iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** III **Month of publication:** March 2017

DOI: http://doi.org/10.22214/ijraset.2017.3193

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Review on Real Time Data Encryption in H.264/Avc Video Streams by Exploiting IPCM Microblocks

Uddhav S. Kadam[1], Rajesh Patil[2]
[1]Mtech Scholar, [2]Associate Professor , Electrical Engineering Dept. , VJTI, Mumbai, India

Abstract: ***In daily life, there is an increase in the use of multimedia applications such video conferencing, video telephony, stream video/audio online etc. For the purpose of highly secure data transmission safely, there is a requirement of encryption of digital data. In this paper, we studied the various methods of data encryption technique, and find out the best method for the secured data transmission. H.264 is well-known compression standard technique for original raw video. Data hiding using general techniques will not perform under this scheme. We present a data hiding approach in IPCM block. Where these IPCM encoded macroblocks are modified in order to hide the desired data. Generally in video encryption, the numbers of IPCM blocks generated are very less. A method is presented to increase the number of IPCM blocks generated in H.264/AVC algorithm, by which more data can be hidden. It is a blind data hiding approach, i.e. the message can be extracted directly from the encoded stream without the need of the original host video.***
Keywords: H.264/AVC, Intra prediction, IPCM, Data hiding, encrypted domain, Codeword substitution.

I. INTRODUCTION

The security of data in a cloud networking is crucial and it is very important to preserve the security like confidentially, integrity and the availability over the cloud network as well as the other networks. In recent years there is exponential increase of size of multimedia files and because of the significant increase in affordable memory storage on the wide spread of World Wide Web (www).Also there is need for the efficient tool to retrieve the images from the large data base becomes crucial. However with the substantial increase of the size of images as well as size of image database, the task of user-based notation becomes very complex and at some extent subjective and thereby, incomplete as the text often fails to convey the rich structure of images. To find out the solution for these difficulties this motivates the research into what is referred as data hiding and compress the image using vector quantization so that small database is required. The different available technologies which provide the highly efficient computation and large-scale storage solution for video data is cloud computing. The security of data in a cloud networking is critical and it is very important to maintain the security like confidentially, integrity and the availability over the cloud network as well as the other networks. The most popular used standard technique for video is H.264/AVC (Advanced Video Coding), gives the high efficiency in video encoding.

H.264 is a next-generation video compression standard technique. H.264 is also called as MPEG-4 AVC, designed for use in high systems such as HDTV, Blu-ray and HD DVD as well as low resolution supported devices such as Sony's PSP and Apple's iPod. H.264 gives better quality at lower file sizes than both MPEG-2 and MPEG-4 technique. Apple has officially used H.264 as the format for quick access. The H.264/AVC standard was designed for high compression efficiency, error resilience and flexibility so that it could support a wide variety of applications and different transport environments such as wired and wireless networks. The video color space used by H.264/AVC diffentiate a color representation into three components namely Y, Cb and Cr. Component Y is called luma, and gives brightness. The two chroma components Cb and Cr gives the extent to which the color differ from gray toward blue and red, respectively.

High speed computer networks, the Internet and the World

Wide Web creates revolution in the digital data distribution method. The vast and easy accesses to multimedia contents and possibility to make infinite copy without loss of considerable quality of data have motivated the need for digital rights management. Digital watermarking is a technology that can use for this purpose. Watermarking is the addition of irremovable data to multimedia content for the purpose of authentication, copy identification and tracking. Watermarking technique is most important and valuable for sensitive images such as medical, military and art work images gives a big challenge to technique used in the various most

watermarking methods. Data hiding is also equally used like watermarking in order to hide the data & sends safely. Data encryption and watermarking techniques are usually studied together because a watermarking technique can perform as a data hiding technique, as well, although the opposite is not always possible. Early video data hiding approaches were necessary, still image watermarking techniques extended to video by hiding the message in each frame independently.

