Secret Data Hiding in Encrypted Compressed Video Bit Streams for Privacy Info Protection

M. Sankaragomathi
M.E-Communication Systems
Department of ECE,
Sriguru Institute of Technology, Coimbatore.

Mr. M. Navin Kumar
M.E., M.I.S.T.E.,
Department of ECE,
Sriguru Institute of Technology, Coimbatore.

Abstract: **- This project presents that encryption of compressed video bit streams and hiding privacy information to protect videos during transmission or cloud storage. Digital video sometimes needs to be stored and processed in an encrypted format to keep up security and privacy. Data hiding approach is critical to perform in these encrypted videos for the purpose of content notation and change of state detection. During this method, data hiding in encrypted domain without secret writing preserves the confidentiality of the content. Additionally, it's more economical without secret writing followed by data hiding and re-encryption. Here, data hiding directly within the encrypted version of H.264/AVC video stream is used, which has the subsequent 3 components, i.e., data embedding, H.264/AVC video encryption and data extraction. After analyzing the property of H.264/AVC codec, the code words of motion vector variations, the code words of intra prediction modes and therefore the code words of residual coefficients are encrypted with stream ciphers. Then, hider might enter extra data within the encrypted domain by using bits replacement technique, without knowing the first video content. Chaos crypto system is employed here to encrypt/decrypt secret text data before/after data embedding/extraction. so as to adapt to totally different application scenarios, data extraction can be done either within the encrypted domain or within the decrypted domain. The project simulated results shows that used methods provide higher performance in terms of computation efficiency, high data security and video quality after decryption.**

Keywords: H.264/AVC Coder, Data hiding, Embedding and Extraction.

I. INTRODUCTION

Multimedia security has become one in all the foremost aspects of communications with the continual increase within the use of digital knowledge transmission. Additionally, some applications, like TV broadcast video in demand and video conferencing need a special and reliable secure storage or transmission of digital pictures and videos which can use in several applications [16]. In general, multimedia system security is provided by a technique or a collection of ways wont to shield the multimedia system contents. These ways wherever heavily supported Cryptography. However, cryptography is that the art of keeping info secret by remodeling it into associate indecipherable format by exploitation special keys. Then representing the data decipherable once more for trusty parties by exploitation constant or different special keys[11]. Moreover, fashionable cryptography doesn't lock up itself to solely maintaining the secrecy of knowledge however goes on the far side that by making certain the identity of human activity parties (authentication), making certain that info has not been
tampered with others (integrity), and preventing that any of the human activity parties denies having received or sent info (non-repudiation).

In multimedia system knowledge, cryptography is critical once human activity over any untrusted medium as well as public networks notably the net. Additionally to shield info from felony, alteration or misuse, cryptography may be used for user authentication. In fashionable field of cryptography, there are 3 varieties of scientific discipline schemes: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions [7]. Symmetric-key cryptography refers to cryptography ways within which each the sender and receiver share constant key. Public key cryptography uses 2 keys, one for encrypting info by sender, and one for decrypting info by the receiver.

A Hash operate, conjointly known as message digest or unidirectional cryptography, it's a metamorphosis that takes associate input and returns a fixed-size string, that is named the hash price. Whereas satellite or uneven cryptography ways offer suggests that to confirm info confidentiality, hash functions, offers a live of the integrity of a file [10]. Hash algorithms are generally wont to offer a digital signature of a file's contents usually won't to make sure that the file has not been altered by an entrant or virus.

In some applications like business TV broadcast, military applications, and intelligence needs to have a secured transmission or storage media. What is more, videoconferencing has become a daily characteristic of economic businesses. Because it saves time, effort, and travel expenses for giant corporations. This communicated video application needs to be utterly secured against felony, alteration or misuse. For this purpose, cryptography algorithms may be applied to those multimedia system applications to confirm their security [12].Encryption of video and audio multimedia system content isn\'t merely the applying of established cryptography algorithms, like DES or AES, to its binary sequence. It involves careful analysis to see and determine the best cryptography methodology once coping with video knowledge [9]. Recently, cryptography techniques offer the essential technology for building secure multimedia. So as to supply real time reliable security of digital pictures and videos, many cryptography algorithms

are brought forward to secure networked continuous media from potential threats like hacker and eavesdroppers and most of video cryptography algorithms ar designed for various video committal to writing standards like MPEG-1, MPEG-2/H.262, and MPEG-4 [13].

