ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

Secrete Data Hiding In H.264/AVC Compressed Video Bitstreams for Private Data Protection

Bhagyashri Raut, Prof.V.B.Raskar

ME Student, Department of Electronics and Telecommunication Engineering, Imperial College of Engineering and Research, wagholi, Pune, India.

Assistant Professor, Department of Electronics and Telecommunication Engineering, Imperial College of Engineering and Research, wagholi,Pune, India.

ABSTRACT: Video authentication has become an rising issue for video streaming over lossy networks.Though the advanced video secret writing standards, such as H.264/AVC, expeditiously cut back the quantity of knowledge to be transmitted, the secret writing dependency brings new challenges in planning economical stream authentication theme. In this paper, we tend to propose a completely unique joint-designed-layered supply–channel adaptive theme that integrates authentication into source and channel secret writing parts to sufficiently use the connected data to expeditiously address the secret writing dependency and to style the best rate allocation theme for the sake of end-to-end video quality. The projected stratified framework is in a position to attenuate end-to-end quality degradation incurred by each the wireless channel noise and therefore the authentication failure. Specially, the competitory needs of high verification likelihood and low authentication overhead are at the same time happy by the elegant style of stratified hash appending with economical adaptation to the H.264 supply secret writing and channel conditions. A joint source–channel-authentication rate allocation theme is then developed to realize best end-to-end video quality. The experimental results on H.264 video sequences make sure the effectiveness of this joint adaptive theme and demonstrate that it so outperforms the progressive graph-based authentication algorithms.

***KEYWORDS*:**Internet of Things; Raspberry pi;Wireless sensor network (WSN);AndroidSmart phones;Cloud;

I. INTRODUCTION

Video encoding has been heavily researched at intervals the recent years. Digital videos are the very standard owing to their frequency on their net. There are varied techniques are gift for activity personal info in videos. Digital video should be hold on in encrypted format. To save videos throughout transmission or cloud storage, coding of compressed video bit streams and activity privacy knowledge is finished. For the aim of content notation and or change of state these it's a necessity to perform info activity in these encrypted video. With the rising of net and transmission applications in distributed environments, it becomes easier for digital knowledge house owners to transfer transmission documents across everyplace the globe via cyber web. Secure adaptation wants a ascendible bitstream and specific coding routines that preserve the quality at intervals the encrypted domain. Cloud computing has become a really vital technology trend, which can provide very economical computation and large scale storage resolution for video knowledge. But cloud services might attract lots of attacks and unit at risk of undependable system administrators, it's desired that the video it's desired that the video content is accessible in encrypted type. The aptitude of performing arts knowledge activity directly in encrypted H.264/AVC video streams would avoid the outpouring of content, which may facilitate address the protection and privacy issues with cloud computing [1].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

II. RELATED WORK

Buyer-seller watermarking protocols

Till now, few triple-crown information concealing schemes within the encrypted domain are found within the open literature.[6] A watermarking theme exploitation Parlier cryptosystem is projected supported the protection needs of buyer-seller watermarking protocols[4]. In Walsh-Hadamard remodel image watermarking algorithmic rule is employed within the encrypted domain exploitation Paillier cryptosystem is given [4]. However, owing to the constraints of the Paillier cryptosystem, the coding of an imaginative image shows high overhead in storage and computation. Note that, many researches on reversible information concealing in encrypted pictures are found recently. The coding is performed by exploitation bit-XOR operation. In these strategies, the host image is in associate uncompressed format.

Conventional LSB replacement scheme

In June 2009, Arup Kumar Bhaumik, Minkyu Choi, RosslinJ.Robles, and MaricelO.Balitanas [3]proposed a knowledge concealment and extraction procedure for prime resolution AVI (Audio Video Interleave) videos. They diagrammatical 2 totally different procedures, that square measure used at the sender‘s finish and receiver‘s finish severally. The procedures square measure used because the key of knowledge concealment and Extraction. at first stream the video and collect all the frames in ikon format, and collect the knowledge like beginning frame, beginning macro block, range of macro blocks and frame amount. Then author have used standard LSB replacement with multiple bit planes.

Motion estimation process scheme

In the year 2007, Spyridon K. Kapotas, Eleni E. Varsaki and Athanassios N. Skodras [2] planned technique that takes blessings of varied block sizes employed by the H.264 encoder throughout the entomb prediction stage to cover the fascinating information. It's blind information concealing theme which means information will be reconstructed directly from encoded stream. The foremost necessary a part of entomb prediction is motion estimation method. That aims at finding macroblock of current frame. Then every macroblock, among the present frame, is motion paid i.e. its best match is deducted from it, and also the residual macroblock is coded.