Data hiding dealing with the ability of embedding data into a digital cover with a minimal amount of perceivable error in the data. Data hiding consist of two set: 1. Covered medium and 2. Embedding external data. Either of the set used for data hiding can be text, audio, picture or video depending on the size of the message and the capacity of the cover. When data is hidden & send safely, motion vector is estimated at

Encoder side to remove temporal or spatial redundancy. The H.264/AVC standard technique uses the spatial correlation property through an Intra prediction. A macroblock of interest can be from block, generally located above and to the left side of the block, As they have already been encoded and reconstructed. The use of IPCM for data hiding is in fact true inspiration because it can maintain the video quality perfectly.

II. LITERATURE SURVEY

B. Zhao, W. D. Kou, and H. Lip resent 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 enhance the scheme in terms of avoiding the additional overhead. J. Zheng and J. W. Huang, gives the walsh hadamard transform (WHT) implementation also gives its application for image watermarking. They used the method in which they implemented WHT with very less quantization error. Anyone can extract the watermark in encrypted domain as well as from plain text domain.

W. Puech, M. Chaumont, and O.Straussgives the method for reversible data hiding in encrypted images. They use the method from which we can embed any data in the image and then again we can decrypt the original data back safely. Also we get original image without that hidden data. But the data hiding capacity is less as compared to the other techniques. X. P. Zhang proposed method in which data hiding for the encrypted image can be done reversibly. In encryption method the uncompressed image can be embedded by using stream cipher technique. We can decrypt the data using the encryption key and the original image can be recovered back with almost negligible loss with the extracted embedded data.

W. Hong, T. S. Chen, and H. Y. Wu,gives the best results as compared to the other research paper. They find out an improved data hiding method using side match technique. Using the side match technique the error rate of extracted bits can be decreased to considerably. X. P. Zhang propose 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 by using encryption key. If we have both the encryption as well as data hiding key then hidden data and original image can be reconstructed back securely.

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 space after encryption. Previously after the encrypted image they vacate the space accordingly the data capacity. But due to this the errors are occurred while data extraction. But this author presents a method in which the data hiding in encrypted images by reserving the room space before encryption so that we can achieve real reversibility with no loss.

A. Different Methods of Video Compression

Several important standards like the Moving Picture Experts Group (MPEG) standard, H.261, H.263 and H.264 standards are the widely used techniques for video compression.

1) *H.261:* The International Telecommunication Union (ITU) developed the H.261 standard for data rates that are multiples of 64Kbps. Motion temporal prediction is done with the help of H.261standard. It supports two resolutions, called, Common Interface Format (CIF) with a frame size of 352 × 288, and Quarter CIF (QCIF) with a frame size of 172 × 144 [10].
2) *H.263*: The H.263 standard uses an encoding algorithm called test model (TMN), which is similar to that used by H.261 but with improved performance and error recovery leading to higher efficiency. It is optimized for coding at low bit rate [6]. The standard provides the same quality as H.261 but with nearly half the number of bits. The functionality of the H.263 is enhanced by features like: bi-directionally encoded B-frames, overlapped-block motion compensation on 8 × 8 blocks instead of 16 × 16 macroblocks, unrestricted motion vector range outside the picture boundary, arithmetic encoding; and fractional-pixel motion-vector accuracy [6].
3) *Mpeg-1*: Intra-coded (I-frames): encoded as discrete frames (still frames), independent of¬ adjacent frames. Predictive-coded (P-frames): encoded by prediction from a past I-frame or P-frame,¬ resulting in a better compression ratio (smaller frame). Bi-

directional-predictive-coded (B-frame): encoded by prediction using a previous¬ and a future frame of either I-frames or P-frames; offers the highest degree of compression.[5]

