A Cryptographic based Approach for Data Hiding in Advanced Video Sequences

[1] **Vinay D R**, Research Scholar, Department of ISE, Malnad College of Engineering, Hassan, Karnataka 573201.
E-mail: vinu.ise@gmail.com

[2] **Dr. Anand Babu J,** Associate Professor, Department of ISE, Malnad College of Engineering, Hassan, Karnataka 573201.
E-mail: babu.tiptur@gmail.com

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract: Data hiding in video streams became more popular in the present world, since there is a high frequency of data communication over the internet. Hiding the data in video streams provides more security as well as increases embedding capacity than hiding inside the images. The quantity of information to be embedded into the video increases, it can badly influence the video excellence make it inappropriate for certain appliances. The main concerns in data hiding in videos are its high visual excellence, increased hiding capacity, video stream size etc. In this paper, a new data hiding technique is proposed in compressed H.264 Video Streams. At first, the information to be embedded is encrypted using Cryptography approach. The Cryptographic approach helps to encrypt the plain information based on the elliptic points produced by choosing the large prime number. The encrypted data is embedded into the transformed DCT coefficients of I, B and P video frames. The experiment is conducted for different set of video sequences. The results shows that the proposed method yields better performance in terms of Peak signal to noise ratio (PSNR), Structural similarity index (SSIM) and Video quality measure (VQM) when compare to existing methods.

Keywords: DCT (Discrete Cosine Transformation); Video Quality; Data Hiding; Video Streams; Watermarking; Cryptography Approach; PSNR value (Peak Signal Noise Ratio).

1. INTRODUCTION

The world exchanges information over communication channels during transmission. The correct data is delivered to destination matters during transmission. So, secure data transmission needs to be implemented in all parts of communication network. Data can get easily for third party or used by intruder for specific purpose. The method of embedding data into content is well known in data hiding technique without affecting its quality or features. This must lead to minimal degradation whenever tried to embed external data into all formats such as video, image, audio, text. Earlier, spatial or transform domain used by majority of data hiding techniques as a part of encoding. Besides, the access to video series originally is not at all viable and reclaims of the marked video to conceal required a diverse data. Initially bit stream to be decoded and to embed new data re encoding is preferred. Though it leads to degraded video quality because of lesser PSNR value is achieved during data hiding process. Apart from it, marked video cannot be get back using re encoding and decoding during real time.

Watermarking and Data hiding method are generally considered together since a watermarking method can provide as a data hiding method, even though the reverse is not at all feasible. Years ago, video data hiding techniques were motionless picture watermarking techniques used towards video by data hiding in every frame separately. The fundamental concept is to message distribution over large frequency range of original data. Data hiding approach wish to have transform domain because of equivalent robustness considered for spatial domain and the outcome added extra pleasant to human visual system (HVS).

Steganography is hiding data into existing data and helps to transfer data more securely. As on other end, cryptography plays a major role for added security. But steganography can’t be used to replace cryptography. The probability of data being detected is reduces by using steganography techniques. Cryptography methods helpful to provide additional security layer for protecting a data by encrypted message. Consequently, cryptography added with steganography to provide security at its best. The proposed paper concerns about security, video quality degradation and increasing embedded capacity and data hiding approach used elliptical curve cryptography in VIDEO stream.

2. LITERATURE SURVEY

[1] Proposed method gives the concept of contrast enhancement to improve video quality in AVC streams. The important thing here is to preserve file size of the video after applying contrast enhancement. Hence, objective of this paper is to have minimal video size for better visual quality. The frames were used to apply the contrast enhancement, so possibility of using it in different applications are getting increased such as medical imaging , satellite field and so on. As we all know application domains always preferred to follow file size preservation strategy with contrast enhancement for to achieve better results.

[2] Introduced simple and efficient method which suits well for video stream. Based on the message content to be hidden can be done by allocating macro blocks to divided group. The one more advantage is hiding message works for skipped and coded macro blocks and its well suited for constant bit rate (CBR) and variable bit rate (VBR). The technique uses 3 bits per macro block for message payload. The encryption algorithm such as AES (Advanced Encryption Standard) algorithm used further to enhance security and divided groups followed macro block allocation to hide the message bits twice. The work to be carried further to check the robustness of proposed technique and its resistance.