III. PROPOSEDSYSTEM

We are using ultrasonic sensor algorithm is basically used for detection of an obstacle. If any obstacle comes in between the sensors that detects displays as result. We are going to set the distance, if the distance increases beyond particular range message will be displayed. This way the algorithm works.

a) Video encryption and data Hiding

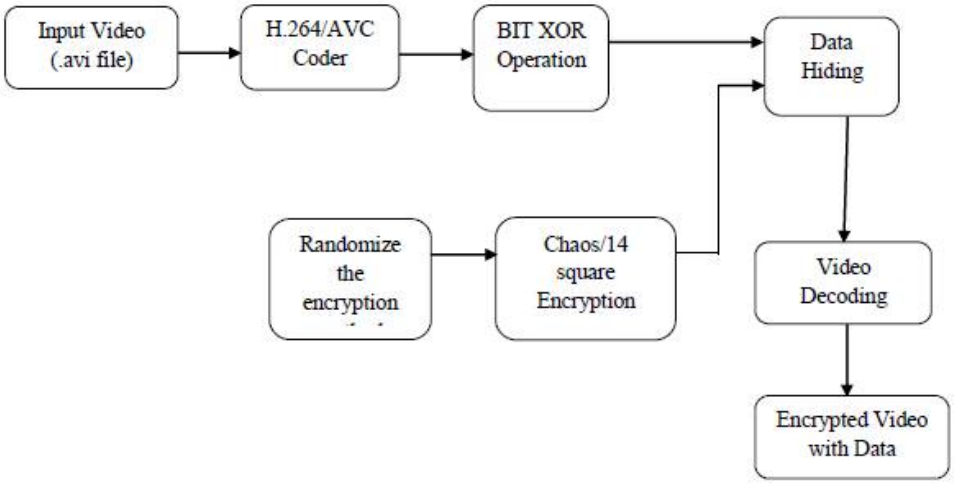


Fig1: Proposed System Architecture

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

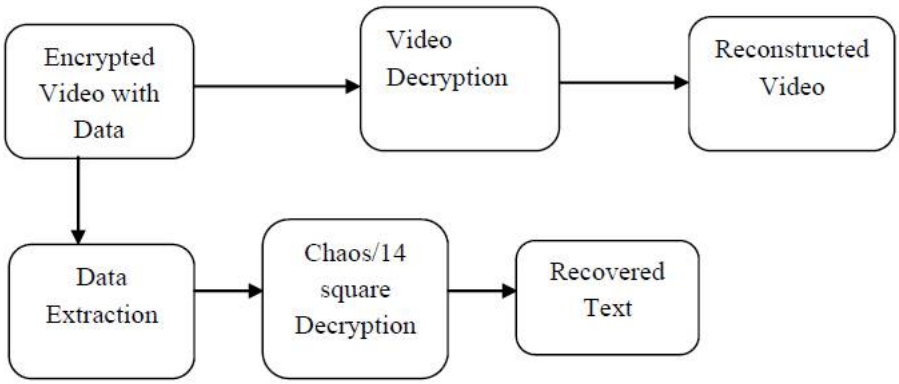
(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

The system implementation steps can be summarized from the above diagram as below:
Step 1: Input the video (.avi) and convert it into frames.
Step 2: Apply H.264 coding to the frames.
Step3: Select the secret images to be processed and encrypt it.
Step 4: Select the input data information encrypt it with chaos encryption/14 sqare and embed the data into the Frames
Step 5: Enter data hiding key and enter the encryption password and encrypt the H.264 Coded frames
Step 6: Convert frames to video to get encrypted video with hidden data

b) Data Extraction and Video Decryption



Step 1: Load encrypted video with hidden data and convert it into frames
Step 2: Apply H.264 decoding to the frames.
Step3: Enter the decryption password and decrypt the H.264 coded frames
Step 4: Enter data hiding key and extract the data (secret image) from the frames.
Step 5: Display the secret image.
Step 6: Convert frames back to the original video