4) *Mpeg-2*: The MPEG-2 project was approved in November 1994, and was focused on extending the compression technique of MPEG-1 to cover larger pictures and higher quality at the expense of a higher bandwidth usage. MPEG-2 is designed and implemented for digital television broadcasting applications that specially require a bit rate of between 4 and 15 Mbps (up to 100 Mbps), such as digital high definition TV (HDTV), interactive storage media (ISM), and cable TV Profiles and levels were introduced in MPEG-2 [7].
5) *Mpeg-4*: MPEG-4 was approved in October 1998, and it enables multimedia to be transmitted in low bit rate networks and allows the user to interact with the objects [8]. The objects represent aural, visual or audiovisual content that can be synthetic such as interactive graphics applications, or natural such as in digital television. By combining these objects we can form compound objects, and multiplexed and synchronized to provide QoS during transmission. Media objects can be in any place in the coordinate system. Streamed data can be applied to media objects to change their parameter.[8]
6) *Mpeg-7:* The MPEG-7 standard was approved in July 2001 (Chang, et al., 2001) to standardize a language to gives description technique. MPEG-7 is a various kind of standard as it is a multimedia content description standard, and does not useful with the actual encoding of moving pictures and audio. With MPEG-7, the content of the video is presented and associated with the content itself, for example, to allow quick and significant searching in the material [9]. MPEG-7 uses XML to store metadata, and it can be attached to a time code in order to tag particular events in a stream. Although MPEG-7 is independent of the actual encoding technique of multimedia, the representation that is defined within MPEG-4, i.e. the representation of audio-visual data in terms of objects, is very good to the MPEG-7 standard. Usually, I-frames are used for random accessing of the data and are used as references data for the decoding of other pictures. Intra refresh periods of a 0.5sec are very common on applications such as digital television broadcast and DVD storage. Longer refresh time may be used in some platform. For example, in video conferencing systems it is common to send I-frames very infrequently [9]
7) *H.264/AVC.*: In early 1998, the Video Coding Experts Group (VCEG) of ITU-T gives a call for proposals on a project called H.26L, with the view that double the coding efficiency in comparison to any other existing video coding standards for various applications. The Moving Picture Expert Group (MPEG) and the Video Coding Experts Group (VCEG) developed a new and an outstanding standard that promises to outperform the earlier MPEG- 4 and H.263 standards. The first draft design for the new standard technique was developed in October 1999. It gives a good balance between coding efficiency, cost, and implementation complexity [10]. It has been accepted and done by the Joint Video Team (JVT) as the draft of the new Coding standard technique for formal approval submission, referred to as H.264/AVC, and approved by ITU-T in March 2003 (known also as MPEG-4 part 10. The standard was also designed to give lower latency as well as better quality for higher latency. In addition, all these improvements, compared to previous standards, come without the need to increase the complexity of the design [10].

III. INTRA PULSE CODE MODULATION IN H.264/AVC

Data hiding in H.264 makes use of three different types of predictions like inter prediction, intra prediction & IPCM blocks to encrypt the data. In inter prediction mode, motion vector can be estimated between the two frames, In case of intra prediction mode, motion vector can be estimated within the frame with left & top side of the frame. Third type of prediction is done by using IPCM microblocks without compression data is send in IPCM method. i.e. loss of data due to compression is decreased because in case of inter or intra prediction, data compression at the encoder side & data decompression at the decoder side gives a lot of data loss during encoding & decoding process. But in case of IPCM block, without compression data can be send i.e. at the decoder side same data as that of original one, this means that probability of loss of data is completely decreased. But one problem is their while using IPCM blocks is scarcely of IPCM blocks. Although many researchers have presented data hiding standard techniques based on intra-prediction mode of H.264 video [6], [7], [9] but Kapotas et al [1], [8] was to first to propose it using IPCM macroblocks. Data hiding based on motion vectors estimation has been presented [3], [5] but this suffers from the basic limitation of low embedding capacity, as lot of extra information is to be embedded to make the watermark data safe and secure.

The basic procedure for frame (picture) is that it is partitioned into fixed-size macroblocks, which covers a rectangular picture area of 16X16 samples of the luma components and 8X8 samples of each of the two chroma components. All luma and chroma samples of a macroblock are either spatially or temporally estimated, and the resulting prediction residual is encoded using transform coding technique. For transform coding purposes, each color component of the

prediction residual signal is sub categorized into smaller 4X4 blocks.