[3] In order to protect data, encryption plays a major role to protect video bit streams during transmission. In some cases, video are processed and stored in encrypted format for to continue its security. Hiding the data can be done straight away for encrypted form of video stream. The methods have been divided into three different steps such as Encryption of video stream, embedding and extraction of data. The following things were used for encryption with stream ciphers such as motion vector difference, code words of intra prediction modes and residual coefficients. The bit replacement method is used to embed extra data in encrypted domain without the knowledge of actual video content. To encrypt or decrypt secret text data, chaos crypto system is used.

[4] The concept of secure data communication can be achieved by using steganography. Based on the data combination of secret and cover images, this paper proposed a “non-blind data hiding technique”. The Discrete Cosine Transform (DCT) is used for the embedding process. H.264 compression can be applied for cover image in order to reduce spatial redundancy. The results shows that the given method stands as better technique not by imperceptibility and also it concern on capacity of hiding data. This method measured against different performance parameter and compared with early methods.

[5] The proposed method makes use of IPCM encoded macro blocks to hide the data during intra prediction process. This process is also called blind data hiding scheme. In the sense, without having original video the data to be taken out from encoded stream. Here the technique reveals the property of recycling the compressed stream to hide several data which doesn’t get affect for bit rate as well as perceptual quality. This particular method permits real time data hiding in compressed stream. The application areas like content authentication and covert communication will be best suited.

[6] Usually data management in cloud is tedious task due to privacy preserving requirements. This paper proposed technique to embed extra information in encrypted video bit stream. This algorithm helps us to preserve bit rate after encryption and used to carry out in encrypted and compressed domain. The encrypted bit stream is used to embed extra data using code word substitution without having original content of video. The encrypted domain is preferred to hide the data, it preserves confidentiality of video content, and it decreases the degradation of video quality due to data hiding.

[7] Tuneable data hiding is a method proposed in video streams. Due to some varying requirements of users, greater flexibility is provided. Furthermore, introduced the easiest operation to control the hiding capacity of secret message. To hold the secret message bits, single coefficient group selected from particular macro block. Finally it gives better results in terms of parameters such as PSNR and bit rate with minimum degradation.

[8] The process of embedding can be done on video data where the data is encrypted without having the knowledge or unknowing the decryption key. The combination of multiple base notation system and paired code word substitution are explained. The encrypted or decrypted domain chosen for data extraction.

[9] Proposed the Context adaptive binary arithmetic coding bin string substitution as a advanced scheme for hiding the data directly into video stream which is partially encrypted. With the residual encryption, encrypting luma prediction can also be designed leads to major improvement in structural deterioration. Since encrypted domain can be taken for data embedding, proposed technique preserves video confidentiality.

Among the steganography calculations for H.264 dependent on the intra expectation mode (IPM) [10-19], [10] adjusted the intra forecast mode dependent on the planning between the mysterious message and the expectation mode. [12] Enhanced the best expectation mode coordinating with strategy by utilizing the least Lagrangian cost. [13] Set up a planning between the data and intra forecast mode with grid coding. [14] Introduced a calculation dependent on [13] and used an installing/extricating lattice. Zhang et al. [16] built up a high security versatile installing calculation by utilizing STC (Syndrome-Trellis Code). To oppose the recognition from [18], [19] presented to limit embedding distortion‖ characterized by SAD (Sum of Absolute Difference).

3. METHODOLOGY

3.1 Elliptic Curve Cryptography

Elliptic curve cryptography is a cubic polynomial condition specified as follows

$$y^2 = x^3 + ax + b \tag{1}$$

Considering and as two positive whole numbers whose qualities are not exactly with and the two factors whose qualities are somewhere in the range of zero and (0<x<) individually. The estimations of a and b are picked to such an extent that they fulfil the state of segregate.

$$4a^3 + 27b^2 \; mod \; P \neq 0 \tag{2}$$

The value of a and b is selected to be a large prime number (>3).

