IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Volume-3, Issue-9 E-ISSN: 2347-2693

Data Hiding In Encrypted Video Stream By Code-Word Substitution

Sagar Hajare[1], Sujata Nikam[2], Kavita Vispute[3], Ravindra Bodke[4]

[1,2*,3,4]*Computer Engineering, SavitribaiPhule Pune University, India*

www.ijcseonline.org

Received: Sep/02/2015 Revised: Sep/11/2015 Accepted: Sep /27/2015 Accepted: Sep/30/2015

Abstract - Inspired by the SMVQ technique, this dissertation proposes a reversible data hiding based on VQ-compressed images.This scheme can completely recover the original VQ cover image from an embedded image after the embedded message is extracted. Compared to the SMVQ technique that is very time consuming to set up a state codebook and then search the nearest codeword, the proposed scheme employs block match coding (BMC) to reduce the complexity and preserve a satisfactory embedding capacity. The main problems in the former works are low embedding capacities, low embedding rates, high complexities, or high bit rates. To improve these problems, the proposed scheme applies the BMC prediction to encode indices, and thus can obtain a higher embedding capacity, higher embedding rate, higher processing efficiency, and lower bit rate simultaneously. This chapter describes the method used for data hiding that is vector quantization and its type side match vector quantization in detail.

Keyword: Data hiding, encrypted domain, H.264/AVC, codeword substituting

I. INTRODUTION

The widespread use of thenet offers nice convenience to the transmission of anoutsizequantityofknowledge over networks, thatare open however insecure channels, exposing severalpersonal and secret knowledge to dangerous things. Today, makingcertain that info transmission over thenet remains safe and secure has become veryvital. Tostay the unauthorized user farawayfrom the transmission info, arrange of techniques are proposed; knowledgeactivity is oneineveryof the protecting techniques in knowledge security.

All the ways existing untilcurrentlyattemptto vacate space from the encrypted pictures directly. However, since the entropy of encrypted pictures has been maximized, these techniques will solelydeliverthegoodstiny payloads or generate marked image with poor quality forbig payload andeveryone of them are subject to some error rates on knowledge extraction and/or image restoration. Though the ways in will eliminate errors by error correcting codes, the pure payloads aregoingtobeany consumed. Inspired by the SMVQ technique and vacating area once cryptography (VRAE) technique, this piece of writing proposes a reversible information activity supported reserving area before cryptography (RRBE) technique and VQ-compressed footage. This theme can absolutely recover the initial VQ cowl image from Associate in Nursing embedded image once the embedded message is extracted. Compared to the SMVQ technique that is very time intense to line up a state codebook then search the nearest codeword, the planned theme employs block match cryptography (BMC) to cut back the standard and preserve a satisfactory embedding capability. the foremost problems inside the previous works [2] are low embedding capacities, low embedding rates, high complexities, or high bit rates. to reinforce these problems, the planned theme applies the BMC prediction to cypher indices, and thus can acquire succeeding embedding capability, higher embedding rate, higher method efficiency, and lower bit rate at an equivalent time.

A. System Methodology

- DATA HIDING TECHNIQUES IN STILL IMAGE
- DATA HIDING TECHNIQUES IN AUDIO SIGNALS
- DATA HIDING TECHNIQUES IN VIDEO SEQUENCES
- REVERSIBLE DATA HIDINGTECHNIQUES

B. Problem Definition

Due to exponential increase of size of therefore known as multimedia system files in recent years attributable to the substantial increase of reasonable memory storage on one hand and also the wide unfold of World Wide net (www) on the opposite hand, the requirement for the economical tool to retrieve the pictures from the massive information base becomes crucial. This motivates the in depth analysis into image retrieval systems. From the historical perspective, the sooner image retrieval systems ar rather text-based with the thrust from management community since the pictures ar needed to be annotated and indexed consequently. but with the substantial increase of the scale of pictures in addition as size of image information, the task of user-based annotation becomes terribly cumbersome and at some extent subjective and thereby, incomplete because the text typically fails to convey the made structure of pictures. to beat these difficulties this motivates the analysis into what's referred as information concealment and compress the image exploitation vector quantization so tiny information is needed. This chapter reviews the all existing approaches for information concealment. It summarizes the analysis work dole out by completely different researchers for information concealment, the techniques employed by them and also the results of the analysis work. the main points are explained in following sections.