Unfortunately, these cryptography algorithms don't acceptable for secure the present multimedia system. Therefore, current analysis is concentrated on modifying and optimizing the prevailing cryptosystems for period of time video. it\'s conjointly orientated towards exploiting the format specific properties of the many customary video formats so as to realize the specified speed and alter period of time security streaming [1].

II. LITERATURE SURVEY

P. J. Zheng and J. W. Huang (2012) proposed a watermarking method to protect the copyright of digital media by hiding proprietary information in media [9]. The security of watermarking is a challenging problem in the watermarking community. In fact, there are at least two Problems on the security. The first one is the security of the original media. Almost all the previous watermarking schemes accomplish the watermark embedding and extraction on the plain media. Hence, the watermark embedded must be the owner of the plain media, in order to make sure the original media is not showing to the untrusted party. The second one is the security of the watermark scheme itself. For example, how to prevent illegal watermark embedding, extracting and removal. Though there are some reports on integrating watermark embedding and encrypting, it causes additional constraints to the watermarking algorithm. Some works have been proposed to solve the first problem, however, the visual quality of the watermarked images are not as good as expected. This new technology allows one to manipulate the encryption data by means of signal processing without decrypting. The main advantages of WHT are as follows. 1) WHT can be implemented in the encrypted domain without any quantization error. 2) The extraction is done by watermark both in the plain domain and the encrypted domain. 3) Watermarking scheme is used to design a secure media distribution system.

X. P. Zhang (2012) has focused on the use of computer networks for knowledge transmission and security [19]. Several strong message cryptography techniques are developed to produce this demand. The quantity of digital pictures has magnified speedily on the web. Image security becomes more and more necessary for several applications, e.g., confidential transmission, and video police investigation, military and medical applications. Nowadays, the transmission of pictures is daily routine and it's necessary to seek out an efficient thanks to transmit them over networks. To decrease the transmission time, the data compression is important. The protection of this transmission data is through with a tangle or information concealment algorithms. Since few years, a retardant is to undertake to mix compression, encoding and information concealment in an exceedingly single step. 2 main teams of technologies are developed for this purpose. The primary one is predicated on content protection through encoding. There square measure many strategies to encipher binary pictures or grey level pictures. The second cluster is predicated on the protection on digital watermarking or information concealment, geared toward in secret embedding a message into the info. Encoding and watermarking formulas square measure relay on Kirchhoff’s principle: all the main points of algorithm square measure illustrious and solely the key to encipher and rewrite the info ought to be secret. The benefits of this projected methodology square measure: 1) the info concealment and image encoding are done by mistreatment 2 completely different keys. that's encoding key and information concealment key. 2) The receiver UN agency has the info concealment key will retrieve the info embedded. 3) The receiver UN agency has the encoding key will retrieve the initial image while not removing or extracting the info embedded within the encrypted image. 4) The receiver UN agency has each keys will retrieve the info hidden and therefore the original image from the encrypted image.

K. D. Ma, W. M. Zhang, X. F. Zhao, N. Yu, and F. Li (2013) have dealt at reversible information concealment (RDH) in encrypted pictures moreover as in audio and video by victimization RDH methodology, the first image (cover) is receive because it is recovered once embedded information is extracted conjointly protective the image content’s confidentiality [7]. All previous strategies embedding data into image by reversibly vacating space within the encrypted pictures, which can be result as some errors on information extraction and/or image restoration. That mean some secrete data is loss in information extraction conjointly degraded quality of image. Reversible information concealment (RDH) could be a technique in image process space for cryptography, by that the first cowl is recovered in lossless manner once the embedded message, is extracted. The RDH approach is wide utilized in life science, defense field and rhetorical workplace, wherever there's no degradation of the first content is allowed. The Reserving space before cryptography during this we tend to initial compress the redundant image in lossless manner so encrypts it with relevance maintain privacy. The advantages are: 1) by victimization the new FTO methodology improves potency of image. 2) The projected methodology improve potency & quality encrypted image sometimes utilized in medical space, aromatic etc. 3) The new algorithmic program utilized in novel RDH ar cut back noise result. 4) The projected methodology for plain image and attain extraordinarily sensible performance while not loss of privacy and quality of knowledge. 5) This projected methodology conjointly achieves real reversibility; separate information from encrypted version of image 6) it's extremely improve the standard of marked decrypted pictures.