The state of the elliptic curve fluctuates with various estimations of a and b. Elliptic bends are utilized for the public key cryptosystems (unbalanced encryption) where two unique keys where one for (public key) encryption and (private key) unscrambling are utilized. The Public key cryptosystems utilized with ECC are supreme in conditions such as low handling, smaller Bandwidth, less storage area and low power utilization. ECC are utilized to change over plain picture into an encoded picture and consider for limited prime area in which all math is carry out with modulo. The elliptic gathering incorporates the focuses for rigid estimations of a and b variable (<). For the example estimations of which fulfils the condition (2), the quadratic remainder are gotten for various estimations of a and b. The quantity of a and b focuses in the quadratic residues is equivalent to zero. For the current estimation of residues, there are two distinct focuses in the EP gathering. In ECC, every pixel in the plain picture is planned into a point from the elliptic gathering. At that point for each estimation of x, decide whether a place with the arrangement of quadratic build-ups has. Assuming it has a place, mark two focuses in the elliptic gathering one with (x1, y1) and another with (x2, y2). The figure 1. Shows how the elliptic gathering points are dispersed

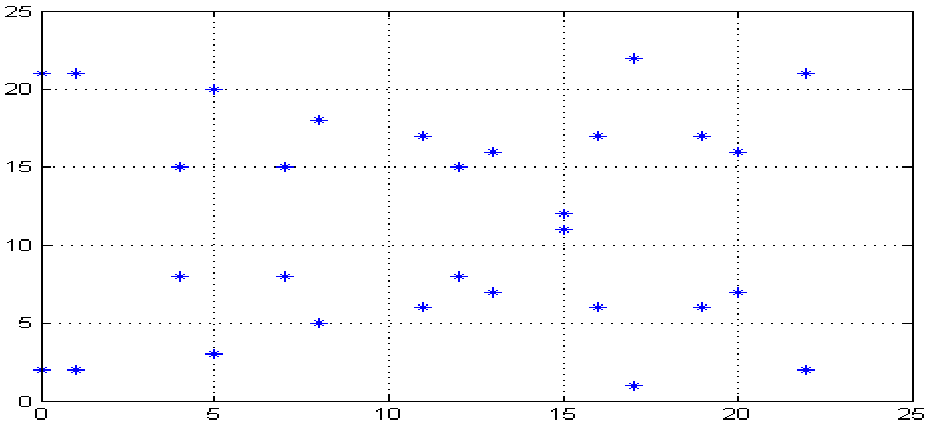

Figure 1. Scatter plot of elliptic group

The complete set of points in the EC along with the point at boundlessness 'O' (both x and y are ∞) is the request for the elliptic curve meant by M. The littlest number worth N for which the result of N and P is equivalent to point at 'O' (NP=O) is the request for point P to such an extent that N≤M. At that point the focuses P, 2P, 3P…(N-1)P is obvious on the EC. The public key is a point on the curve, while a private key is an irregular number created by owner. Client A chooses private key n_A <N. The public key P_A is determined as P_A= n_A G and PB= n_B G. Where n_A and n_B are the private keys of gathering An and B separately. G is a generator guide having a place toward an elliptic gathering, the result of n and G yields an extremely enormous indivisible number O. EP (a, b) and G are disclosed in the ECC.

In the encryption of a pixel estimation of the plain picture, the sender picks an irregular number K and decides the cipher picture point group PC.

$$P_C = [(KG), (P_M + KP_B)] \tag{3}$$

Where PM is the plain picture pixel and PB is the receiver's public key. The encryption interaction in ECC likewise incorporates finding the summation and result of elliptic focuses on the elliptic curve.