IV. METHOD FOR DATA HIDING

In order to hide the data using IPCM block in which data is directly processed without compression or without any loss of data. In this method of data embedding based on IPCM block is a secure and safe one. Secondly we check the robustness of hidden data & thirdly we perform capacity estimation of the data hiding space available. When IPCM blocks are used to hide the data lower bits of luma and chroma samples are used. Because of change in lower bits of luma and chroma it does not affect the image or video degradation quality much more. But regarding the IPCM blocks there is one practical problem i.e. Scarcity of IPCM blocks.

In data hiding process, numbers of IPCM blocks needed to hide the data are less than the number of IPCM blocks required to dynamically generate the IPCM blocks. Data hiding at the encoder side is shown in Figure 1, where raw video is taken as input to the encoder which is passed at the same time when embedded data is passed to the encoder, so that data can be hide at the encoder side & converted to the H.264 bit stream. Output of encoder is passed to the decoder where hidden data can be extracted from the bit stream and original raw video can be reconstructed back.

Data extraction during decoding is shown in figure 2, where input to the decoder is in the form of H.264 bit stream. Decoder will first find IPCM micro block. If IPCM block is present then extract embedded data from the IPCM block as well as reconstruct back the original input frame as it is without loss at the decoder side.

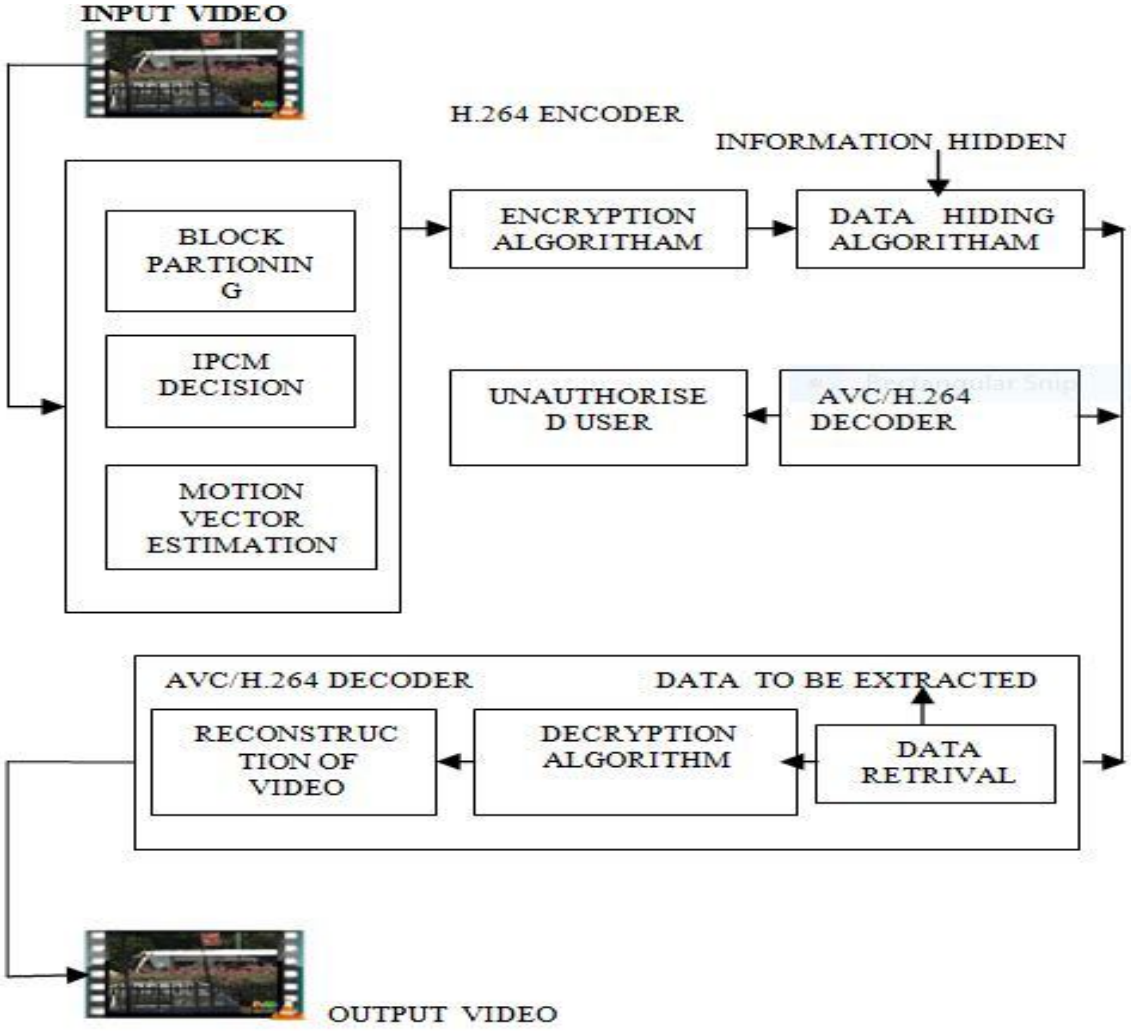


Fig 1: Block diagram of data hiding by exploiting IPCM microblock

In order to hide the data in the H.264 encoder, we pass input to the mode decision. Mode decision will find the type of prediction from the given prediction (inter prediction or intra prediction or IPCM) and hide the data in IPCM blocks. If the type of prediction is