The System presents that cryptography of compressed video bit streams and concealment privacy data to shield videos throughout transmission or cloud storage. Digital video typically must be keep and processed in an encrypted format to take care of security and privacy. Information concealment approach is critical to perform in these encrypted videos for the aim of content notation and meddling detection. During this approach, information concealment in encrypted domain while not secret writing preserves the confidentiality of the content. Additionally, it's a lot of economical while not secret writing followed by information concealment and re-encryption. Here, information concealment directly within the encrypted version of H.264/AVC video stream is approached, which incorporates the subsequent 3 elements, i.e., H.264/AVC video cryptography, information embedding, and information extraction.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

IV.RESULTS

Encryption Process

Step 1: Provide (.avi) Input video and convert the video in to frames/images

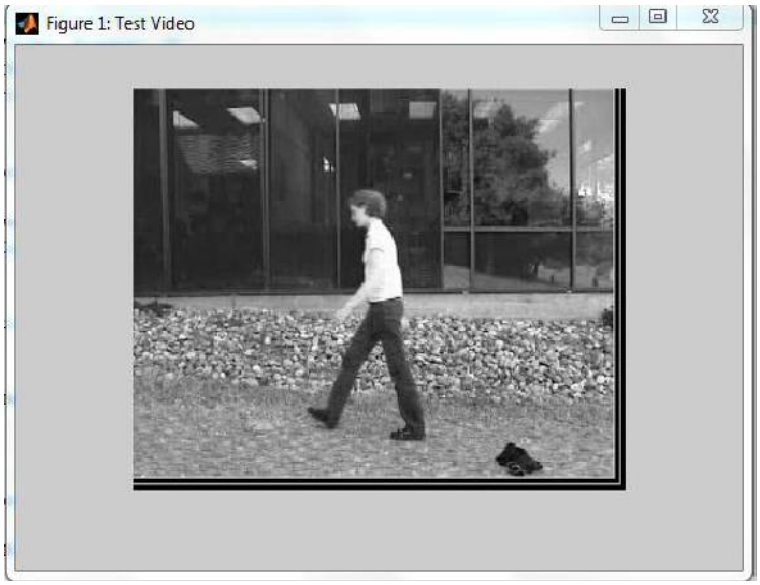


Fig:Input test video

Step 2: Implement H.264 coding to the separated video frames.

Step3: Select the secret images to be processed and encrypt it.