3.1.1 Addition and Multiplication of Elliptic Points

Expecting P and Q be two focuses on EP (a,b) and O the infinity point. The expansion technique utilized is P+O=P

1. If Q=-P i.e. P(x_1, y_1), Q(x_2, y2) =(x_1,-y_1) =-P, then P+Q=O.
2. If Q≠-P, then P+Q=(x_3,y_3)

   Where x_3=$\lambda^2 - x_1 - x_2$ mod P (4)

   Y_3=$\lambda(x_1 - x_3) - y_1\ mod\ P$ (5)

   Where $\lambda \cong \frac{y2-y1}{x2-x1}$ if P≠ Q

   $\frac{3x_1^2+a}{2y_1}$ If P= Q

The multiplication KG in the above condition is rehashing the expansion of the point G for K number of times utilizing the conditions (4) and (5).The starting value for a and b are - 1 and 188. Where the indivisible numeric P is equivalent to 751.

3.2 Data Hiding

The encrypted data obtained from ECC encryption is converted into stream of binary bits for hiding. The raw YUV video file contains a sequence of frames. Let be the sequence of original video where is the total number of frames. Each frame consists of two Chroma components namely Cb, Cr and one luma component Y. These entire components are compressed using H.264 encoder. The compression process is carried out by organizing the frames into frames, frames and frames. Where the reference is frame, and is the predicted frames.

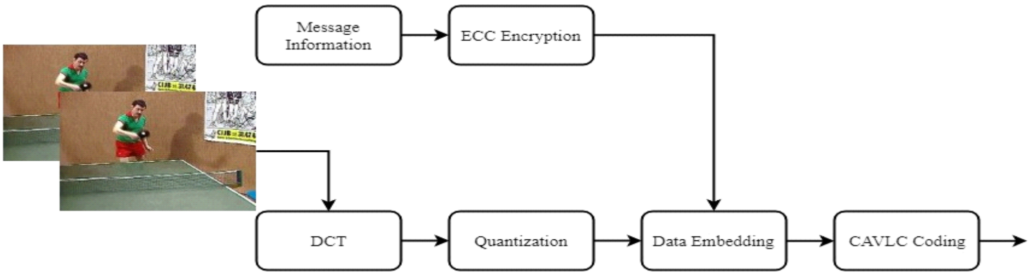

Figure 2. Detailed Block Diagram of Proposed Work

Data can be hidden into all the I, P and B −frames of F. Here we select only I −frames to embed the encrypted bits stream. Let $I = \{ I_1, I_2, I_3 \dots \dots . . I_m\}$ be the total number of I −frames in a video file, where $m < n$. As we know with I, each I −frame contains Y, C_b and C_r Component, let $I_i = \{Y^i, C_b^i, C_r^i\}$ and we are considering Y^i component for embedding the encrypted data. Here each Y^i component of size $n_1 * n_2$ is dived into 8x8 blocks of intensity values. Let$Y^i = \{B_1^j, B_1^j \dots \dots \dots B_l^j\}$, where B_l^j is the j^{th} 8x8 and$l = \frac{(n1*n2)}{64}$. The 8x8 non-overlapping blocks are transformed into 2-dimensional DCT as follows.

$$F_{(u,v)} = \frac{\alpha(u)\alpha(v)}{4} \sum_{x=0}^{7} \sum_{y=0}^{7} B_i^j\,(x,y)\hat{g}(x,y,u,v) \quad (6)$$

$$z\hat{g}(x,y,u,v) = \cos\left(\frac{(2x+1)u\pi}{16}\right) cos\left(\frac{(2y+1)u\pi}{16}\right) \quad (7)$$

$$\alpha(e) = \begin{cases} \frac{1}{\sqrt{2}}\ if\ e = 0 \\ 1\ if\ e \neq 0 \end{cases} \quad (8)$$

Here the value of u, v lies between 0 to 7 and $B_l^j(x,y)$ symbolize the intensity value of pixel.$F_{u,v}$ Signify the coefficients in transform field obtained after pertaining DCT. The inverse DCT is taken by using below equation

$$B_i^j(x,y) = \sum_{u=0}^{7}\sum_{v=0}^{7}\frac{\alpha(u)\alpha(v)}{4}F_{(u,v)}\,\hat{g}(x,y,u,v) \tag{9}$$