inter prediction, the motion estimation and compensation have become powerful techniques to eliminate the temporal redundancy due to high exactness between successive frames. Because two successive frames of a video sequence often have small differences, it decreases the temporal redundancy.

Block matching process takes more time during encoding process. To get the correct a matching block, each block of the current frame is compared with a past various frame within a search area.

If the type of estimation intra prediction has been conducted in the transform domain intra prediction in H.264/AVC is always carried out in the spatial domain, by referring to neighboring samples of previously-coded blocks which are to the left and/or above the block to be identified.

If the encoder get success to find out matching block on a reference frame, it will gives a motion pointing to the matched block and a prediction error. Using both the elements, the decoder will be able to recover the original pixels of the block.

There are chances to lost some data due to compression; such type of data can be seen to to the owner as it is without compression. For sending such type of data IPCM blocks are used. If IPCM blocks are used then there is no need of transformation and quantization.

In order to reduce the number of expensive motion estimation calculations, they are calculated only if the difference between two blocks at the same level is higher than a threshold value; otherwise the whole block is transmitted as it is. In H.264/AVC, there are two methods of entropy coding are possible to supported. The simpler entropy coding method uses a single unlimited extent code word table ` Length Coding (CAVLC) is used. In the CAVLC entropy coding method, the number of nonzero quantized element coefficients (N) and the actual size and position of the coefficients are coded differently.

