IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727,
PP 36-40
www.iosrjournals.org

A Novel Approach for Codeword Substitution Using Encrypted H.264/AVC Video Streams for Data Hiding

Nikita Ramdas Bodke[1], Sandip Nathu Kapse[2],Jayashri Shantaram Khule[3], Premlata Uttam Shinde[4]

[1,2,3,4,]*(I.T. Dept. ,B.V.C.O.E.&R.I. Anjaneri ,university .Pune, India)*

Abstract : *Digital videos are very most popular because of their frequency on their internet and to strictly preserve the size of file There are different types of techniques present for hiding secure data in videos. Digital video necessary to be stored in encrypted format. The purpose of content notation and or tampering these it is necessary to perform data hiding in these encrypted video. The data embedding in video following three parts that is H264 /AVC, video encryption, data insertion, data extraction. The working of the system have three stages, first the analyzing of H.264/AVC video the codewords of intraprediction modes, the codewords of motion vector differences, and the codewords of residual coefficients are encrypted with stream cipher. second data hider may embed additional data in the encrypted domain with codeword substitution technique, and also does not knowing the original video data. This technology will help future innovations and researchers in military application, video in medical field and other applications. third one is data extraction can be done either in the encrypted domain or in the decrypted domain.*

Keywords - *Data hiding, encrypted domain, H.264/AVC, codeword substituting.*

I. INTRODUCTION

Now a days the world wide web have change the way of handling the digital information . Data hiding deals with the ability of insertion of secure information into a digital cover with a minimum amount of perceivable degradation that is the inserted data is invisible to a human observer. H.264/AVC video streams would avoid leakage of video content which can helpful for security and privacy concerns with cloud computing. Similarly when medical videos or surveillance videos have been coded for protecting the privacy of the people a database manager may embed the personal information into the corresponding encrypted videos to provide the data management capabilities in the encrypted domain. With the increasing demands of providing video information security and confidential protection data hiding in encrypted H.264/AVC videos will become popular in the near future.

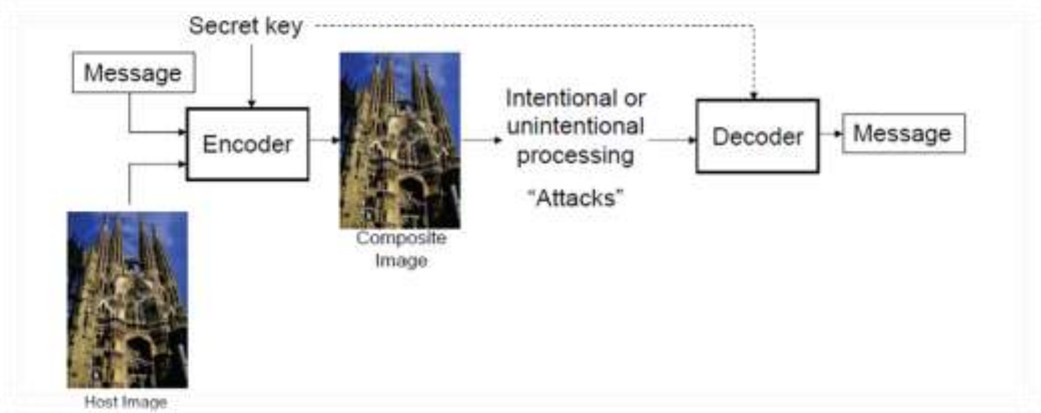


Fig 1: Normal Encryption Technology

II. Problem Defination

Due to exponential increase of size so it is called multimedia files in recent years the reason of the substantial increase of reasonable memory storage on one hand and the wide spread to the other hand. This system motivates the extensive research into retrieval systems image. To overcome these types of difficulties it motivates the research into what is referred as data hiding and compress the image using vector quantization for that reason the small database is required.. This chapter follow the all existing approaches for data hiding. A novel scheme of data hiding in the encrypted version of H.264/AVC videos consist of three parts, first part is H.264/AVC video encryption, second part is data embedding and the last one is data extraction. To produce an encrypted video stream the content owner can encrypts the original H.264/AVC video stream by using standard stream ciphers with encryption keys. After that without knowing the original video content the data-hider can insert the additional data into the encrypted video stream by use of codeword substituting method. The hidden data extraction can be successfully completed in encrypted or decrypted domain at the receiver end.

