International Journal of Science Engineering and Advance Technology

Review on Data Hiding Schemes into Multimedia Data

Ashwini G. Kamble , Prof. Nikita J. Kulkarni.
Computer Engineering
ZES's DCOER, Pune.
ashwinikamble1992@gmail.com
nikita.kulkarni@zealeducation.com

Abstract— In this period of internet, Multimedia data security is crucial issue because there are many cases of illegal production and redistribution through the Internet. Data hiding and encryption algorithms can be used for Security and protection of multimedia data. Video encryption is new area of research for researchers. Data hiding in encrypted videos is important to conquer the aim of content annotation, copy right protection, access control and/or tapering detection. This survey summarizes the latest research results on video encryption with a special focus on applicability and on the most widely-deployed video format H.264 including advanced video Coding.

***Index Terms*—Data hiding, Image encryption, Video encryption, H.264/AVC, H.264 Encoder.**

I. INTRODUCTION

The mounting reputation of digital media has concern over security related issues. As the internet technology is developing with a great speed media data like images, audios or videos are used more and more in day to day life. Internet technology made possible easy to transfer of such data through media but also easily copy data from media. Thus the protection of media is the main issue of discussion. To protect media data, two ways are proposed, media encryption and media watermarking.

Media data is encrypted into incomprehensible ones with ciphers in media encryption. Contents confidentiality is protected by media encryption. In case of video encryption, Encrypted videos are difficult to understand. Video encryption is different from text or binary data encryption. The approach used for video encryption should be time efficient and format grievance. So that it can meet real time applications requirements. Using traditional ciphers [8], such as data encryption standard (DES) or advanced encryption standard (AES), we cannot encode the video data completely because the computational cost is very high. Only fraction of data is encrypted in partial encryption and it improves the efficiency. Some approaches are stated to encode the videos encoded with advanced video coding (H.264/AVC). The approach stated in [9] scrambles the intra-prediction mode (IPM) of intra-macro block.

In media watermarking some special information is embedded into a video. It protects media data's identification. There are also types of watermarking, visible watermarking invisible watermarking. Imperceptibility and robustness are required for invisible watermarking.

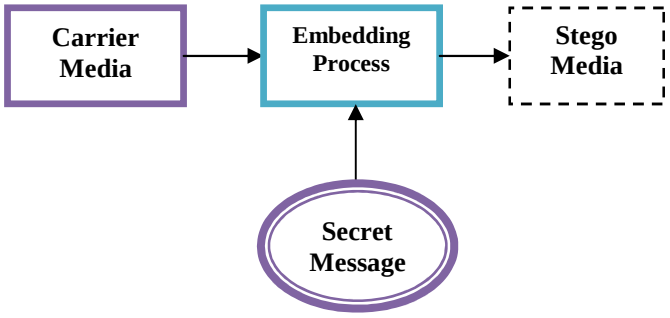

Fig.1: Data Hiding Method

Video processing techniques typically can be adapted from image and audio processing techniques, but the rich information and large data volume of video brings unique challenges and also attracts active research. Problem formulation is one of the challenges. There are three main parameters to estimate sheltered video processing technique [1]**:**

- Security: Sometimes in media have private data then protect or securely transmission those data for security, i.e., how much information is revealed from the encrypted video and its auxiliary features.
- Performance: Three processing tasks performed only on the encrypted data not based on Host media data means oppose to plaintext data. Performance evaluates the accuracy of those processing task.
- Complexity: At user side performing computational complexity of preprocessing then form of Auxiliary features used to secularly prevent the information leak. Minimize

communicational cost for computing the secure video processing.

Clear security definition and objectives need to be developed for designing secure video processing techniques. Information leakage is minimized by considering multimedia data as ordinary data and using cryptographic ciphers like RSA and AES, but practically it is found to be inefficient for video processing applications.