4. EXPERIMENTAL RESULT

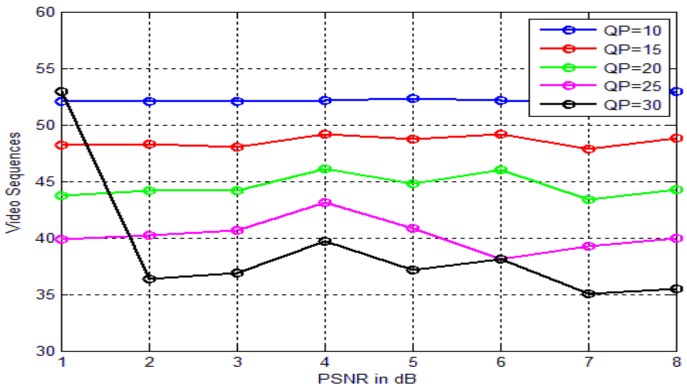

Figure 3. Shows the variation of PSNR in dB for different values of QP for different Video

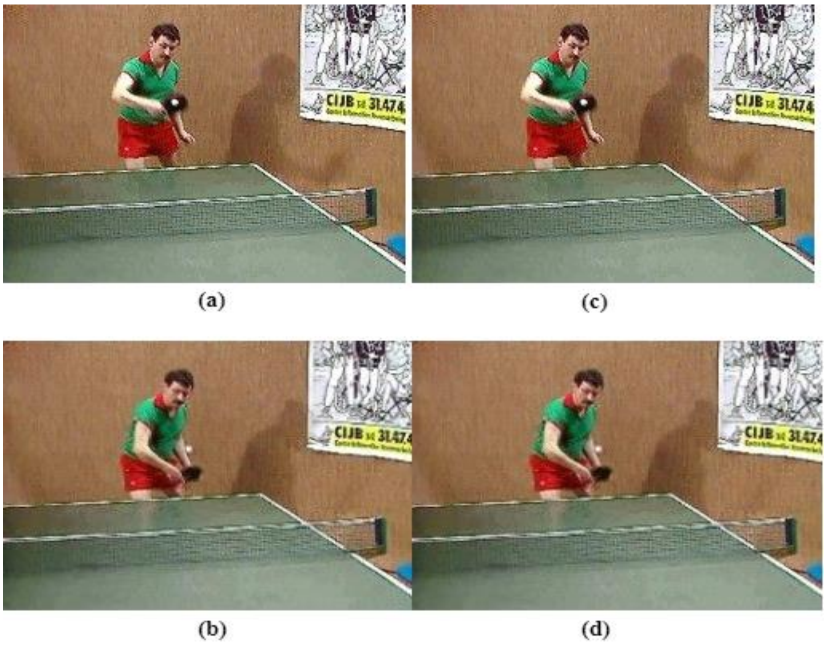

Figure 4. (a) and (b). Original Video Frame from input Video.

(c) and (d). Video Frame Containing Data

QP=10

Video File Name	PSNR	SSIM	VQM
Foreman	52.1028	0.9999	0.9999
Grandma	52.0600	0.9998	0.9998
Hall_Monitor	52.0678	0.9999	0.9991
Miss_America	52.1418	0.9998	0.9997

Mother_Daughter	52.3065	0.9992	0.9994
News	52.1574	0.9994	0.9996
Salesman	52.0097	0.9998	0.9996
Tennis	52.9511	0.9999	0.9992

QP=15

Video File Name	PSNR	SSIM	VQM
Foreman	48.2101	0.9998	0.9996
Grandma	48.2845	0.9996	0.9994
Hall_Monitor	48.0670	0.9997	0.9999
Miss_America	49.1253	0.9995	0.9994
Mother_Daughter	48.7262	0.9997	0.9995
News	49.1675	0.9998	0.9996
Salesman	49.8919	0.9995	0.9993
Tennis	48.8355	0.9999	0.9991