III. System Overview

A. Encryption of H.264/AVC Video Stream

In Fig. (a) Shows Video encryption standered is requires the process is a time effective to meet the requirement of real time and format compliance. It is not encrypt the whole compressed video bitstream alternatively, only a fraction of video details encrypted to improve the efficiency while still achieving sufficient security. The key issue of encrypted video steam is that it concentrate on how to select the sensitive data to encrypt. An H.264/AVC video encryption scheme with good performance consist of security, efficiency, and format compliance is proposed. The encryption algorithm is performed not only in H.264/AVC encoding but also in the H.264/AVC compressed domain. Encryption of H.264/AVC Video Stream compressed domain has been presented on context-adaptive variable length coding (CAVLC) and context-adaptive binary arithmetic coding(CABAC). By analyzing the property of H.264/AVC codec, there are three sensitive parts are encrypted with the stream ciphers. The system have improved and enhanced the previous proposed approach by encrypting more syntax elements. The proposed system encrypt the IPMs codewords, the MVDs codewords, and the residual coefficients codewords.

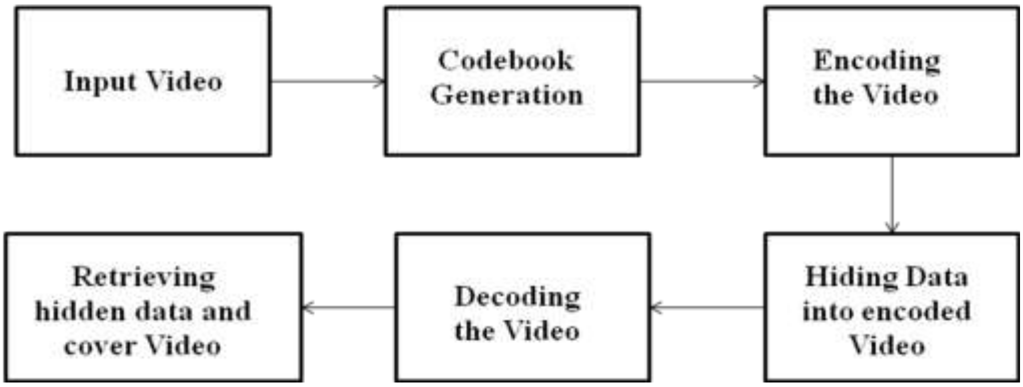

Input Video
Codebook Generation
Encoding the Video
Hiding Data into encoded Video
Decoding the Video
Retrieving hidden data and cover Video

Fig. 2 Video encryption and data embedding and Data extraction and video display

B. Data Embedding

In Fig.(a) Shows the data embedding process few methods are proposed to embed data into H.264/AVC bitstream directly. No anyone methods are implemented in the encrypted domain. In these process the levels of sign are encrypted, so that data hiding should not affect the levels of sign. In the codewords substitution following three types of limitation are satisfied. First limitation is that, the codeword substituting after bitstream must remain syntax compliance so that it can be decoded by standard decoder. Second limitation is that, the bit-rate remains unchanged, to take care that the substituted codeword and the original codeword having the same size. Third limitation is that ,data hiding does causes the visual degradation but having impact should be kept minimum. That is after video decryption, the embedded data has to be invisible to a human observer. So the level corresponding the substituted codeword value should be close to the level corresponding value to the original codeword value.

C. Data Extraction

In data extraction process the hidden data can be extracted either in Encrypted domain or in decrypted domain. The data extraction process is the fast and simple. In the encrypted Domain Extraction a database manager only access the data hiding key and to manipulate data in encrypted domain for purpose of protecting privacy. In this case data extraction in encrypted domain guarantees the feasibility. In encrypted domain, encrypted video with hidden data is directly send to the extraction module. The codeword is a part of codespaceC0, the bit of data extracted is “0”. The codeword is part codespaceC1,the bit of data extracted is “1”. In that way the data hiding key, the equal chaotic pseudo-random sequence P was used in the embedding process can be generated.