Next challenge is video processing tasks. Application considered is where user searches his private data by means of video queries but keeps the query and database secret from the server. In [2, 3] same problem of content-based search over encrypted image database is considered.

The concept is to encrypt visual features or search indexes from images in a distance preserving fashion, which in turn gives permission to the server to compare the similarity of encrypted images directly in the encrypted database without additional communication with the user.

Another interesting processing task is to automatically assign tags, such as beaches, portrait, indoor, to videos and classify the collection into different categories. Privacy-preserving video classification and annotation is desirable because it can better organize and present the private video collection for the users.

II. Literature Review

In[4]Watermarking is the process that embeds data called watermark or tag or label into multimedia object may be an image or audio or video such that watermark can be detected or extracted later to make an assertion about the object. Watermarking technique is developed for authentication; copyright protection and multimedia distribution a seller normally add a watermark or tag in host multimedia content to uniquely identify a buyer. If the seller finds an unauthorized copy, the added watermark traces the traitor's identity. But there is sometimes occurs framing and repudiation issue. watermark image is encrypted by a buyer's public key, and it is not exposed to the seller. This scheme increases effective watermarking capacity, removes the additional overhead, an inherent flaw that watermarking capacity depends on the probability distribution of input watermark sequence. New watermarking scheme with flexible watermarking capacity using security requirements of buyer–seller watermarking protocols is discussed in [4].

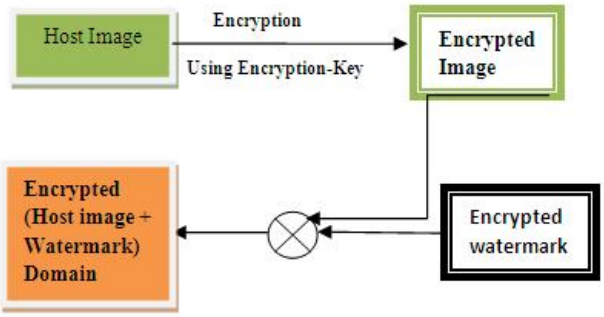

Fig.2. Structure of Watermark embeds into the encrypted domain

In [5], a reversible data hiding algorithm for encrypted image. In reversible data hiding method firstly host image encrypt using secret key then data hider can hide data into encrypted host image using data hiding key, after decrypt an marked image rebuild the host image with visual quality by extraction of hidden data. The main analysis is during decryption step extraction of hidden data done from marked encrypted image. Encryption or data hiding algorithms are mostly used for protection of multimedia data. The data compression is necessary to decrease the transmission time. A research is on going to combine the three steps compression, encryption and data hiding. In this method use advanced Encryption Standard algorithm for encrypt the Host image .There is one important challenge is to embed data in encrypted images. Embedding data capacity for 16 pixels is 1 bit only. Recent reversible data hiding methods with high capacity but these methods are not compatible with encrypted images.

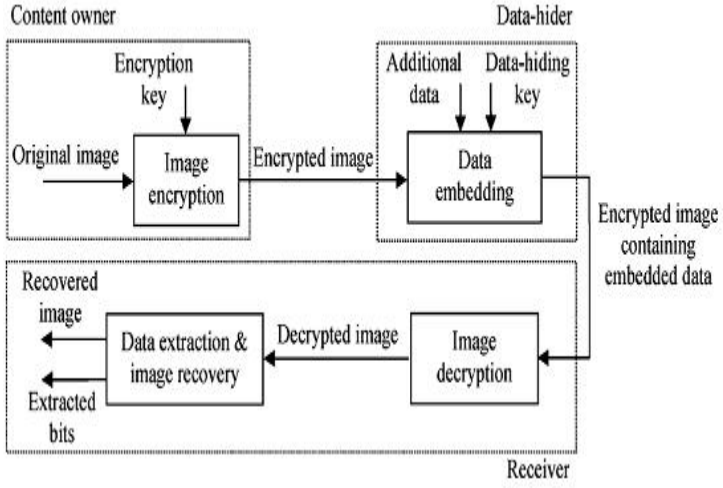

Fig. 3: Reversible data hiding [6]