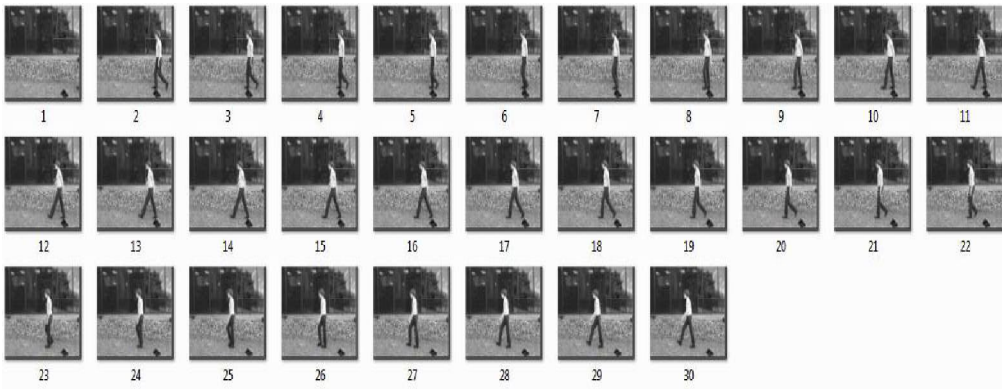


Fig:Frame Separation Logic

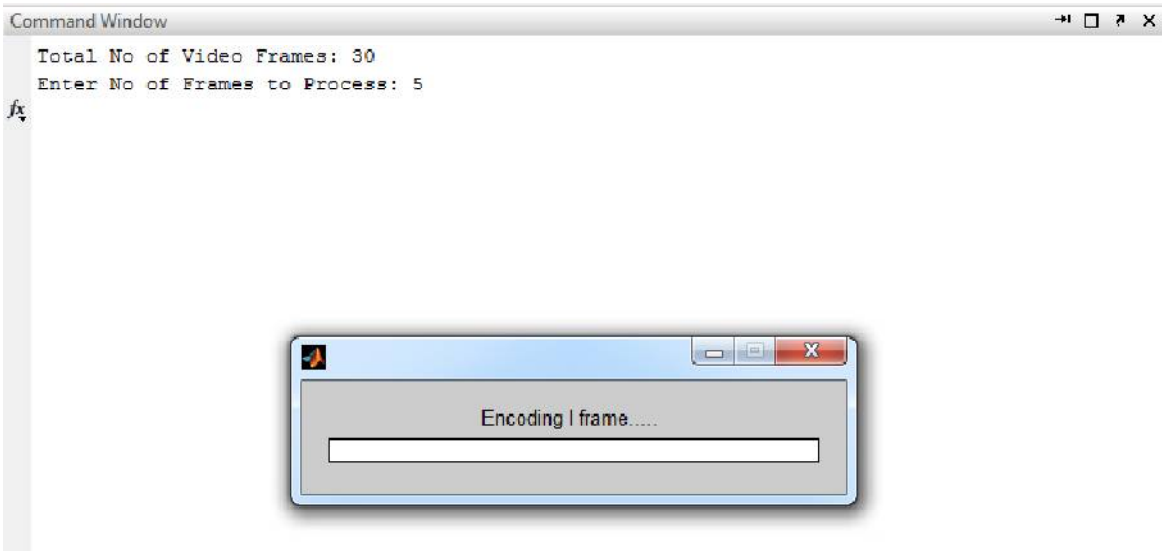
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

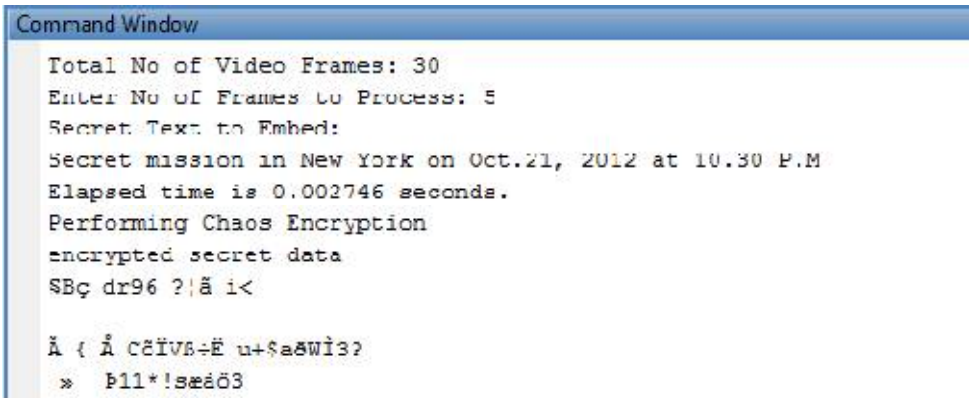
(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017



Step 4: Select the input data information encrypt it with chaos encryption/twelvesquare substitution based on the random key number and embed the data into theFrames
Step 5: Encode the data logic levels to generate the data hiding key and to encrypt the H.264 frames



Step 5: Encode the data logic levels to generate the data hiding key and to encrypt the H.264 frames
Step 6: Convert frames to video to get encrypted video with hidden data

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

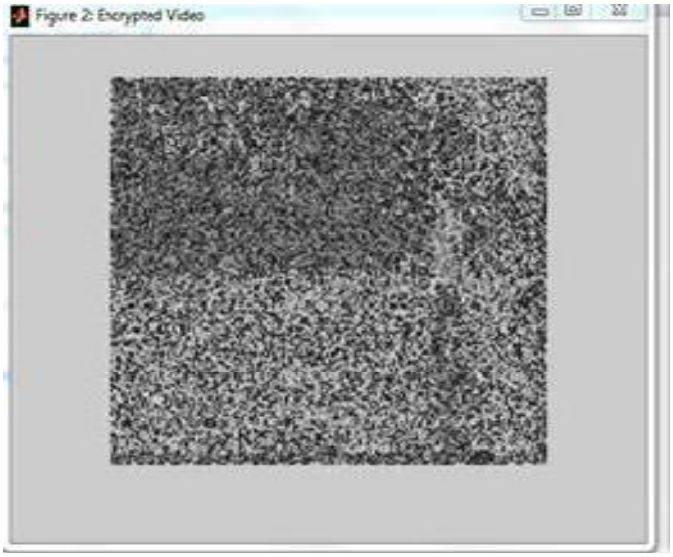


Fig.:Encrypted video with hidden data

Decryption Process

Step 1: Load encrypted video with hidden data and convert it into frames
Step 2: Apply H.264 decoding to the frames