IV. ALGORITHMS

- Privacy of Encryption Algorithm

Video encryption scheme, the privacy includes both cryptographic privacy and perceptual privacy. Cryptographic privacy denotes the privacy against cryptographic attacks, which depends on the ciphers adopted by the scheme. The protect stream cipher is used to encrypt the bitstream, and chaotic pseudo-random sequence generated by logistic map is used to encrypt the additional data. They have been proved to be protect cryptographic attacks. Perceptual privacy refers to whether the encrypted video is unintelligible or not. It depends on the encryption scheme's properties. Encrypting only IPM cannot keep protect enough, since the encrypted video is intelligible .The encrypts IPM, MVD and residual coefficients, which keeps perceptual privacy of the encrypted video. The demonstration and an original frame from each video is depicted, and their corresponding encrypted results are depicted in Other frames have a similar effect of encryption. Due to space limitations, do not list the results of all frames. It should be mentioned that not every video can be degraded to the same extent. The perceptual quality of high-motion videos with a complex textured background becomes much more scrambled after encryption than that of slow-motion videos with a static background. The reason is that there are less residual coefficients and MVDs in low-motion videos that are available for encryption. Scrambling performance of the encryption system is more than sufficient.

- Intra-Prediction Mode (IPM) Encryption

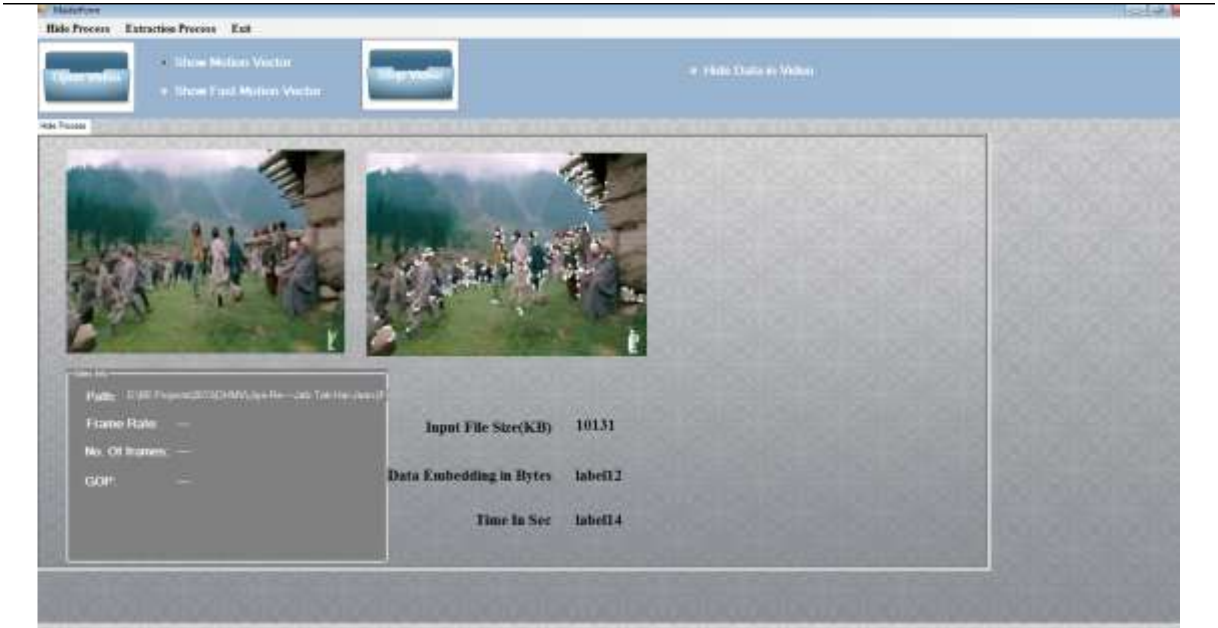
In data hiding H.264/AVC standard there are four types of intra coding are useful and which are denoted by Intra_4 × 4, Intra_16×16, Intra_chroma, and I_PCM . Intra_4×4 and Intra_16 × 16 blocks are used to encrypt data. In Intra_16 × 16 four intraprediction are available. Intra_16 × 16 block is specified in the mb_type (macroblock type) as well as it specified in the from of coded block pattern (CBP). To keep unchanged codeword length, the encrypted codeword the same size as original codeword. The combination of CBP is the same in every four lines, and the codewords have the same length in every two consecutive lines.

