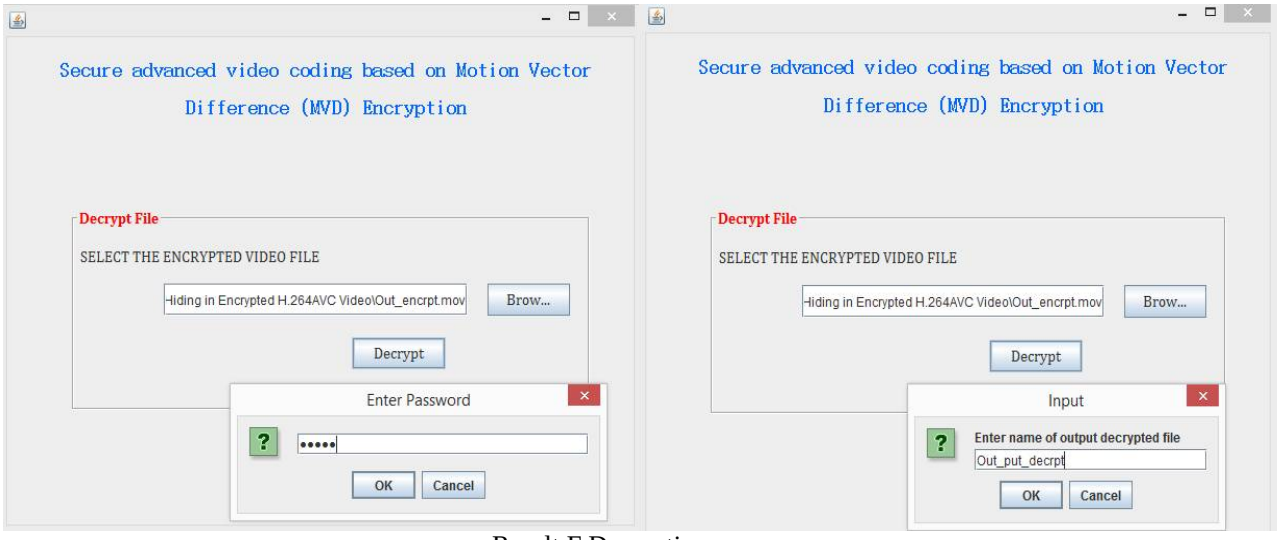


Fig. E Encrypt the video using secure password

Encryption is the most effective way to achieve data security. To read an encryptedfile, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text. Encryption is done with a secret password.

Decryption: Decrypt the Video after data Decode using Encryption Password and also provide a file name in which video is saved.



Result F Decryption process

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys.
Then we Decode the message from Decrypted Video.

Result G Before data Process Result H After data Process

V. CONCLUSION

Data hiding in encrypted media is a new topic that has started to draw attention because of the privacy-preserving requirements from cloud data management. In this paper, an algorithm to embed additional data in encrypted H.264/AVC bitstream is presented, which consists of video encryption, data embedding and data extraction phases. 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, i.e., it does not require decrypting or partial decompression of the video stream thus making it ideal for real-time video applications. The data-hider can embed additional data into the encrypted bitstream using codeword substituting, even though he does not know the original video content. Since data hiding is completed entirely in the encrypted domain, our method can preserve the confidentiality of the content completely. With an encrypted video containing hidden data, data extraction can be carried out either in encrypted or decrypted domain, which provides two different practical applications. Another advantage is that it is fully compliant with the H.264/AVC syntax. Experimental results have shown that the proposed encryption and data embedding scheme can preserve file-size, whereas the degradation in video quality caused by data hiding is quite small.

.

REFERENCES

[1] Data Hiding in Encrypted H.264/AVC Video Streams by Codeword SubstitutionDawenXu, RangingWang, and Yun Q. Shi, Fellow, IEEE TRANSACTIONS ONINFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 4, APRIL 2014
[2] K. D. Ma, W. M. Zhang, X. F. Zhao, N. Yu, and F. Li, Reversible data hid-ing in encrypted images by reserving room before encryption, IEEE Trans. Inf.Forensics Security, vol. 8, no. 3, pp. 553562, Mar. 2013.
[3] W. Hong, T. S. Chen, and H. Y. Wu, An improved reversible data hiding inencrypted images using side match, IEEE Signal Process. Lett., vol. 19, no. 4,pp. 199202, Apr. 2012.
[4] DawenXu, Rangding Wang, and Yun Q. Shi, Fellow, IEEE "Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 4, APRIL 2014.
[5] M. N. Asghar and M. Ghanbari, "An efficient security system for CABAC bin-strings of H.264/SVC," IEEE Trans. Circuits Syst. Video echnol. vol. 23, no. 3, pp. 425–437, Mar. 2013.
[6] X. P. Zhang, Separable reversible data hiding in encrypted image, IEEE Trans.Inf. Forensics Security, vol. 7, no. 2, pp. 826832, Apr. 2012.
[7] A. V. Subramanyam, S. Emmanuel, and M. S. Kankanhalli, Robust watermark-ing of compressed and encrypted JPEG2000 images, IEEE Trans. Multimedia,vol. 14, no. 3, pp. 703716, Jun. 2012.
[8] T. Stutz and A. Uhl, A survey of H.264 AVC/SVC encryption, IEEE Trans.Circuits Syst. Video Technol., vol. 22, no. 3, pp. 325339, Mar. 2012.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

[9] D. W. Xu and R. D. Wang, Watermarking in H.264/AVC compressed domainusingExp-Golomb code words mapping, Opt. Eng., vol. 50, no. 9, p. 097402,2011.
[11] D. W. Xu, R. D. Wang, and J. C. Wang, Prediction mode modulated data-hidingalgorithm for H.264/AVC, J. Real-Time Image Process., vol. 7, no. 4, pp. 205214,2012.24
[12] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. RamchandranOn compressing encrypted data, IEEE Trans. Signal Process., vol. 52, no. 10,pp. 29923006, Oct. 2004.
[13] http://ieeexplore.ieee.org/xpl/login.jsp?tp=arnumber=6086613url=http
[14] http://ieeexplore.ieee.org/xpl/login.jsp?tp=arnumber=6086613url=http
[15] http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6725633
[16] http://www.ijcttjournal.org/archives/ijctt-v22p108
[17] T. Kalker and F.M.Willems, Capacity bounds and code constructions forreversible data-hiding, in Proc. 14th Int. Conf. Digital Signal Processing(DSP2002), 2002, pp. 7176.
[18] Miscelaneous Gray Level Images [Online]. Available:http://decsai.ugr.es/cvg/dbimagenes/g512.php
[19]W. Hong, T. S. Chen, and H. Y. Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Process. Let. vol. 19, no. 4, pp. 199–202, Apr. 2012.
[20] D. K. Zou and J. A. Bloom, "H.264 stream replacement watermarking with CABAC encoding," in Proc. IEEE ICME, Singapore, Jul. 2010, pp. 117–121.