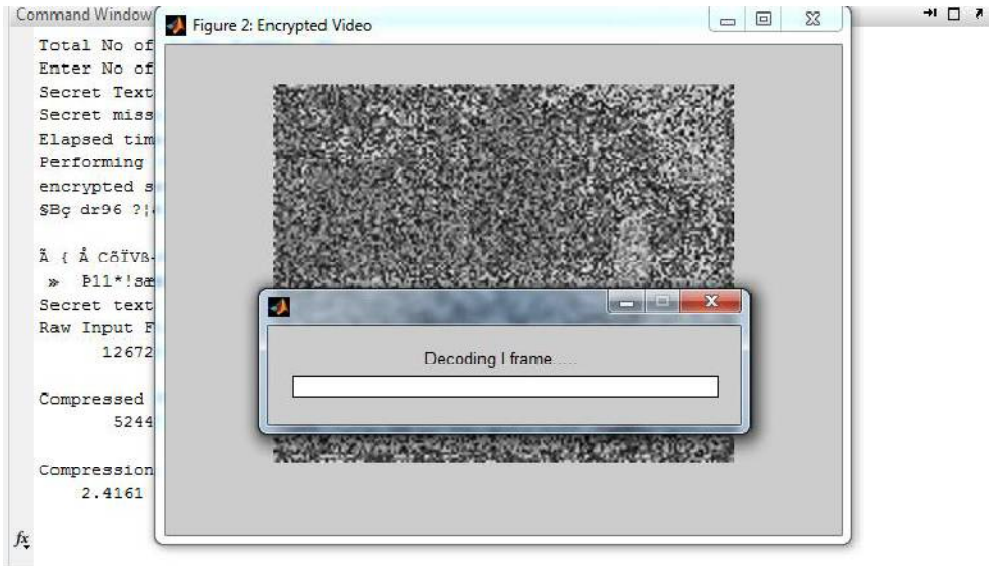


Fig:Encrypted video with hidden data for Decryption Process

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

Step 3: Decode the data logic(decryption method selected based on random key number) levels to extract the hiding key and extract the data (secret image) from the frames.
Step 4: Display the secret text data output from decryption process.

Fig:Decryption method

Performance ParametersEvaluation with variation in QP(Quantisation Parameter)
The number and values of the applicable quantizer step sizes during a video writing is restricted. The applicable quantizer step size is typically indicated by the quantisation parameter (QP), that is associate index to a predefined set of applicable quantisation step sizes. Commonly, low quantisation parameters correspond to fine quantisation and high quantisation parameters correspond to coarse quantizer step sizes. A high roughness of the quantizer step sizes is useful to permit for precise rate management within the encoded bit stream. On the opposite hand, the signalling for a high range of obtainable quantizer step sizes induces extra cryptography price, that must be thought of. The specification should balance roughness and cryptography price.

Case 1: Quantisation Parameter QP =5

Table :Performance Analysis for Both encryption methods at QP= 5

S.no	Input Video	QP	MSE		PSNR		Correlation		Percentage Residual Difference		Structure Similarity Index	
			chaos	14 square	chaos	14 square	chaos	14 square	chaos	14 square	chaos	14 square
1	inp.avi	5	0.0614	0.0614	60.2523	60.2523	1	1	0.0153	0.0153	0.9995	0.9995
2	inp2.avi		0.0542	0.0542	60.7897	60.7897	1	1	0.015	0.015	0.9991	0.9991
3	inp3.avi		0.0548	0.0548	60.7425	60.7425	1	1	0.0143	0.0143	0.9995	0.9995
4	inp4.avi		0.0505	0.0505	61.0941	61.0941	1	1	0.0147	0.0147	0.999	0.999
5	inp5.avi		0.0517	0.0517	60.9968	60.9968	1	1	0.0145	0.0145	0.9993	0.9993
6	inp6.avi		0.058	0.058	60.4934	60.4934	1	1	0.0148	0.0148	0.9992	0.9992
7	inp7.avi		0.0598	0.0598	60.3626	60.3626	1	1	0.0153	0.0153	0.999	0.999