II.LITERATURE SURVEY

In general, information activity techniques will be classified into 2 classes, namely, reversible information activity schemes and irreversible information activity schemes. For irreversible information activity schemes, solely secret information will be extracted and no restoration of canopy pictures is offered. Conversely, reversible information activity schemes will extract the key information and recover the initial cowl pictures at the same time. additionally, 2 styles of strategies, index-modifying and side-match VQ (SMVQ), square measure commonly accustomed introduce secret information into a VQ-compressed image.Many researchers have developed totally different index-modifyininformation activity techniques and aspect match information activity techniques (SMVQ). The analysis disbursed by totally different researchers for information activity is explained in remainder of this chapter.

For associate degree index-modifying information activity, Jo associate degreed Kim [2]in year 2002first planned an irreversible index-modifying data-hidingscheme .This theme was straightforward to understand however because it was associate degree irreversible information activity theme that the original cowl image can't be restoredand the information activity capability was rathersmall.

For associate degree SMVQ-based information activity, Shieet al. [8] in year 2006 developedan adaptive information activity supported a VQ-compressed image,in which image blocks square measure classified into embeddable andun-embeddable blocks supported the variances and side-match distortions (SMDs). Though this theme will yield a high embedding capability, the standard of the reconstructed image reduces because the amount of secret information will increase. Additionally, this theme may be a case of the irreversible data activity.

Principle and sculptor [4] within the year 2006 extended the theme planned by Yangtze River et al. By dividing the VQ codebook into 2ds clusters, and 1/2 that aroused to introduce secret information, wherever denotes the scale of the secret information embedded into every VQ index. Within the theme, both the VQ and SMVQ square measure applied to cover secret information, and so higher embedding capability and lower bit rate will be yield. Moreover, it's a reversible data-hiding theme.

In year 2007, Yangtze River et al. [5] developed another index-modify in data-hiding theme with recovery capability. Indicators are added before of the foremost encoded indices and solely 2-clusters will be accustomed hide secret information in their 2-bit hiding scheme, leading to low embedding capability and high bit rate(BR). In general, high embedding capability will be achieved with SMVQ primarily based data-hiding schemes, within which a state codebook is employed to code every index, however they need more encoding time than that of the index-modifying techniques.

In year 2007C. C. Chang, Y. P. Hsieh, and C. Y. Lin [5], planned a reversible information activity theme for embedding secret information inVQ-compressed codes supported the de-clustering strategy is proposed. The theme is able to do higher embedding capacity but needs several computations to de-cluster a codebook into range of teams.

C. C. Chang, G. M. Chen, and M. H. Lin [9], planned a method within which SOCand original index worth square measure utilized to cover secret bit 0or one. Though the low capability is that the major shortcoming of this theme, the initial cowl image will be restored completely.

III.PROPOSED SYSTEM

In this section, a unique theme of information concealing within the encrypted version of H.264/AVC videos is given, which incorporates 3 components, i.e., H.264/AVC video coding, information embedding and information extraction. The content owner encrypts the first H.264/AVC video stream mistreatment customary stream ciphers with coding keys to provide AN encrypted video stream. Then, the data-hider (e.g., a cloud server) will enter the extra information into the encrypted video stream by mistreatment code-word subbing methodology, while not knowing the first video content. At the receiver finish, the hidden information extraction will be accomplished either in encrypted or in decrypted version. The diagram of the planned framework is shown in Fig. 1, wherever the coding and information embedding are delineated partly (a), and also the information extraction and video cryptography are shown partly (b).

A. Encryption of H.264/AVC Video Stream

In this paper, an H.264/AVC video encoding theme with sensible performance together with security, efficiency, and format compliance is projected. By analyzing the property of H.264/AVC codec, 3 sensitive components (i.e., IPMs, MVDs, and residual coefficients) are encrypted with stream ciphers. Compared with [5], the project dencoding algorithmic rule is performed not throughoutH.264/AVC codinghowever within the H.264/AVC compressed domain. *1) Intra-Prediction Mode (IPM) Encryption*: in line with H.264/AVC normal, the subsequent four kinds of intra secret writing are supported, that aredenoted as Intra_4 ×4, Intra_16×16, Intra-chrome, and I_PCM [12]. Here, IPMs within the Intra_4×4 and Intra_16 ×16 blocks are chosen to encipher. Four intra prediction modes (IPMs) are accessible within the Intra_16 ×16. The IPM for Intra_16 ×16 blocks is laid out in the mb_type (macro block type) field that additionally specifies different parameters regarding this block like coded block pattern (CBP).

In H.264/AVC, each Intra_4 ×4 luminance blocks is predicted from its spatially neighboring samples. Specifically, H.264/AVC offers nine prediction modes (0-8) for Intra_4×4 luminance blocks. The choice of prediction mode for each Intra_4×4 luminance block must be signalled to the decoder and this could potentially require a large number of bits. To efficiently compress the prediction-mode data, the predictive coding technique is applied to signal prediction modes.