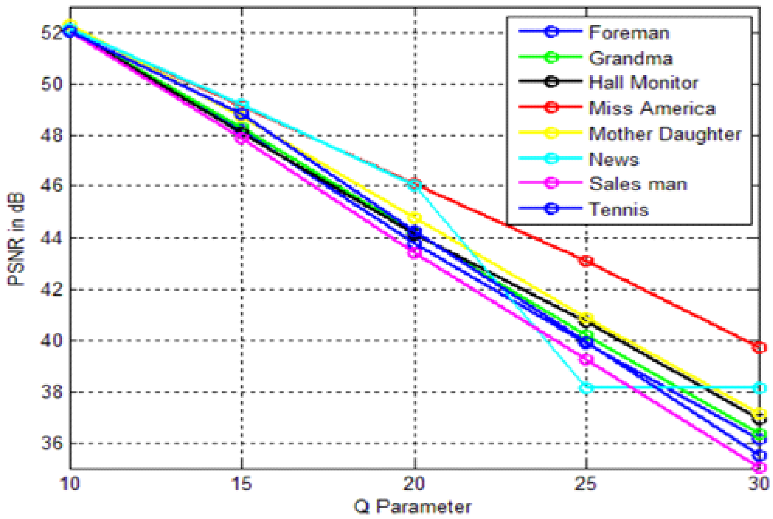

Figure 5. Shows the variation of PSNR in dB different values of QP for different Video sequences.

QP=20

Video File Name	PSNR	SSIM	VQM
Foreman	43.7678	0.9995	0.9993
Grandma	44.2027	0.9989	0.9990
Hall_Monitor	44.1522	0.9994	0.9991
Miss_America	46.0738	0.9990	0.9991
Mother_Daughter	44.7483	0.9992	0.9993
News	46.0116	0.9997	0.9996
Salesman	43.4084	0.9987	0.9986
Tennis	44.2333	0.9996	0.9995

QP=25

Video File Name	PSNR	SSIM	VQM
Foreman	39.8748	0.9988	0.9990
Grandma	40.1937	0.9972	0.9971
Hall_Monitor	40.6994	0.9987	0.9985
Miss_America	43.1035	0.9981	0.9980
Mother_Daughter	40.8576	0.9980	0.9979
News	38.1108	0.9980	0.9981
Salesman	39.2368	0.9965	0.9962
Tennis	39.9440	0.9989	0.9976

QP=30

Video File Name	PSNR	SSIM	VQM
Foreman	36.1356	0.9972	0.9976
Grandma	36.3205	0.9931	0.9937
Hall_Monitor	36.9241	0.9968	0.9964
Miss_America	39.7026	0.9959	0.9963
Mother_Daughter	37.1158	0.9952	0.9959
News	38.1108	0.9980	0.9981
Salesman	35.0037	0.9908	0.9915
Tennis	35.5062	0.9969	0.9970

QP=35

Video File Name	PSNR	SSIM	VQM
Foreman	39.8748	0.9988	0.9990
Grandma	40.1937	0.9972	0.9971
Hall_Monitor	40.6994	0.9987	0.9985
Miss_America	43.1035	0.9981	0.9980
Mother_Daughter	40.8576	0.9980	0.9979
News	38.1108	0.9980	0.9981
Salesman	39.2368	0.9965	0.9962
Tennis	39.9440	0.9989	0.9976

5. DISCUSSION

In this study, a new data hiding technique has proposed for the compressed H.264 video streams using an efficient algorithm called ECC. The outcomes of this proposed method can be compared based on three different performance measures such as PSNR, SSIM and VQM. This proposed data hiding technique has implemented based on six different QP values. While comparing with the other data hiding methods, these outcomes of this proposed methodology shows that it yields better performance in terms of PSNR, SSIM and VQM.

6. CONCLUSION

A new data hiding technique is proposed in compressed Advanced Video Streams. The method involves increasing the Data security by encrypting the information using Cryptographic approach before embedding the information. Data hiding inside transformed DCT coefficients has an advantage that it adds more security. The proposed method yields increased PSNR as there is data embedded into LSB bits of the transformed DCT Coefficients. Further, the method also exhibits high embedding capacity as well as lesser distortion in marked video. Simulation outcome disclose that the perceptual excellence is conserved without surrendering coding efficiency.

References

[1]. M. Lakshmi, K.P. Arjun, N. M. Sreenarayanan, K.A. Arya, (2016).*Reversible Data Hiding in Videos for Better Visibility and Minimal Transfer*, Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology (RAEREST 2016) Procedia Technology, Elsevier 25: 256 – 263.

[2]. M. Lathikanandini, J. Suresh, (2013).*Steganography in MPEG Video Files using MACROBLOCKS*, International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970.

[3]. S.A.Chaudhari , Prof. M.D.Bagde, (2015).*Review on Secret Data Hiding in Encrypted Compressed Video Bit Streams*, International Journal of Computer Science Trends and Technology (IJCST) – 3(2).

[4]. S. Hamad and A. Khalifa, (2015).*Non-blind Data hiding for RGB images using DCT-based fusion and H.264 compression concepts*, ACSIJ Advances in Computer Science: an International Journal, 4(3)(15) ,ISSN : 2322-5157.

[5]. S. K. Kapotas and A.N. Skodras, (2008).Spyridon K. Kapotas Athanassios N. Skodras", Springer-Verlag.

[6]. K. Mogaparthi, T. Alle, V. Anand, Aka.Ramteke,(2015). Data *Hiding in Encrypted VIDEO Video Streams*, International Journal of Engineering Research and Reviews ISSN 2348-697X (Online) Vol. 3, Issue 2, pp: 71-80.

[7]. W-S.Wang, Y-C. Lin, (2015). *A Tunable Data Hiding Scheme for CABAC in H.264/AVC Video Streams*, IEEE, 2015.

[8]. D. Xu, R. Wang, Y. Q. Shi, (2016).*An Improved Scheme for Data Hiding in Encrypted H.264/AVC Videos*.Elsevier, J. Vis. Commun. Image R.

[9]. D. Xu , R. Wang , Y. Zhu, (2017).*Tunable data hiding in partially encrypted H.264/AVC videos*, Elsevier, J. Vis. Commun. Image R. 45: 34–45.

[10]. HU, Yang; ZHANG, Chun-tian; SU, Yu-ting.(2008).*Information hiding for H.264/AVC*. Acta Electronica Sinica,36.4: 690.

[11]. Wang, R., Zhu, H., & Xu, D. (2010).*Information hiding algorithm for H.264/AVC based on encoding mode*. Opto-Electronic Engineering,37(5), 144-150.

[12]. Xu, D. W., Wang, R. D., & Wang, J. C. (2014).*Prediction mode modulated data-hiding algorithm for H.264/AVC*. Journal of Real-Time Image Processing,7(4), 205-214.

[13]. Yang, G. B., Li, J. J., He, Y. L., & Kang, Z. W. (2011).*An information hiding algorithm based on intra-prediction modes and matrix coding for H.264/AVC video stream*. AEU-International Journal of Electronics and Communications, 65(4), 331-337.

[14]. Yin, Q., Wang, H., & Zhao, Y. (2012).*An information hiding algorithm based on intra-prediction modes for H.264 video stream*. Journal of Optoelectronics. Laser, 2012, 23(11), 2194-2199.

[15]. Bouchama, S., Hamami, L., Aliane, H. (2012).*H.264/AVC data hiding based on intra prediction modes for real-time applications*. Lecture Notes in Engineering and Computer Science, vol. 1, 655-658.

[16]. Zhang, L., Zhao, X. (2016).*An adaptive video steganography based on intra-prediction mode and cost assignment*. IWDW 2016. LNCS, vol. 10082, pp. 518–532.

[17]. Wang Y, Cao Y, Zhao X, et al. (2017).*A prediction mode-based information hiding approach for H.264/AVC videos minimizing the impacts on rate-distortion optimization*. International Workshop on Digital Watermarking. Springer, Cham, 163-176.

[18]. Zhao, Y., Zhang, H., Cao, Y., Wang, P., Zhao, X. (2015).*Video steganalysis based on intra prediction mode calibration*. 2015 International Workshop on Digital-forensics and Watermarking, 119-133.

[19]. NIE, Qiankai, et al. (2018).*Defining Embedding Distortion for Intra Prediction Mode-based Video Steganography*. Computers, Materials & Continua,55.1: 59-59