In [10], data hiding is the process of inserting secret information into Host media (video) for copyright protection and secret communication. After embedding secret data into compressed video stream, some distortion

occurs in compression video. There are many data hiding approaches in compressed MPEG video. At First approach quantization scale modulation hides one message bit per macro block. They firstly message convert into a binary bits stream. During MPEG encoding of individual macro-block, quantization scale of constant bit rate (CBR) video is either increment or decrement based on underlying message bit. The decoder use Multivariate regression to predict the message bit hidden in a given macro blocks according its level feature variable with high prediction accuracy. At second approach is flexible macro-block ordering used to allocate macro block arbitrary slice groups according to hide message bit. This approach works for CBR and VBR coding .They achieves maximum payload means three message bits per macro block and high quality of original video after extraction of secret data from compressed video.

In [11], with highly development of network technology and multimedia data like image, video are widely used. The security of sensitive videos such as digital television, video surveillance needs to be protected before transmission. RSA, AES, DES various encryption algorithms are not easy to use directly in video encryption.AVC encoding/decoding process is time-efficient requires encryption/decryption process also with time efficient. In [11] a secure AVC coding approach is stated which is based on some partial encryption algorithms. Sensitive data such as intra-prediction mode, residue data and motion vector are partially encrypted during AVC encoding. The partial-encryption scheme is simple and easy to use in AVC stream but one problem is how to select the sensitive data to be encrypted. First sensitive data Intra-prediction mode is encrypt using Exp-Golomb entropy coding. Then, second is the intra-macroblock DCs are encrypted based on context based adaptive variable length coding (CAVLC) encryption algorithm (CEA)using stream cipher and third is the intra-macro block's AC's and inter-macro block's MVDs are encrypted by Sign encryption algorithm(SEA)using random-Feedback Stream cipher. This approach is very secure. It keeps the not only quality of video but also secure against some attacks like as known plaintext attack. By reducing the encrypted data volumes, it obtains high time efficiency.

In [12] H.264 coding standard has been widely used in multiple multimedia applications, Video encryption is becoming increasingly important as multimedia applications gain more and more popularity. Various encryption algorithms have Security, time efficiency, format compliance, and error robustness features but they are focus on the H.264 video coding standard, encryption algorithms based on the intra prediction mode have been developed while torment plaintext scrambling space is limited and perception security. Existing encryption algorithms are first analyzed with respect to the perception performance, plaintext scrambling space and key security [12]. An encryption algorithm improves using account key distribution and synchronization, for improved encryption effect. Use Improved selective encryption algorithm based on H.264 with features are select all IPMs as plaintext to be encrypted then scrambling space is extended with higher security.

III. H.264/AVC

H.264/AVC (Advanced Video Coding) is newest video coding standard of ITU-T Video Coding Expert Group and ISO/IEC (International Standardization Organization for /International Electrochemical Commission) Moving Pictures Experts Group (MPEG) [7]. This H.264/AVC standard completed final drafting work of first version in May 2003. First version H.264/AVC is a video compression format. This is currently most common format used for recording, compression and distribution of video content. Some Standards for the coded representation of visual information (video). It defines coded representation for visual data (video) in a compressed form and a method of decoding syntax or coded representation for reconstruct visual data (video).

H.264/MPEG part 10 AVC is a block -oriented motion compensation based video compression standard developed by ITU-T VCEG together with ISO/IEC MPEG. Standard have capability of providing video quality at lower or half bit rates than previous standard such as MPEG-2, H.263 or MPEG-4. The main goal of H.264/AVC standard perform the compression of video and wide variety of application on network or system including low or high resolution video, Broadcast ,DVD storage and multimedia telephony.