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

Case 2: Quantisation Parameter QP = 10

Table:Performance Analysis for Both encryption methods at QP= 10

S.no	Input Video	QP	MSE		PSNR		Correlation		Percentage Residual Difference		Structure Similarity Index	
			chaos	14 square	chaos	14 square	chaos	14 square	chaos	14 square	chaos	14 square
1	inp.avi	10	0.1848	0.1848	55.4643	55.4643	0.9999	0.9999	0.0276	0.0276	0.9986	0.9986
2	inp2.avi		0.1752	0.1752	55.6947	55.6947	0.9999	0.9999	0.0262	0.0262	0.9971	0.9971
3	inp3.avi		0.181	0.181	55.5533	55.5533	1	1	0.0261	0.0261	0.9983	0.9983
4	inp4.avi		0.1621	0.1621	56.0322	56.0322	0.9999	0.9999	0.0261	0.0261	0.9977	0.9977
5	inp5.avi		0.157	0.157	56.1707	56.1707	0.9999	0.9999	0.0244	0.0244	0.9971	0.9971
6	inp6.avi		0.177	0.177	55.65	55.65	0.9999	0.9999	0.0258	0.0258	0.9978	0.9978
7	inp7.avi		0.1748	0.1748	55.7055	55.7055	0.9999	0.9999	0.0266	0.0266	0.9972	0.9972

Case 3: Quantisation Parameter QP = 24

Table :Performance Analysis for Both encryption methods at QP= 24

S.no	Input Video	QP	MSE		PSNR		Correlation		Percentage Residual Difference		Structure Similarity Index	
			chaos	14 square	chaos	14 square	chaos	14 square	chaos	14 square	chaos	14 square
1	inp.avi	24	2.956	2.956	43.4238	43.4238	0.9989	0.9989	0.1115	0.1115	0.9826	0.9826
2	inp2.avi		2.0184	2.0184	45.0807	45.0807	0.9994	0.9994	0.0903	0.0903	0.9746	0.9746
3	inp3.avi		2.6977	2.6977	43.8208	43.8208	0.9993	0.9993	0.1037	0.1037	0.9798	0.9798
4	inp4.avi		2.266	2.266	44.5782	44.5782	0.9988	0.9988	0.0975	0.0975	0.9726	0.9726
5	inp5.avi		1.6475	1.6475	45.9627	45.9627	0.9992	0.9992	0.0809	0.0809	0.9755	0.9755
6	inp6.avi		2.432	2.432	44.2711	44.2711	0.999	0.999	0.0962	0.0962	0.9777	0.9777
7	inp7.avi		2.2594	2.2594	44.5908	44.5908	0.9983	0.9983	0.0954	0.0954	0.9669	0.9669

Case 4: Quantisation Parameter QP = 28

Table :Performance Analysis for Both encryption methods at QP= 28

S.no	Input Video	QP	MSE		PSNR		Correlation		Percentage Residual Difference		Structure Similarity Index	
			chaos	14 square	chaos	14 square	chaos	14 square	chaos	14 square	chaos	14 square
1	inp.avi	28	6.6535	6.6535	39.9003	39.9003	0.9976	0.9976	0.1672	0.1672	0.9644	0.9644
2	inp2.avi		3.9518	3.9518	42.1629	42.1629	0.9989	0.9989	0.1229	0.1229	0.9576	0.9576
3	inp3.avi		5.7393	5.7393	40.5422	40.5422	0.9985	0.9985	0.1485	0.1485	0.9628	0.9628
4	inp4.avi		4.7331	4.7331	41.3794	41.3794	0.9976	0.9976	0.1401	0.1401	0.9477	0.9477
5	inp5.avi		3.118	3.118	43.1921	43.1921	0.9984	0.9984	0.1117	0.1117	0.9577	0.9577
6	inp6.avi		4.9555	4.9555	41.1799	41.1799	0.998	0.998	0.14	0.14	0.9615	0.9615
7	inp7.avi		4.4696	4.4696	41.6281	41.6281	0.9966	0.9966	0.1334	0.1334	0.9388	0.9388

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

Case 5: Quantisation Parameter QP = 32

Table :Performance Analysis for Both encryption methods at QP= 32

S.no	Input Video	QP	MSE		PSNR		Correlation		Percentage Residual Difference		Structure Similarity Index	
			chaos	14 square	chaos	14 square	chaos	14 square	chaos	14 square	chaos	14 square
1	inp.avi	32	15.0211	15.0211	36.3638	36.3638	0.9943	0.9943	0.2537	0.2537	0.9288	0.9288
2	inp2.avi		7.457	7.457	39.4051	39.4051	0.9978	0.9978	0.1737	0.1737	0.9285	0.9285
3	inp3.avi		12.0111	12.0111	37.335	37.335	0.9968	0.9968	0.2144	0.2144	0.9336	0.9336
4	inp4.avi		9.2773	9.2773	38.4566	38.4566	0.9951	0.9951	0.2015	0.2015	0.9052	0.9052
5	inp5.avi		6.2587	6.2587	40.166	40.166	0.9968	0.9968	0.1573	0.1573	0.9264	0.9264
6	inp6.avi		10.3035	10.3035	38.001	38.001	0.9958	0.9958	0.2001	0.2001	0.9382	0.9382
7	inp7.avi		8.6505	8.6505	38.7604	38.7604	0.9936	0.9936	0.1818	0.1818	0.8912	0.8912