- Motion Vector Difference (MVD) Encryption

Not only the IPMs encrypted to protect both information texure and motion, but also the motion vector should also be encrypted. In H.264/AVC standard Exp-Golomb entropy coding is very useful to encode MVD. The Exp-Golombcodeword constructed as[M zeros] [I NFO], where I NFO is an M-bit field carrying information.The last bit of the codeword is encrypted by the bitwise XOR operation with stream cipher, which is an encrypted by an encryption E_Key. The last bit encryption may change the sign of MVD, but the length of the codeworddoes not affect and filled with satisfaction and the compliance format. In that way, the resulting ciphertexts are still valid Exp-Golomb codes.

V. Design And Implementation Constraints

A primary cause of poor website design is that the web developers' understanding of how a website should be structured can be considerably different from those of the users. Location extraction is also important task to be done. To extract such differences result in cases where users cannot easily locate the desired information in a website. This problem is difficult to avoid because when creating a website, web developers may not have a clear understanding of users' preferences and can only organize pages based on their own judgments.

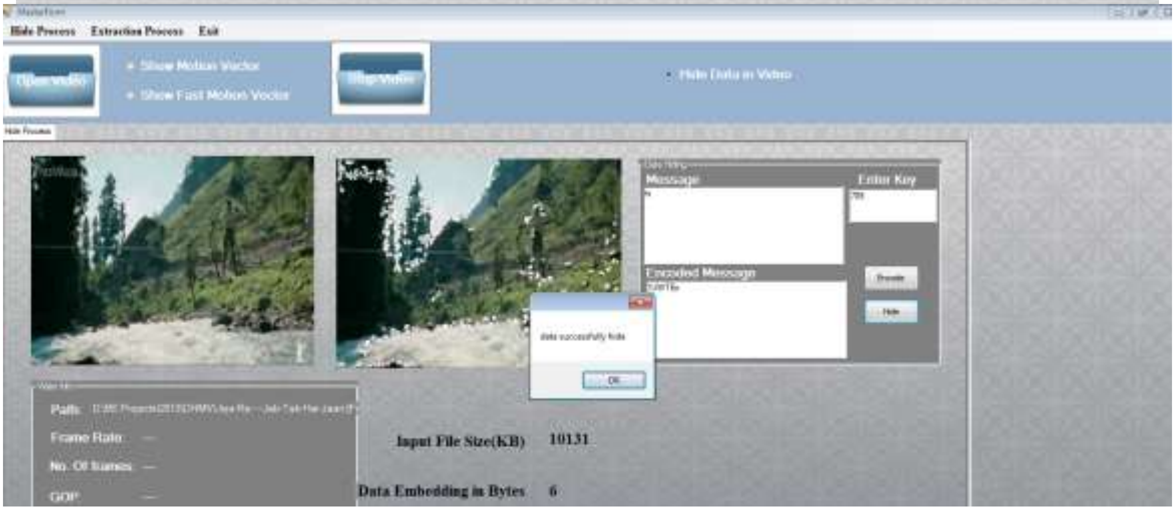


Path:
Frame Rate: --
No. Of frames: --
GOP: --

Input File Size(KB) 10131

Data Embedding in Bytes label12

Time In Sec label14



data successfully hide

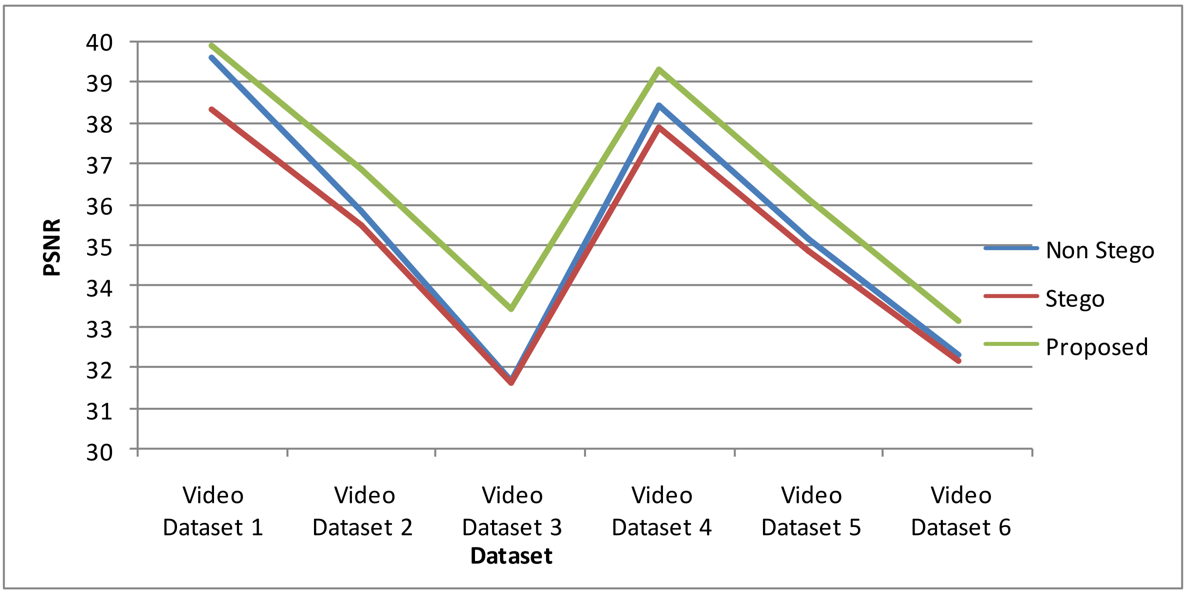
Path:
Frame Rate: --
No. Of frames: --
GOP: --

Input File Size(KB) 10131

Data Embedding in Bytes 6

VI. RESULT SET

Input Data	Non Stego	Stego	Proposed
Video Dataset 1	39.60	38.33	39.89
Video Dataset 2	35.84	35.50	36.87
Video Dataset 3	31.68	31.62	33.43
Video Dataset 4	38.44	37.91	39.32
Video Dataset 5	35.15	34.87	36.12