A. Flowchart of Data Embedding And Retrival

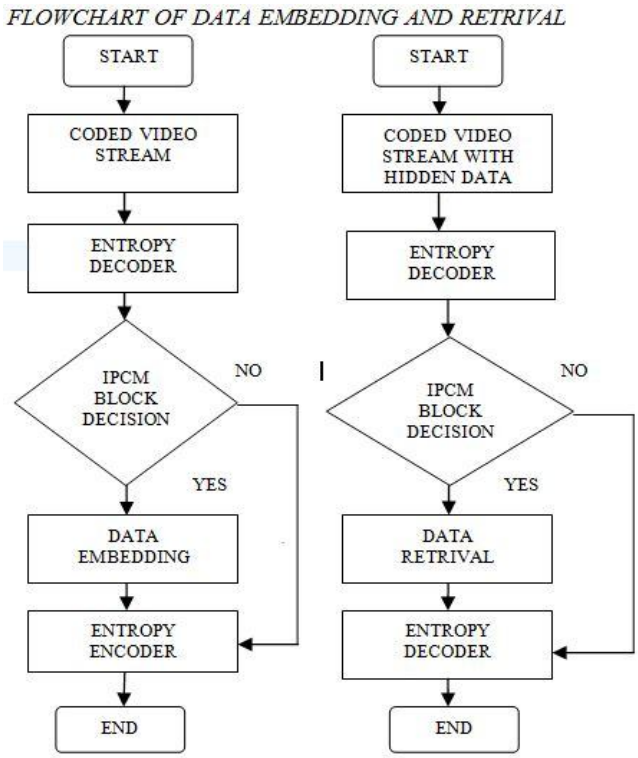


Fig 2.:(a) Data embedding and (b) data retrieval

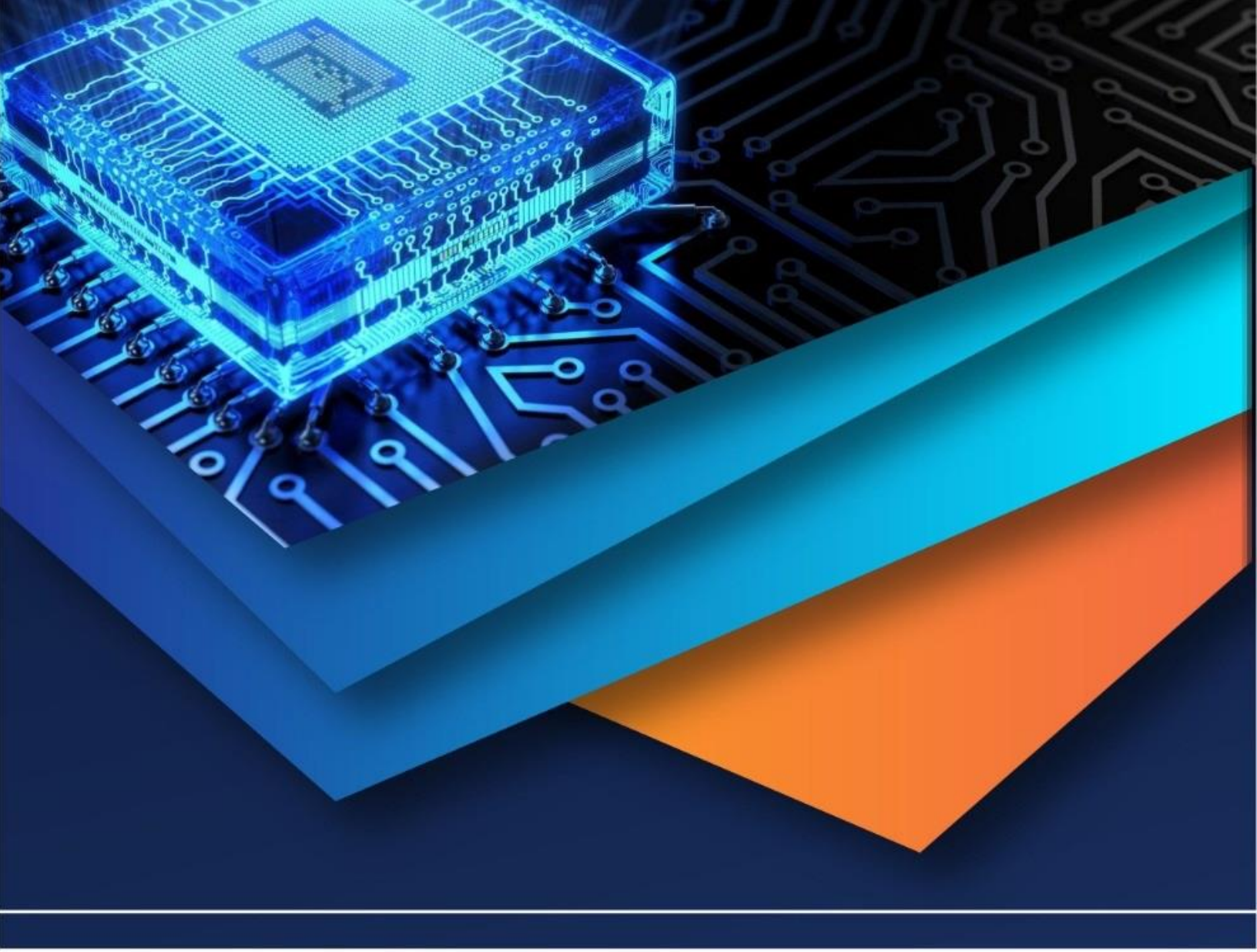
V. CONCLUSION

Data hiding in encrypted video is a new technology that has started to cause attention due to the storage and privacy requirements from cloud server network. Data hiding is done with the help of IPCM microblock. When more data is to be hidden, more no of IPCM blocks are generated which makes the compression less significant. In this paper, an algorithm which gives the methodology to embed additional data in encrypted H.264/AVC bit stream is presented, which includes the video encryption, data embedding and

data extraction steps. The algorithm can maintain the bit-rate exactly same even after encryption and data embedding, and is simpler to perform as it is directly performed in the compressed and encrypted domain, i.e. It does not need to decrypt or partial decompression of the video bit stream thus making it best for real-time video applications scenario. The data-hider can embed additional data into the encrypted bit stream using codeword substituting, even though he does not know the original video content. Furthermore the data hiding process is completed entirely in the encrypted domain, so can preserve the confidentiality of the content completely. Thus there are so many applications by data hiding in encrypted domain such as Content authentication , Copyright Protection, Broadcast monitoring, Finger printing, Metadata binding, Covert communication.

REFERENCES

[1] Dawen Xu, 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,
[2] Spyridon K. Kapotas, Athanassios N. Skodras, "Real time data hiding by exploiting the IPCM macroblocks in H.264/AVC streams" , Springer Journal of Real Time Image Processing, Volume 1, Issue 4,March 2009.