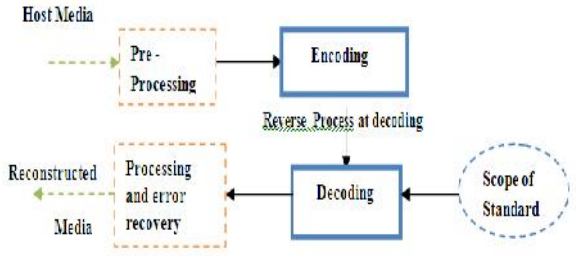

Fig.4: Structure of video coding Standard

IV. H.264/AVC ENCODER

H.264 encoder useful for choose of Intra-prediction modes. In fig. encoder block consist of integer transform, quantization of Context adaptive variable length coding, inverse transform and quantization and reconstructed video data. Encoder includes two data flow path, a forward path and reconstruction path. Input frame Fn of video for encoding, Frame has Sequence of Macroblock's (16x16 pixels in an image) called Slices. Each Macroblock is encoded in either intra or inter mode.

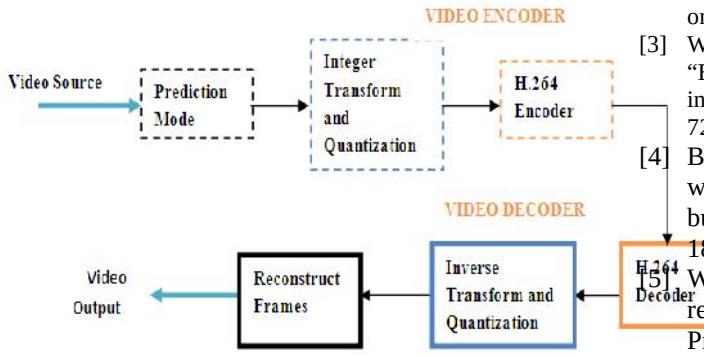

Fig.5: H.264Video encoder and decoder

CONCLUSION

The review explored idea and various security issues in digital media. The detailed Study of various data hiding schemes is done in the survey. The brief idea of H.264/AVC is studied. The survey gives idea of various works done in field of data hiding and video streaming. This survey suggests proper direction for further research to develop data hiding techniques in Encrypted H.264/AVC Video Streams.

REFERENCES

[1] W. J. Lu, A. Varna, and M. Wu, "Secure video processing: Problems and challenges," inProc. IEEE Int. Conf. Acoust., Speech, Signal Processing, Prague, Czech Republic, May 2011, pp. 5856–5859

[2] W. Lu, A. L. Varna, A. Swaminathan, and M. Wu, "Secure image retrieval through feature protection," in IEEE Conf. on Acoustics, Speech and Signal Processing, April 2009.

[3] W. Lu, A. Swaminathan, A. L. Varna, and M. Wu, "Enabling search over encrypted multimedia databases," inSPIE/IS&T Media Forensics and Security, Jan. 2009, pp. 7254–18.

[4] 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.

[5] 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.

[6] X. P. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Let., vol. 18, no. 4, pp. 255–258, Apr. 2011.

[7] White Paper: An Overview of H.264 Advanced Video Coding

[8] A. J. Menezes, P. C. Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL: CRC Press, 2001.

[9] J. Ahn, H. Shim, B. Jeon, and I. Choi, "Digital video scrambling method using intra prediction mode,"inProc. PCM 2004, Nov. 2004, vol. 3333, pp. 386–393.

[10] T. Shanableh, "Data hiding in MPEG video files using multivariate regression and flexible macroblock ordering," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 455–464, Apr. 2012.

[11] S. G. Lain, 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.

[12] . J. G. Jiang, Y. Liu, Z. P. Su, G. Zhang, and S. Xing, "An improved selective encryption for H.264 video based on intra prediction mode scrambling," J. Multimedia, vol. 5, no. 5, pp. 464–472, 2010.