2) Motion Vector distinction (MVD) Encryption: so asto safeguard each texture data and motion data, not solely the IPMs however additionally the motion vectors ought to be encrypted. In H.264/AVC, motion vector prediction is more performed on the motion vectors that yield MVD. In H.264/AVC baseline profile, Exp-Golomb entropy secret writing[9] is employed to encipher MVD. The code-word of Exp-Golombis built as [M zeros] [I NFO], wherever NFO is associate degree M-bit field carrying data.

3) Residual Data Encryption: so asto stay high security, another kind of sensitive knowledge, i.e., the residual knowledge in each I-frames and P-frames ought to be encrypted. During this section, a unique methodology for encrypting the residual knowledge supported the characteristics of code-word is given intimately.

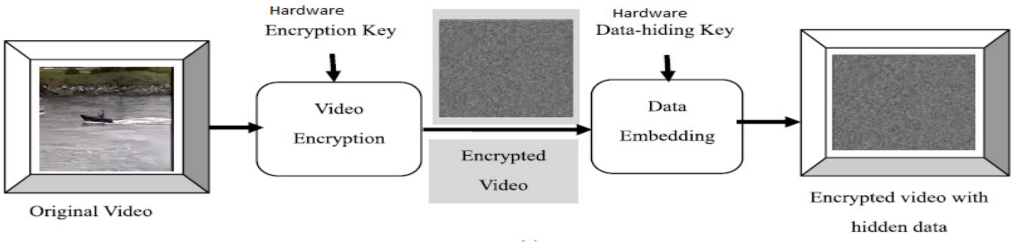

Fig: Data Embedding

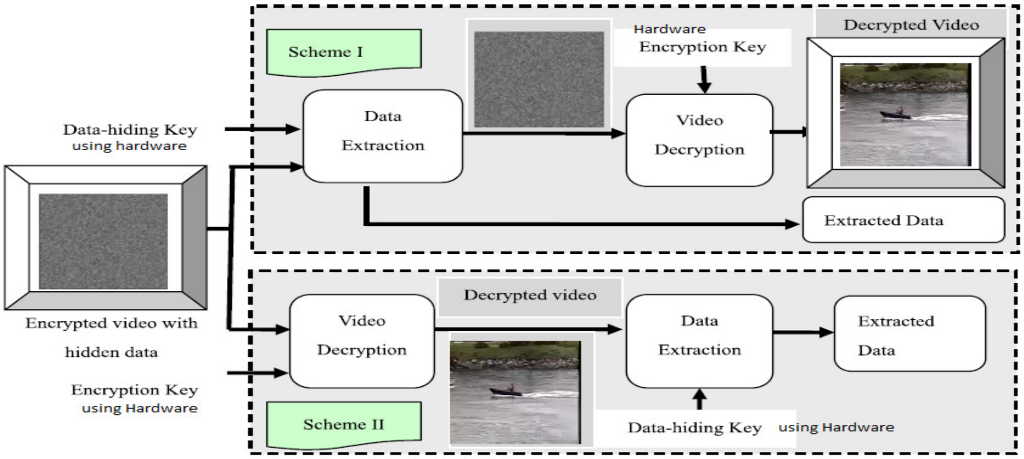

Fig: Data Extraction

B. Data Embedding

Although few ways are projected to implant knowledge into H.264/AVC bit stream directly [3]–[2], however, these ways cannot be forced within the encrypted domain. Within the encrypted bit stream of H.264/AVC, the projected knowledge embedding is accomplished by work eligible codeword's of Levels. Since the sign of Levels are encrypted, knowledge concealmentmustn'thave an effect on the sign of Levels. Besides, the codeword's substitution ought to satisfy the subsequent3 limitations. First, the bit stream oncecode word work shouldstay syntax compliance so it may be decoded by commonplace decoder. Second, to stay the bit-ra1) data once video decoding must be invisible to a personality's observer.

C. Data Extraction

In this theme, the hidden knowledge will be extracted either in encrypted or decrypted domain, as shown in Fig. 1(b). Knowledge extraction method is quicksand straightforward. We'll initial discuss the extraction in encrypted domain followed by decrypted domain.

Scheme I: Encrypted Domain Extraction. To protect privacy, an information manager (e.g., cloud server) might solely get access to the knowledge activity key and need to manipulate data in encrypted domain. Knowledge extraction in encrypted domain guarantees the practicability of our theme during this case. In encrypted domain, as shown in Fig. 1(b), encrypted video with hidden knowledge is directly sent to the information extraction module, and also the extraction method is given as follows.

Step1: The codeword's of Levels are first of all known by parsing the encrypted bit stream.
Step2: If the code word belongs to code house C0, the extracted information bit is "0". If the code word belongs to code house C1, the extracted informationbitis"1".
Step3: in line with the info activity key, identical chaotic pseudo-random sequence P that was employed in the embedding method will be generated. Then the extracted bit sequence can be decrypted by mistreatment P to induce the first furtherdata. Since the total method is entirely operated in encrypted domain, it effectively avoids the outf low of original
video content.

2) Scheme II: Decrypted Domain Extraction. In scheme I, each embedding and extraction of the info area unit performed in encrypted domain. However, in some cases, users need to rewrite the video 1stand extract the hidden knowledge from the decrypted video. For instance, a licensed user, thatowned the coding key, received the encrypted video with hidden knowledge. The received video will be decrypted victimization the coding key. That is, the decrypted video still includes the hidden knowledge, which may be wont to trace the supply of the info. Knowledge extraction in decrypted domain is appropriate for this case.

IV.CONCLUSION

Data concealment in encrypted media could be a new topic that has began to draw attention thanks to the privacy-preserving needs from cloud knowledge management. During this paper, associate degree rule to engraft extra knowledge in encrypted H.264/AVC bit stream is given, that consists of video secret writing, knowledge embedding and knowledge extraction phases. The rule will preserve the bit-rate precisely even when secret writing and knowledge embedding, and is straightforward to implement because it is directly performed within the compressed and encrypted domain, i.e., it doesn't need decrypting or partial decompression of the video stream therefore creating it ideal for time period video applications. The knowledge-hider will engraft extra data into the encrypted bit stream mistreatment codeword subbing, albeit he doesn't understand the initial video content. Since knowledge concealment is completed entirely within the encrypted domain, our technique can preserve the confidentiality of the content fully. With associate degree encrypted video containing hidden knowledge, knowledge extraction may be meted out either in encrypted or decrypted domain that provides 2 totally different sensible applications. Another advantage is that it's absolutely compliant with the H.264/AVC syntax. Experimental results have shown that the planned secret writing and knowledge embedding theme will preserve file-size, whereas the degradation in video quality caused by knowledge concealment is kind of little.

REFERENCES

[1] DawenXu, Rangding Wang, and Yun Q. Shi, *Fellow,*"Data Hiding in Encrypted H.264/AVC Video Streams by CodewordSubstitution"IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 4, APRIL **2014**.

[2] D. W. Xu and R. D. Wang, "Watermarking in H.264/AVC compressed domain using Exp-Golomb code words mapping," *Opt. Eng.*, vol. 50, no. 9, p. 097402, **2011**.

[3] 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.

[4] C. C. Chang, W. C. Wu, and Y. C. Hu, "Lossless recovery of a VQ index table with embedded secret data," *J. Visual Commun. Image Representation*, vol. 18, no. 3, pp. 207–216, **2007**.

[5] C. C. Chang, Y. P. Hsieh, and C. Y. Lin, "Lossless data embedding with high embedding capacity based on de-clustering for VQ-compresse dcodes," *IEEE Trans. Informat. Forensics Security*, vol. 2, no. 3,pp. 341–349, Sep. **2007**.

[6] S. C. Shie, S. D. Lin, and C. M. Fang, "Adaptive data hiding based on SMVQprediction,"*IEICE Trans. Informat. Syst.*, vol. E89-D, no. 1, pp.358–362, **2006**.

[7] C. C. Chang and C. Y. Lin, "Reversible steganography for VQ compressed images using side matching and relocation," *IEEE Trans. Inform. Forensics Security*, vol. 1, no. 4, pp. 493–501, Dec. **2006**.

[8] S. G. Lian, Z. X. Liu, Z. Ren, and H. L. Wang, "Secure advanced video coding based on selective encryption algorithms," *IEEE Trans.Consumer Electron.*, vol. 52, no. 2, pp. 621–629, May **2006**.

[9] C. C. Chang, G. M. Chen, and M. H. Lin, "Information hiding basedon search-order coding for VQ indices," *Pattern Recognnit. Lett.*, vol.25, no. 11, pp. 1253–1261, **2004**.

[10] J. Tian, "Reversible data embedding using a difference expansion," *IEEETrans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug.**2003**.

[11] I. E. G. Richardson, *H.264 and MPEG-4 Video Compression: VideoCoding for Next Generation Multimedia*. Hoboken, NJ, USA: Wiley,**2003**.