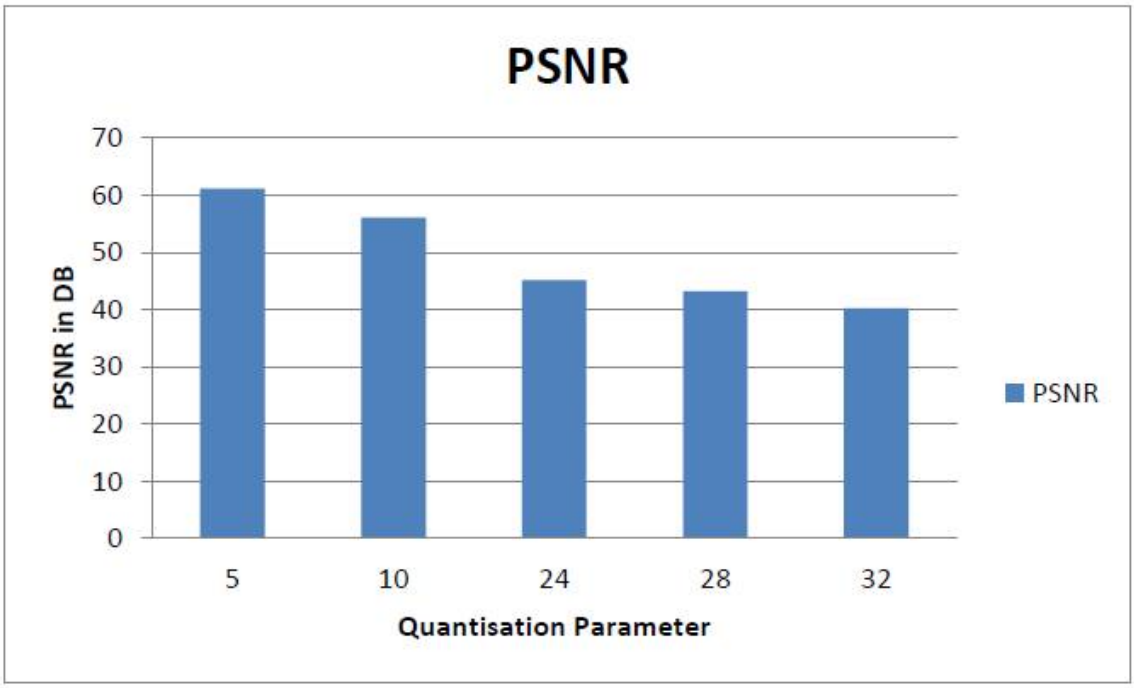


Fig: Average PSNR for various Quantisation Parameter

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

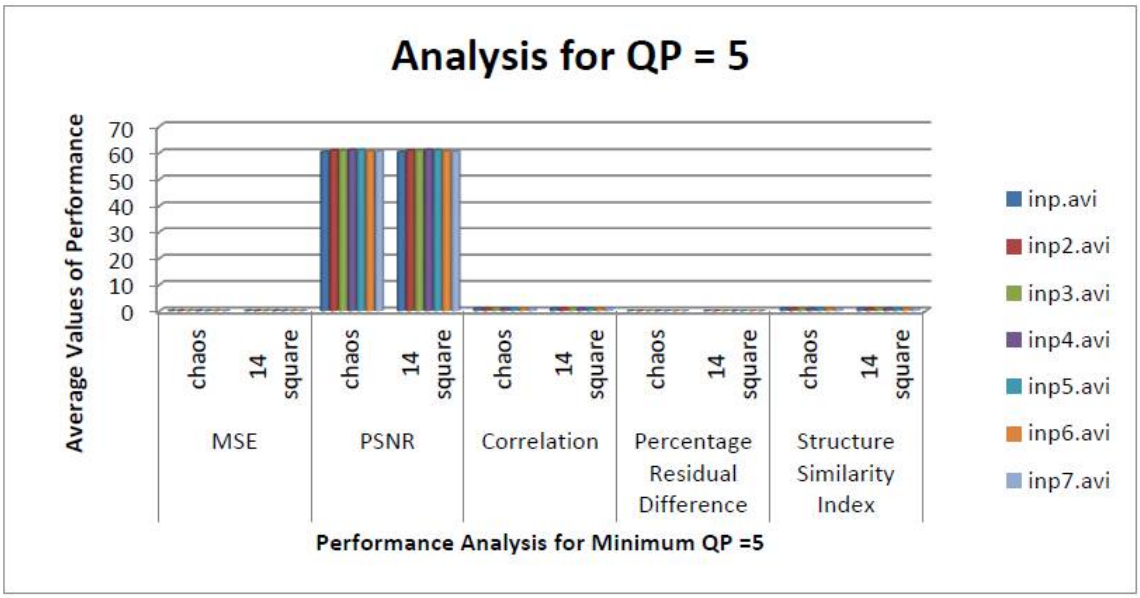


Fig:Analysis for Performance parameters with QP =5

With the variation in QP for the Video it is observed that The experimental results are shown in above tables and graph plots. As can be seen, a higher QP (quantization parameter) will result in lower video quality. The visual quality degradation of decrypted video containing hidden knowledge is incredibly low even for giant payloads, i.e., it's typically onerous to find the degradation in video quality caused by knowledge concealment.Payload of the proposed scheme depends on type of video content and the QP values. From the above experimental results it is clear that the increase quantisation parameter values decreases the PSNR and increases the MSE which adds uptothe visual degradation of the Image. To conclude over the results and analysis it is necessary aspect that quantisation parameter value to keep as minimum as possible to avoid possible visual quality degradation of decrypted video containing hidden data.

IV.CONCLUSION

The security and robustness of the data hiding scheme is achieved by using two well known and standardly accepted data encryption techniques which are selected on the basis of random key generated for the selection and the key is used in the packetisation for the receiver to decode and use the same algorithm to extract the data hidden and recover the private information. Bits replacement method was used to embed secret message bits with compressed bit streams to prevent the video from tampering. In order to adapt to different application scenarios, data extraction was done either in the encrypted domain or in the decrypted domain to recover original data without any loss. Finally the simulated results shown that utilized methodologies given high PSNR and high structure similarity index values and lower MSE (Mean square Error) and PRD (Percentage residual difference) with