Video Dataset 6	32.31	32.17	33.15



VII. Conclusion

Data hiding in encrypted media is one of the important concept for privacy-preserving requirements from cloud data management. This paper focus on an algorithm to embed additional data in encrypted H.264/AVC bit stream is presented, which furtherly divided into video encryption, data embedding and data extraction phases. The algorithm maintain the bit-rate after encryption and data embedding. The algorithm is also useful to implement to performed in the compressed and encrypted domain. It means that ,it does not require partial decompression of the video stream. Thus algorithm is ideal for video applications. The data can be hide which is embed additionally data into the encrypted bit stream using codeword substituting. Data hiding is done totally in the encrypted domain, the method which is given in this paper can preserve the confidentiality of the content completely. When encrypted video contain hidden data, data extraction can be carried out either in encrypted or decrypted domain, which having two different practical applications. One of the important benefit as it is fully compliant with the H.264/AVC syntax. The experiment shows that the proposed encryption and data embedding scheme can maintain &preserve file-size, where the degradation in video quality caused by data hiding is quite small.

References

Journal Papers:

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

[2] 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.

[3] P. J. Zheng and J. W. Huang, "Walsh-Hadamard transform in the homomorphic encrypted domain and its application in image watermarking," inProc. 14th Inf. Hiding Conf., Berkeley, CA, USA, 2012, pp. 1–15.

[4] 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.

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