S. G. Lian, Z. X. Liu, and Z. Ren (2007) projected a theme to implement independent video cryptography and watermarking throughout advanced video secret writing method [10]. In H.264/AVC compression, the intra-prediction mode, motion vector difference and discrete cosine transform(DCT) coefficients’ signs are encrypted. The cryptography and watermarking operations are independent. Thus, the watermark may be extracted from the encrypted

videos, and therefore the encrypted videos can be re-watermarked. This theme embeds the watermark without exposing video content's confidentiality, and provides an answer for signal process in encrypted domain. in addition, it will increase the operation potency, since the encrypted video may be watermarked without cryptography. These properties make the scheme a good selection for secure media transmission or distribution. Compared with media cryptography, media watermarking embeds some info into media knowledge noticeably or unnoticeably, that protects media data's possession or identification. For invisible video watermarking physical property and strength are usually needed. The physical property implies that the watermarked video is perceptually same to the first video, and therefore the strength implies that the watermark survives such operations as recompression or signal process.

S. G. Lian, Z. X. Liu, Z. Ren, and H. L. Wang (2006) projected a sophisticated Video coding is recently declared and widely used, though the protection haven\'t been developed totally [11]. in this paper, a secure AVC coding scheme is presented based on some partial coding algorithms. throughout AVC encryption, such sensitive information as intra-prediction mode, residue information and motion vector are encrypted partly.Among them, the intra-prediction mode is encrypted supported Exp-Golomb entropy writing, the intra-macro blocks' DCs ar encrypted supported context based mostly adaptive variable length writing (CAVLC), and intra macro blocks' ACs and also the inter-macro blocks' MVDs are sign-encrypted with a stream cipher followed with variable length writing. This coding theme is secure in perception, keeps format compliance, and obtains time potency tho\' reducing the encrypted information volumes. These properties build it sensible to include encryption/decryption method into compression/decompression method, and therefore appropriate for secure video transmission or sharing. In AVC, every frame is partitioned off into macro blocks that are encoded with either intra-frame mode or inter-frame mode. so as to safeguard video information, both the texture information and motion information should be encrypted. However, the AVC encoding/decoding method is time-efficient itself, which needs that the encryption/decryption method ought to be conjointly time-efficient. Thus, the partial-encryption theme is a lot of appropriate, in which, the key downside is the way to choose the sensitive information to be encrypted. A video coding theme is bestowed and analyzed during this paper, which mixes coding method with AVC writing. The theme encrypts the intra -prediction mode, the intra-macro block's residue information and also the inter-macro blocks' MVDs partly and by selection throughout AVC encryption, and keeps the format info and different information unencrypted. It obtains high time-efficiency through reducing the encrypted information volumes, that makes it sensible to include coding practicality into the players or browsers. Each the feel information and motion information are encrypted, that makes the theme not solely secure in perception however conjointly secure against brute-force and known-plaintext attacks. in addition, the segment-encryption mode makes the theme of upper hardiness to transmission errors. These properties build the theme appropriate for period applications.

III. PROPOSED SYSTEM

The proposed system shows video encryption and data hiding, Data extraction and decryption. In this system both the techniques stegnography and cryptography is used. In that, input video is encrypted and compressed using H.264/AVC coder. Input text message is encrypted using chaos encryption and then it is embedded into the input video frames using codeword substitution. After that both the video with hidden data is encrypted and then transmitted. In the receiver side, embedded data and input video is decrypted. Both the input video and secret data is extracted.

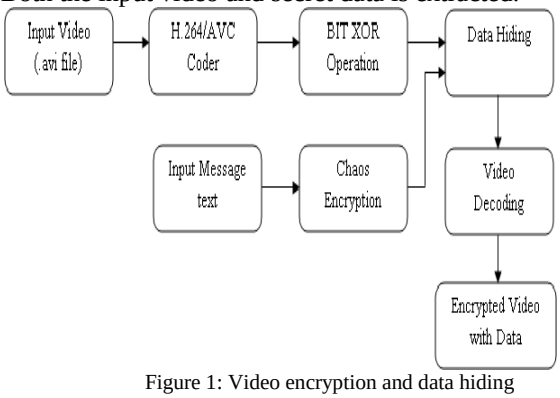

Figure 1: Video encryption and data hiding

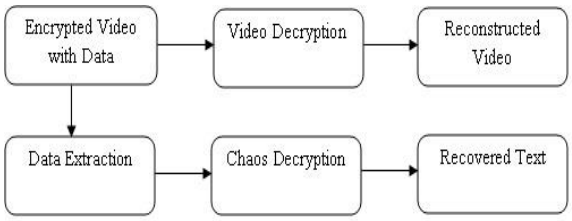

Figure 2: Data Extraction and Video Decryption

A. H.264/AVC CODER

H.264 / AVC is an industry standard for video compression, it converts a digital video into a format that takes up less capacity when it is stored or transmitted [14]. Video compression or video coding is an essential technology for applications such as digital television, DVD, and Blue – ray disks, mobile TV, video conferencing and internet video streaming. Standardizing video compression makes it possible for products from different manufactures such as encoders, decoders and storage media to interoperate. An encoder converts video into a compressed format and a decoder converts compressed video back into an uncompressed format. Advanced video coding is a video compression format, which is commonly used format. H.264 / AVC is an industry standard for video compression. Advanced video coding is used to record, compression and distribution of video format. It is also used to streaming internet sources such as YouTube.

B. 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 encrypted domain. Since the sign of Levels are encrypted, data hiding should not affect the sign of Levels. Besides, the code words substitution should satisfy the following three limitations [4].

First, the bit stream after codeword substituting must remain syntax compliance so that it can be decoded by standard decoder. Second, to keep the bit-rate unchanged, the substituted codeword should have the same size as the original codeword. Third, data hiding does cause visual degradation but the impact should be kept to minimum.

That is, the embedded data after video decryption has to be invisible to a human observer. So the value of Level corresponding to the substituted codeword should keep close to the value of Level corresponding to the original codeword. In addition, the code words of Levels within P-frames are used for data hiding, while the code words of Levels in I-frames are remained unchanged. Because I-frame is the first frame in a group of pictures, the error occurred in I-frame will be propagated to subsequent P-frames. The substitution cipher method is one of the code word substitution methods. In this method, the plain text is replaced by cipher text.

C. DATA HIDING

Data hiding embeds data into digital media for the purpose of identification, explanation, and copy right. Data Hiding is the process of secretly embedding information inside a data source without changing its perceptual quality [9]. Although AVI videos are large in size but it can be transmitted from source to target over network after processing the source video by using these data hiding and extraction securely. Two different methods, which are used here at the sender's end and receiver's end respectively. The methods used here is the key of Data Hiding and Extraction.

Data Hiding is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message. Generally, in Reversible Data Hiding, the actual information is not maintained in its original format and thereby it is converted into an alternative equivalent multimedia file, video or audio which in turn is being hidden within another object [17]. This message is sent through the network to the recipient, where the actual message is separated from that message.

Data Hiding is the different concept than cryptography, but uses some of its basic principles. The purpose of hiding such information depends on the application and the needs of the owner/user of the digital media.

D. CHAOS ENCRYPTION

Image encryption algorithm is proposed based on combination of pixel shuffling and three chaotic maps. This algorithm is based on pixel scrambling where in the randomness of the chaos is utilized to scramble the location of the data. Shuffling is mainly used to expand diffusion in the image and dissipate the high correlation among image pixels. Due to sensitivity to initial conditions, it has a designing dynamic permutation map. The plain image is first decomposed into 8x8 size blocks and then the block based shuffling of image is executed. After that the shuffled image is encrypted using chaotic sequence generated by one another chaotic map. In order to evaluate performance, algorithm was measured through a series of tests.

IV. SIMULATION RESULTS

In this project MATLAB simulation tool is used. Table 1 shows the compression process results. Here quantization parameter is fixed as 15. Input file size can be varied according to the videos

Table 1: Simulation Results

QP Value	15
Input File Size (bytes)	760320
Compressed File Size (bytes)	216056
Compression Ratio	3.5191
Maximum Capacity (Kbits/s)	95.3990

In table 2 performance measures Mean square error, peak signal to noise ratio, correlation, percentage residual difference and structure similarity index is shown. From these results it is analyzed that it have very good performance accuracy.