[3] Chae, J.J., Manjunath, B.S.: Data hiding in video. In: IEEE Proceedings of International Conference on Image Processing (ICIP), pp. 243–246 (1999)
[4] Sarkar, A., Madhow, U., Chandrasekaran, S., Manjunath, B S.: Adaptive MPEG-2 video data hiding scheme. In: Proceedings of SPIE Security, Steganography, and Watermarking of Multimedia Contents IX, January 2007
[5] Gary J. Sullivan, Pankaj N. Topiwala, and Ajay Luthra, "The H.264/AVC advanced video coding standard: overview and introduction to the fidelity range extensions," Proc. SPIE, vol. 5558, 454-476, 2004.
[6] Fang, D.-Y., Chang, L.-W.: Data hiding for digital video with phase of motion vector. In: IEEE Proceedings of International Symposium on Circuits and Systems (ISCAS), May 2006
[7] Cao, H., Zhou, J., Yu, S.: An implement of fast hiding data into H.264 bitstream based on intra-prediction coding. Proc. SPIE 6043, 123–130 (2005)
[8] Hu, Y., Zhang, C., Su, Y.: Information hiding based on intra prediction modes for H.264/AVC. In: IEEE International Conference on Multimedia and Expo (ICME), Beijing, China, July 2–5, 2007
[9] Kapotas, S.K., Varsaki, E.E., Skodras, A. N.: Data hiding in H.264 encoded video sequences. In: IEEE International Workshop on Multimedia Signal Processing (MMSP), Chania, Greece, October 1–3, 2007
[10] Kim, S.M., Kim, S.B., Hong, Y., Won, C.S.: Data hiding on H.264/AVC compressed video. In: Proceedings of ICIAR 2007. LNCS, vol. 4633, pp. 698–707 (2007)
[11] Wiegand, T., Sullivan, G.J., Luthra, A.: Draft ITU-T Recommendation H.264 and Final Draft International Standard 14496- 10 AVC, JVT of ISO/IEC JTC1/SC29/WG11 and ITU-T SG16/ Q.6, Doc. JVT-G050r1, Geneva, Switzerland,May2003.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY