A Novel Approach for Enhanced Data Hiding in Encrypted Video Streams

M.Vijetha and Dr.V.Padmanabha Reddy

DVR&Dr.HS MIC College of Engineering and Technology

***Abstract*—A novel approachfor processing the digital video in encrypted format is essential to maintain privacy and security. The data should be embedded in the encrypted videos for the purpose of content notation and also for tampering detection. By utilizing this technique, it preserves the confidential information present in the video and can be retrieved without decryption. The method mainly includes three modules namely encryption of H.264/AVC video, embedding and extraction of data. The code words of motion vector differences, residual coefficients and intra prediction modes of the video are encrypted using linear predictive coding (LPC) in the first module. The technique, codeword substitution can be utilized for embedding private information in the encrypted video without knowing the content of original video. Data can be retrieved or extracted from the encrypted domain or decrypted domain based on different application scenarios. Furthermore even after the completion of encryption and data hiding, the video file size can be strictly preserved. The feasibility and efficiency of proposed article can be illustrated by experimental results.The proposed algorithm effectively retrieves the confidential information without any loss of information which can demonstrated in terms of peak signal to noise ratio (PSNR), structural similarity index mode (SSIM), video quality measurement (VQM) and visual quality at low computational cost.**

***Index Terms*—LPC, encryption, decryption, H.264/AVC, Data hiding, code word substitution**

I. INTRODUCTION

In recent years, with the development of computer technology, multimedia data is used more and more widely such as images, videos, audios and so on. The wide usages of videos in various applications include satellite communications, forensic analysis, photography, medical applications, cloud computing and film industry. So in order to prevent the leakage, some sensitive videos need to be protected before transmission; it can be avoided by embedding the private information directly in the encrypted H.264/AVC video streams. The data hiding technology can be applied for various applications such as surveillance videos and medical videos which can be encrypted for security and privacy of public, by hiding the confidential information into the encrypted videos. Existing data hiding in encrypted domain include watermarking, cryptography, walshhadamard transform based on image watermarking. Hence, we propose a new approach for data hiding in encrypted H.264/AVC videos for providing security and privacy for the video data. The encryption can be done by using bit-XOR operation. The following challenges must be achieved for hiding the data in encrypted and compressed bit stream directly.

- The first challenge is to evaluate how and where the bit stream alteration can be done so that video with hidden data is still a criticism compressed bit stream
- The second difficult task is to make sure that decrypted videos which consist the hidden data can still appear to be of high visual fidelity
- The third challenge is to maintain the file size after the encryption and data hiding which remains the minimum effect on the compression gain

The H.264/AVC codec can be analyzed with the help of codewords of motion vector differences (MVD), intra-prediction modes (IPM) and residual coefficients which in turn are encrypted with stream cipher using LPC.In order to maintain the constant codeword length the encryption algorithm is combined with context adaptive variable length coding (CAVLC), Exp-Golomb entropy coding and LPC. After encryption, the confidential data is hided in the encrypted domain which is based on codeword substitution scheme.

II. DESIGN METHODOLOGY

The proposed technique involves three phases which includes 1) Video Encryption 2) Data Hiding and 3) Data Extraction. The flow diagram of data hiding in encrypted videos is shown in the Fig. 1.

The encryptedvideo is yielded as output in the first phase, which consists of three stages: 1) Calculating the codewords of motion vector differences (MVD) 2) Evaluating the codewords of intra-prediction mode (IPM) 3) Measuring the codeword of residual coefficients. These codewords are

***M. Vijetha**, Dept. of ECE, DVR & Dr. HS MIC college of Engineering and Technology (vijji.muppala91@gmail.com), Kanchikacherla, Andhra Pradesh, India.*

***Dr.V.Padmanabha Reddy,** Professor, Dept. of ECE, DVR & Dr. HS MIC college of Engineering and Technology, Kanchikacherla, Andhra Pradesh, India.*

ISSN: 2278 – 7798

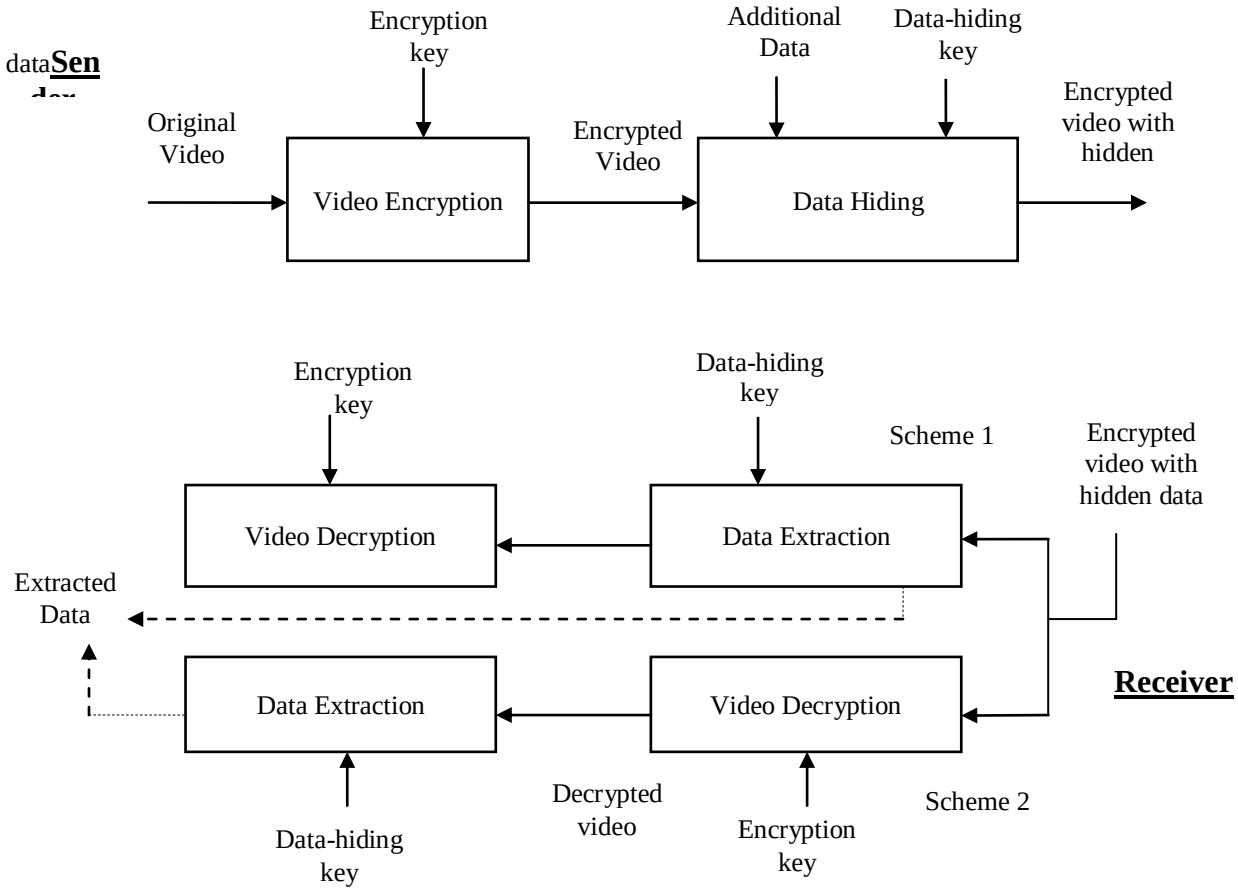

Fig. 1. Flow diagram of proposed technique. (a) Video encryption and data embedding at the sender end. (b) Data extraction and video display at the receiver end in two scenarios.

encrypted using CAVLC, Exp-Golomb and LPC. The resultant encrypted video is given as input to next phase. Data hiding involves codeword substitution method to hide the confidential information in the encrypted video which results in encrypted video with hidden data. The final phase includes the data extraction with or without video decryption domain at receiver end.

A. Video Encryption

In the first phase of this novel technique, initially the encryption video requires the scheme which is time efficient in order to accomplish the necessities of real time and format compliance. The main limitations for video encryption utilizing traditional ciphers are format compliance and computational cost. The most important point in encryption of video is to select the data to encrypt which is very sensitive. During the encoding of the H.264/AVC the encryption of both texture information and motion information is essential. The three main sensitive parts for encryption with stream ciphers consist of Intra prediction Mode [IPM], Motion Vector Difference [MVD], and residual coefficients. The encryption process is essentially accomplished during H.264/AVC compressed domain and not during encoding of H.264/AVC. In compressed domain the bitstreams will be absolutely changed. Although H.264/AVC compressed domain is previously existing in CAVLC.

1) Intra Prediction Mode (IPM): The four main kinds of intracoding that are sustained for H.264/AVC standard represented as Intra_4×4, Intra_16×16 and Intra _Chroma .In this encryption process Intra_4×4 and Intra_16×16 blocks are preferred.

2) Motion Vector Difference (MVD): Including IPMs the motion vector difference also be encrypted to protect both texture as well as motion information.

3) Residual Data Encryption: One more kind of sensitive data that is the residual data in both I and P frames must be encrypted to keep high security. By operating bitwise XOR operation with standard stream cipher the encryption of last bit of codeword is done.

4) Linear Predictive Coding (LPC): LPC is mainly used for signal processing.Linear predictive coding have four main attributes bit rate, delay, complexity, quality, removes redundant bits.Due to motion estimation is a computationally intensive process. Fortunately, only encoder must estimate the

ISSN: 2278 – 7798

macroblock motion. The decoder for the known vectors of the macroblocks accesses the areas of the reference frames that were used in the encoder to form the prediction residuals. For this reason, most video compression standards do not include motion estimation. Instead, compression standards focus on the decoder place constraints on the macroblock dimensions, motion vector precision.The H.264/AVC support intraframepredictive coding (in I-frames) to reduce spatial redundancy.

B. Data Embedding

In order to embed the data into bit streams of H.234/AVC directly the techniques are proposed. But these techniques are not probable to implement in encrypted domain in order to achieve the data encryption in bitstreams of H.264/AVC. The proposed data embedding includes the substitution of eligible codewords [1]. An example of data embedding is shown in Fig.3 (a)

The following three limitations should be satisfied by the codeword substitution

- After the substitution of codeword the bitstreams must remain syntax compliance for decoding it by standard decoder.
- The size of the codeword that is substituted should be similar to original one so that the bit rate should not be altered.
- The impact of visual degradation should be minimum which is caused by data concealing.

```
Procedure
  if (data bit= =0)
  {
        if (the codeword belongs to C0)
            The codeword is unmodified;
        else if (the codeword belongs to C1)
            The codeword is replaced with the corresponding codeword in C0.
  }
  else if (data bit= =1)
  {
        if (the codeword belongs to C1)
            The codeword is unmodified;
        else if (the codeword belongs to C0)
            The codeword is replaced with the corresponding codeword in C1.
  }
```

Fig. 2. Procedure of codeword mapping

3) Data Extraction

The data that is hidden can be extracted either in encryption or decryption domain.

The extraction in encrypted domain:

The extraction of data in this domain generates thepossibility and the encrypted video with data hiding it can be sent directly into the module of data extraction. The process of extraction are as follows

STEP 1: By analyzing the encrypted bitstream the identification of codewords of the levels is done.

STEP 2: If the extracted data bit is 0 and 1. If the codeword belongs to codespace C0, the extracted data bit is "0". If the codeword belongs to codespaceC1, the extracted data bit is "1".

STEP 3: To get the original additional data the extracted bit sequence should be decrypted, since it is carried out in encrypted domain avoids leakage of content of original video. An example of data extraction in encrypted domain is shown in Fig.3 (b)

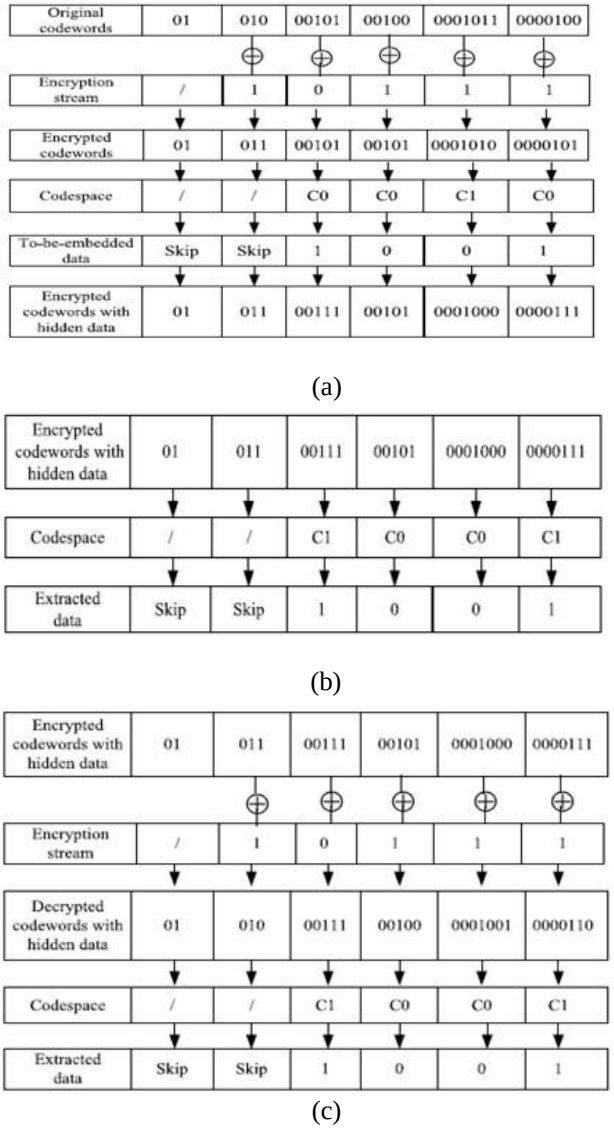

Fig. 3. An example of data embedding and extraction. (a) Data embedding. (b) Data extraction in encrypted domain. (c) Data extraction in decrypted domain.

The extraction of decrypted Domain:

In this method the video is decrypted first and then the data hidden is extracted. The video is decrypted by using these encryption keys, but these decrypted video still includes the hidden data which traces the source of the data. The extraction process is as follows:

STEP 1: The encryption streams are generated with keys in encryption process.

STEP 2: The intra prediction modes and motion vector difference codewords are identified by encrypted bit stream.

STEP 3: Due to the symmetry of XOR operation both encryption and decryption process are same. By performing XOR operation the codewords that are extracted can be

ISSN: 2278 – 7798

decrypted with generated encryption streams. An example of data extraction in decrypted domain is shown in Fig.3(c).
STEP 4: If the extracted data bit is 0 the decrypted codeword belongs to codespace C0 and if the extracted data bit is 1 the decrypted codeword belongs to codespace C1.
STEP 5: The extracted bit sequence has to be decrypted to get original data.

III. ALGORITHM

Algorithm: Data hiding is directly performed in encrypted bitstream

Input: Input video for encrypting and data hiding
Output: Decrypted video with extracted data.
Steps:

- For increasing the security, the data is encrypted in binary form to generate the embedded sequence. It is not possible to recover additional data if the data hiding key is lost.
- By parsing the bitstream of encrypted H.264/SVC the codewords are obtained.
- The data should be embedded by codeword substitution only if current codewords belongs to C0 or C1 codespaces.
- By selecting the upcoming codeword the above step is repeated for data concealing. The process is stopped if there are no data bits are found.

IV. DESIGN FLOW

The design flow diagrams at sender for encrypting and data hiding in the video and at the receiver for decrypting video with extracted data are shown in Fig. 4 and Fig. 5. First at the sender selecting the video and then this video is segmented into images. And from the segmented image, select any one of the image. After selecting any one of the image, the RGB image is converted intogray image and then the gray image is encrypted using linear predictive coding (LPC). In this encryption process the last bit of the codeword and pseudo random bit gets XOR operation and provides the encrypted codewords. Along with these codewords the texture information and motion information should be encrypted. And also the residual data in both I-frames and P-frames should be encrypted. The message image is embedded into the encrypted image.This data is hided using codeword substitution here the codeword is replaced with another codeword using codeword mapping. Now the encrypted image with hidden data is given to the receiver. At the receiver the data that is hidden can be extracted by scheme I or scheme II that is from either encryption domain or decryption domain. In encryption domain extraction first the data is extracted and then image is decrypted. In the decryption domain extraction after the image is decrypted then the data is extracted. In this proposed technique scheme II executed.

The performance of the technique is estimated by using metrics PSNR, SSIM and VQM.

Sender

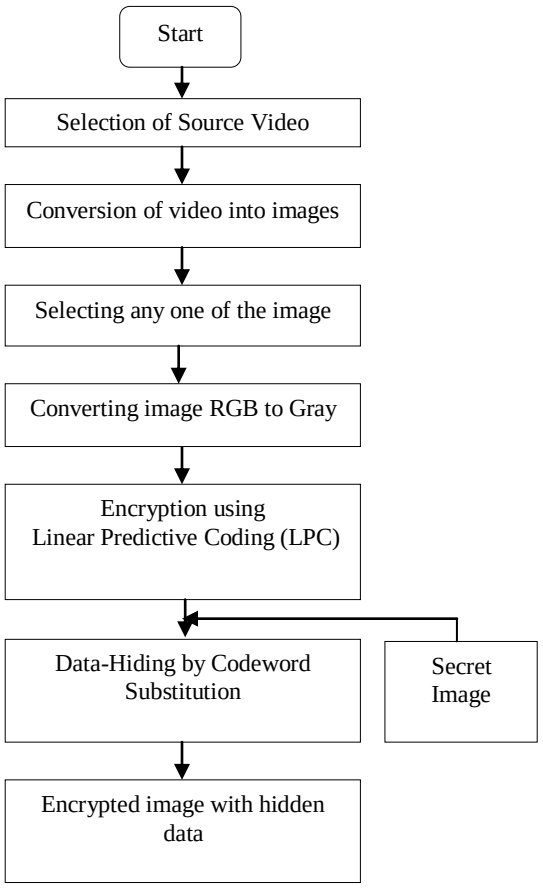

Fig.4. Design flow for Encryption and Data Hiding

Receiver

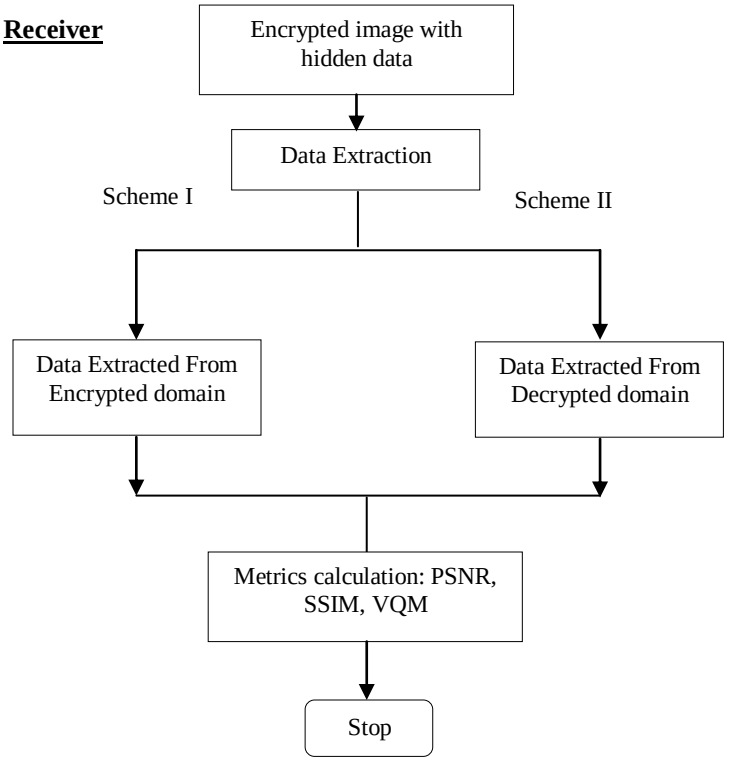

Fig.5. Design Flow for Decryption and Data Extraction

ISSN: 2278 – 7798

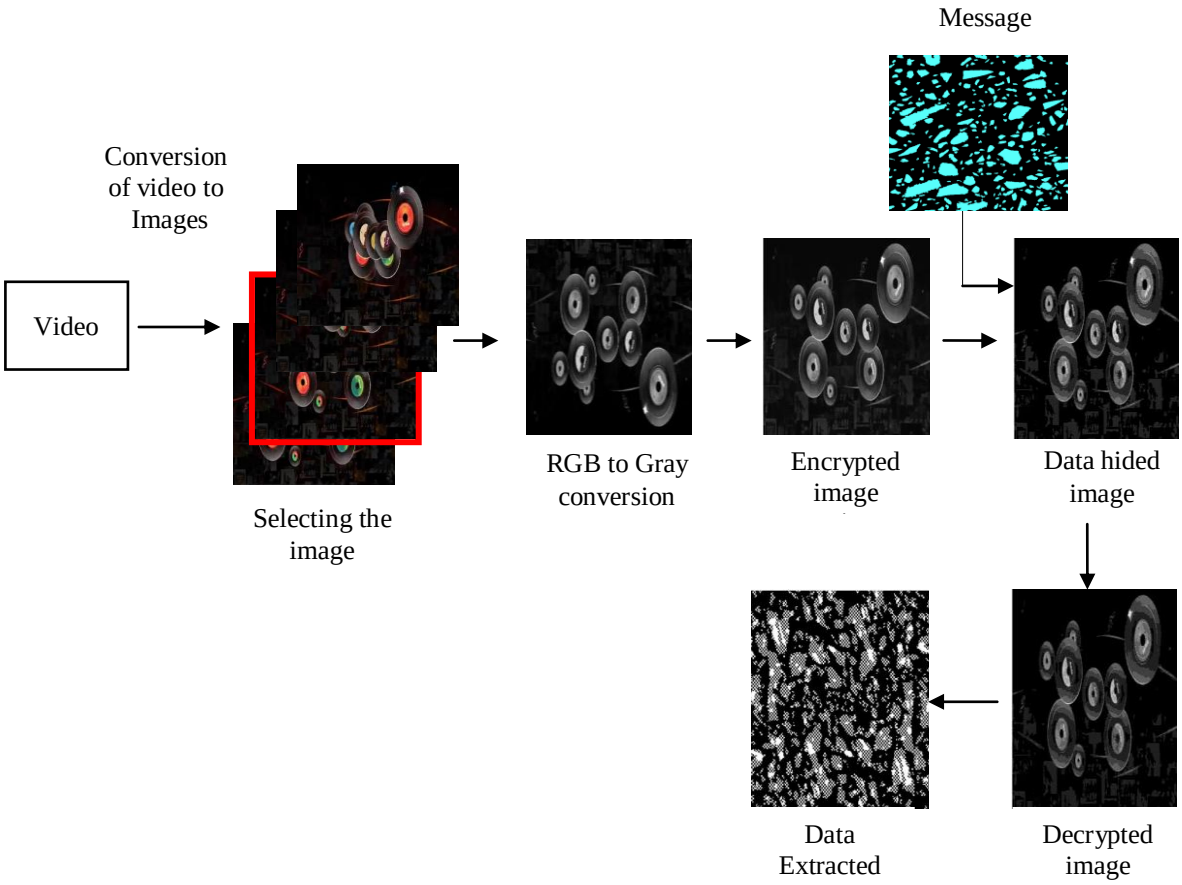

Fig. 6 Results obtained for sample video 1. In this figure we illustrate that video transmission in a secure way using LPC

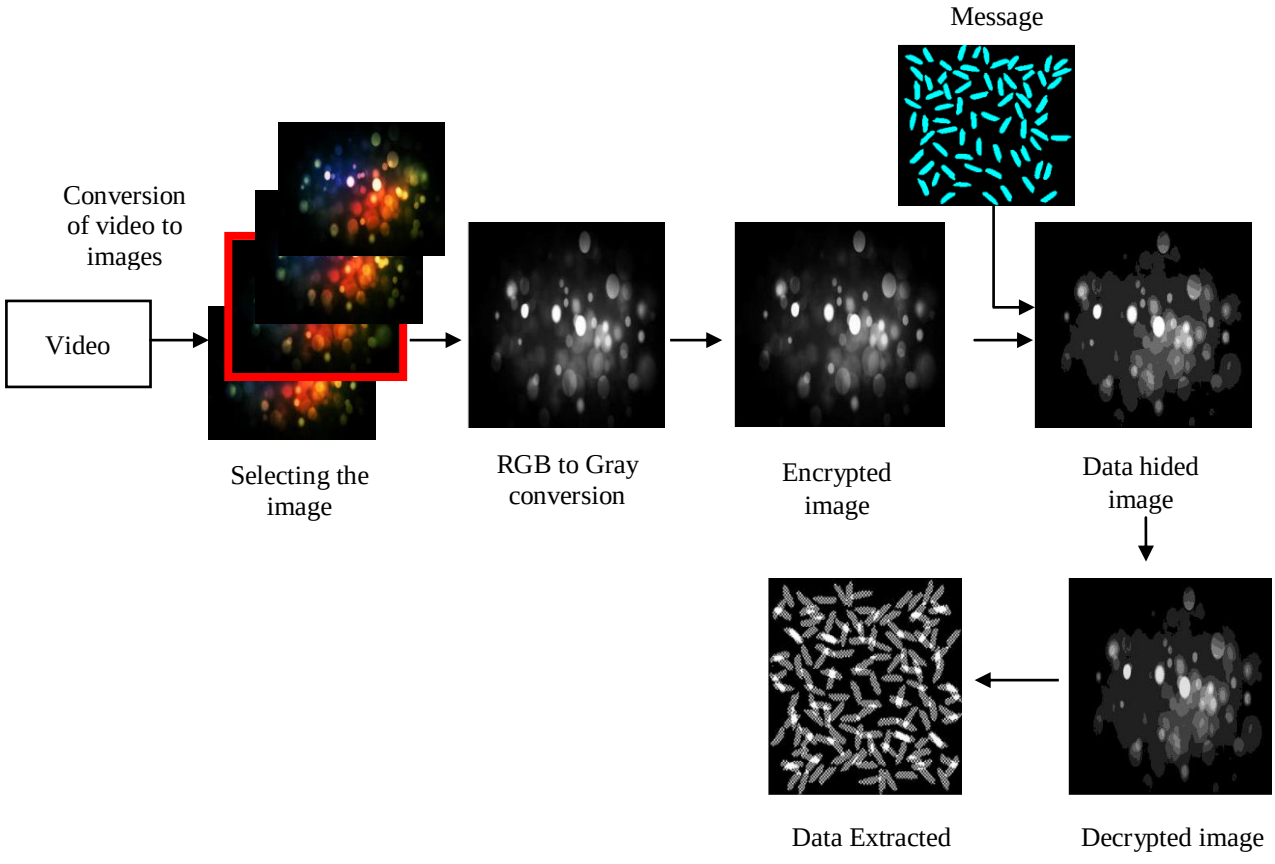

Fig. 7 Results obtained for sample video 2. In this figure we illustrate that video transmission in a secure way using LPC

ISSN: 2278 – 7798

TABLE I
Comparison of metrics for two sample videos

Input Image Sequences	Metric	Secure video transmission	Secure video transmission using LPC
Video 1	PSNR(dB)	53.1100	*58.4201*
	SSIM	0.9526	*0.9763*
	VQM	73.3172	*86.5691*
Video 2	PSNR(dB)	53.6638	*59.0113*
	SSIM	0.9489	*0.9745*
	VQM	72.6800	*86.2940*

V. RESULTS SUMMARY

In this section, the performance of the proposed technique is estimated. The video is transmitted in a very secure manner by using proposed method and compared with existing technique i.e. secure video transmission without using LPC technique. To measure the efficiency of our technique, PSNR, SSIM and VQM are calculated. We choose two sample videos to check the performance of the proposed method. We construct 30 high resolution frames for each sample video and perform our analysis.

In Table I, the PSNR, SSIM and VQM values for two sample videos for two techniques. The best value of each metric is italicized, which is resulted by using LPC technique. The proposed technique is always better choice for the secure video transmission which shows the feasibility of the algorithm. We have shown the simulated results for two sample videos compared with the secure video transmission technique without using LPC technique in Fig. 6 and Fig. 7. We can visualize from our results that confidential data is embedded and data is recovered effectively from encrypted video streams. The main program is executed in a fraction of 6 min on a 1.8 GHz Intel ® Core ™ i3 processor based minicomputer even for large sized images.

VI. CONCLUSION

The proposed technique is a novel method of secure video transmission where data is hided in encrypted video streams directly and the confidential information can be transmitted in a secure way. For hiding the data in encrypted H.264/AVC bit stream using an algorithm mainly consists of three steps which are encryption of video, data hiding and retrieval of data. The bit-rate can be preserved by method exactly even after encryption and data hiding and data extraction and the implementation is also simple. The additional data can be hided and confidential data can be greatly preserved since the data embedding is performed in encrypted domain directly. By using LPC algorithm in encryption module, it reduces the complexity compared to existing methods and bit rate alsopreserved. The merit is the full compliance with the syntax of
H.264/AVC. The results obtained experimentally reveals that the file size can be preserved by the proposed technique. By using data concealing, a very small degradation in video quality is caused. Various metrics are calculated and compared with existing method. We can deduce that the proposed technique gives better experimental results in terms of PSNR, SSIM and VQM. This work can be extended to along with additional data; audio signal can be embedded for more privacy so thatreliability will increase.

ACKNOWLDGEMENT

The authors express deep sense of thanks and gratitude to the Head of the Department, the supervisor, management and staff of MIC College of Technology for their inspiration and necessary technical suggestions during the research pursuit.

REFERENCES

[1] DawenXu, Rangding Wang and Yun Q. shi.fellow, " Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution", *IEEE Transactions OnInformation and Security*, Vol. 9, no. 4, Apr. 2014.

[2] N. Keshavanu, S. Ramachandran and K. S. Gurumurthy, "Implementation of Context Adaptive Variable Length Coder for H.264 Video Encoder", *International Journal of Recent Trends in Engineering*, Vol. 2, no. 5, Nov. 2009.

[3] Sangeeta Mishra, SAnjeevGhoshPayelSaha, "Chaos Based Encryption Tecnhique for Digital Images", Kandivali (E), Mumbai-400101.

[4] Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography", *International Journal of Applied Acience and Engineering, atternRecog*., Vol. 4, no. 3, pp. 275-290, 2006.

[5] T. Wiegand, G. J. Sullivan, G. Bjontegaard and A. Luthra, "Overview of the H.264/AVC Video Coding Standard", *IEEE Transactions On Circuit systems for Vidoe Technology*,Vol. 13, no. 7, pp. 560-576, ,Jul. 2003.

ISSN: 2278 – 7798

[6] Bibhudendra Acharya, Saroj Kumar Panigraphy, Sarat Kumar Patra and Ganapati Panda, "Image Encryption Using Advanced Hill Cipher Algorithm", *International Journal of Recent Trends in Engineering*, Vol. 1, no. 1, May. 2009.
[7] Zhang Yun-peng, Liu Wei, Cao Shui-ping, ZhaiZheng-jun, NieXuan and Dai Wei-di, "Digital Image Encryption Algorithm based on Chaos and improved DES", *International Conference on Systems*, Man and Cybernetics, 2009.
[8] Seyed Mohammad Seyedzade, Reza EbrahimiAtani and SattatMirzakuchaki, "A Novel Image Encryption Algorithm based on Hash Function", 6th Iranian Conference on Machine Vision and Image Processing, 2010.
[9] Ismail Amr, Mohammed Amin HossamDiab, "A Digital Image Encryption Algorithm based a Composition of Two Chaotic Logistic Maps", *International Journal of Network Security*, Vol. 11,, no. 1, pp. 1-10, Jul. 2010.
[10] A. Murat Teklap, "Digital Video Processing", Prentice Hall Signal Processing Series, Upper Saddle River, 1995
[11] Wenjun Lu, Avinash Varna and Min Wu, "Secure Video Processing:Problems and challenges", University of Maryland, College Park, USA.
[12] Arup Kumar Bhaumik, Minkyu Choi, Rosslini J Robles and Maricel O. Balitanas, "Data Hiding in Video*", International Journal of Data base theory and Application*, Vol. 2, no. 2, Jun. 2000.
[13] Yubing Wang, EMC corporation Hopkinton, "Survey of Objective Video Quality Measurements", MA 01748, USA
[14] Iain Richardson, "Vcodex White Paper:An Overview of H.264 Advanced Video Coding", 2007-2013
[15] Peter Meyer,"An Introduction to the use of Encryption"
[16] Yusra A. Y. AI-Najir and Dr. Der Chen Soong, " Comparison of Image Quality Assessment: PSNR, HVS, SSIM, UIQI*," International Journal of Scientific & Engineering*, Vol. 3, Issue 8, pp. 2229-5518, Aug. 2012.
[17] C. Saslvarnan, A. Jagan, Jaspreet Kaur, DivyaJyoti and Dr. D. S. Rao, " Image Quality Assessment Techniques on Spatial Domain," *International Journal of Computer Science and Technology*, Vol.2, Issue 3, pp. 0976-8491, Sep. 2011.
[18] Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, " Image Qaulity Assessment: From Error Visibilty to structural similarity," *IEEE Transcations on Image Processing*, Vol. 13, no. 4, pp. 600-612, Apr. 2004.
[19] Stallings, William, 2007. "Data and Computer Communications", 8th Edition, Upper Saddle River, N. J. : Pearson/Prentice Hall.
[20] R. C. Gonzalez and R. E. Woods, "Digital Image Processing," 2nd edition, Prentice-Hall, Inc. 2002, ISBN: 0-201-18075-8.
[21] Rafael C. Gonzalez, Richard E. Woods and Steven L. Eddins, "Digital Image Processing Using MATLAB", Pearson Education, Inc. 2004, ISBN 0-13-008519-7.

ISSN: 2278 – 7798