more compatibility where the observations says a higher QP (quantization parameter) will result in lower video quality. So in the future, more effective methods should be taken into account to further increase the embedding capacity and enhance the security of the algorithm as well as the data compression can also be taken care while embedding the data when the maximum payload size is selected and which goesbeyond the actual frames selected for the processing.

REFERENCES

[1] DawenXu, Rangding Wang, and Yun Q. Shi, *Fellow, IEEE"* Data Hiding in Encrypted H.264/AVC VideoStreams by Codeword Substitution‖, VOL. 9, NO. 4, APRIL 2014
[2] Spyridon K. Kapotas, Eleni E. Varsaki and Athanassios N. Skodras ―Data Hiding in H.264 Encoded Video Sequences‖ in IEEE trans, 2007

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

[3] Arup Kumar Bhaumik, Minkyu Choi, RosslinJ.Robles, and MaricelO.Balitanas Proposed Data hiding in video‖ International Journal of Database Theory and ApplicationVol. 2, No. 2, June 2009
[4] Xiaojing Ma, Zhitang Li, HaoTu, and Bochao Zhang, ―A Data Hiding Algorithm for H.264/AVC Video Streams without Intra-Frame Distortion Drift‖, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 20, NO. 10, OCTOBER 2010
[5] Z. Shahid, M. Chaumont and W. Puech ―FAST PROTECTION OF H.264/AVC BY SELECTIVE ENCRYPTION OF CABAC FOR I & P FRAMES‖, 17th European Signal Processing Conference (EUSIPCO 2009) Glasgow, Scotland, August 24-28, 2009
[6] DawenXuRangding Wang ―Watermarking in H.264/AVC compressed domain using Exp-Golomb code words mapping‖, Optical Engineering Volume 50, Issue 9, 1 September 2011
[7] *Advanced Video Coding for Generic Audiovisual Services*, ITU, Geneva,
Switzerland, ar. 2005.
[8] Gandharba Swain, Saroj Kumar Lenka, ‖Steganography using the Twelve Square Substitution Cipher and Index Variable‖,IEEE transactions on Image Processing, 2011.
[9] Saleh Saraireh. "A Secure Data Communication System Using Cryptography An Steganography", International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.3, May 2013.