Table 2: Performance Measures

MSE	0.4744
PSNR (dB)	51.3694
Correlation	0.9998
PRD	0.0438
SSIM	0.9968

V. CONCLUSION

In this project a new approach stenography and cryptography has been combined. The data hiding can embed encrypted data into the encrypted bit stream using codeword substitution method, even without knowing the original video content. Since data hiding is completed entirely in the encrypted domain, this method can preserve the confidentiality of the content completely. From the results it is shown that, this encryption and data embedding method can protect file-size and video quality degradation caused by data hiding is quite small.

REFERENCES

[1] Dawen Xu, Rangding Wang, and Yun Q. Shi, Fellow, (april 2014) "Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution" IEEE transactions on information forensics and security, vol. 9, no. 4.

[2] B. Zhao, W. D. Kou, and H. Li, (2010) "Effective watermarking scheme in the encrypted domain for buyer-seller watermarking protocol," *Inf. Sci*., vol. 180, no. 23, pp. 4672–4684.

[3] D. K. Zou and J. A. Bloom, (Jul. 2010) "H.264 stream replacement watermarking with CABAC encoding," in *Proc. IEEE ICME*, Singapore, pp. 117–121.

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

[5] J. G. Jiang, Y. Liu, Z. P. Su, G. Zhang, and S. Xing, (2010) "An improved selective encryption for H.264 video based on intra prediction mode scrambling," *J. Multimedia*, vol. 5, no. 5, pp. 464–472.
[6] K. D. Ma, W. M. Zhang, X. F. Zhao, N. Yu, and F. Li, (Mar. 2013) "Reversible data hiding in encrypted images by reserving room before encryption," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 3, pp. 553–562.
[7] M. N. Asghar and M. Ghanbari, (Mar. 2013) "An efficient security system for CABAC bin-strings of H.264/SVC," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 23, no. 3, pp. 425–437.
[8] P. J. Zheng and J. W. Huang ,(2012) "Walsh-Hadamard transform in the homomorphic encrypted domain and its application in image watermarking," in *Proc. 14th Inf. Hiding Conf.*, Berkeley, CA, USA, pp. 1–15.
[9] Puech .W, M. Chaumont, and O. Strauss, (Jan. 2008) "A reversible data hiding method for encrypted images," *Proc. SPIE*, vol. 6819, pp. 68191E-1–68191E-9.
[10] S. G. Lian, Z. X. Liu, and Z. Ren, (Jun. 2007) "Commutative encryption and watermarking in video compression," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 17, no. 6, pp. 774–778.
[11] S. G. Lian, Z. X. Liu, Z. Ren, and H. L. Wang, (May 2006) "Secure advanced video coding based on selective encryption algorithms," *IEEE Trans. Consumer Electron.*, vol. 52, no. 2, pp. 621–629.
[12] Subramanyam .A .V, S. Emmanuel, and M. S. Kankanhalli, (Jun. 2012) "Robust watermarking of compressed and encrypted JPEG2000 images," *IEEE Trans. Multimedia*, vol. 14, no. 3, pp. 703–716.
[13] T. Wiegand, G. J. Sullivan, G. Bjontegaard, and A. Luthra, (Jul. 2003) "Overview of the H.264/AVC video coding standard," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 7, pp. 560–576.
[14] T. Stutz and A. Uhl, (Mar. 2012) "A survey of H.264 AVC/SVC encryption," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 22, no. 3, pp. 325–339.
[15] T. Shanableh, (Apr. 2012) "Data hiding in MPEG video files using multivariate regression and flexible macro block ordering," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 455–464.
[16] W. J. Lu, A. Varna, and M. Wu,(May 2011) "Secure video processing: Problems and challenges," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Processing*, Prague, Czech Republic, pp. 5856–5859.
[17] X. P. Zhang, (Apr. 2011) "Reversible data hiding in encrypted image," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258.
[18] X. P. Zhang, (Apr. 2012) "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832.
[19] Z. Shahid, M. Chaumont, and W. Puech, (May 2011) "Fast protection of H.264/AVC by selective encryption of CAVLC and CABAC for I and P frames," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 21, no. 5, pp. 565–576.