MODIFIED FRAME SEPARATION METHOD WITH IDEA (MFSMI) FOR SECURE VIDEO ENCRYPTION

[1]Shubhi Nehra, [2]Prof. Zohaib Hasan

GGITS, Jabalpur

***Abstract*: Video streaming over a wireless network such as mobile ad hoc network (MANET), where wireless terminals (like Personal Device Assistance, mobile phones, palmtops) access in video conferencing system, new challenges will be brought about. First for all, a refactoring for original system with security design should be considered due to limited wireless bandwidth for wireless terminals. In addition, a lightweight encryption algorithm to protect media data should be given due to limited battery power & computational resource. Proposed work is a Design of Secure Video Encryption module with a new Key based Frame Isolation technique & International Data Encryption Algorithm (IDEA) Encryption may be named modified frame separation method with idea (MFSMI) for secure video encryption (MFSMI). MFSMI is also useful when we store our confidential video or image on cloud server it so it will be secure we just have to save an encrypted videos & images on cloud servers & it is a new key based algorithm to find out frame & specific pixel in video & use IDEA encryption instead for AES. Proposed methods causes significant speed enhancement for video encryption with similar security. MATLAB is generalized simulator & provides all necessary functions for image processing. Work is been implemented & simulated on MATLAB standard videos are been taken for simulation of MFSMI.**

***Keywords*: IDEA: International Data Encryption Algorithm., NIDS: Network Intrusion Detection System., MPEG: Moving Picture Action Group, PSNR: Peak Signal to Noise Ratio, MFSMI: Key based Frame Isolation & IDEA Encryption**

I-INTRODUCTION

Today, there are several to video encryption-based security solutions available in many companies or origination in market areas, it may be Financial Services & Broadcasting to Government. Encryption has proven its name as a secure & universally applicable block encryption algorithm, encryption permits effective protection to transmitted & stored data against unauthentic access by third parties (intruders). Basic criteria to development of encryption were very high security requirements along with less easy, hardware & software implementation with fast execution. Video encryption may be used to protect information transmission & storage.

This algorithm encrypts video data frame by frame because a video is sequence of images (frames)[7] which are presented in a sequence one after another in a constant time slice. That's why, main concept of this algorithm is to perform encryption or decryption on an individual frames. That's why this algorithm is called Frame based Encryption for streaming data. This algorithm is a symmetric key encryption algorithm in which two keys are used. One is a static Key & another is dynamic. Static key is transferred before any data transmission is carried out by using a secure communication link (on connection oriented environment) & dynamic key is send with encrypted video frame.

II-PROPOSED METHODOLOGY

Most for organization & personal data, images & videos are storing & accessing from cloud servers. Someone other users for same server may get access & may steal confidential video or images. Video broadcasting anyone may develop antennas & receivers & may easily access video & enjoy paid video in free hence encryption required so they cannot receive correct video. Another problem is security level if we try to enhance security means increasing total avalanche it may cost many of time & we try to speed up level of security (i.e. avalanche) decreases, so one should have to take a procedure which is good in speed as well as in security AES[3] & IDEA are two major techniques available to data encryption. Our aims is to use a technique as encryption for videos & out of this available two methods IDEA encryption is technique which has easy computation & does not necessary use S-box hence does not need slow Memory elements. Hence IDEA[6] encryption best suited as real time video encryption because it does not takes long time to develop cipher video. All existing designs & observe their performance & to compare them.

If we go for encryption on full video pixel security, major problem in video security is its size as any video may have many of frames & size of frames depends upon quality of video let say we have a video of 5 minutes & it is been recorder at 30 fps (frames per seconds) & its frame standard size of 640x480 then,

No of pixels in one frame is 640x480 = 307200

No of frame in one min. is 30 then in 5 min is 5x30 = 150 frames

No of pixels in 5 minutes video s 150*307200 = 46080000

Each pixel has 8 binary bit

Total binary bits = 46080000*8 = 368640000

Available work use AES which is capable of encrypting 128 bit at one time hence for 5 minutes video ASE has be run 368640000/128 = 2880000 times

AES necessary minimum 25 ms to encrypt 128 bit, Hence for five minute video 2880000*25 ms = 20 hours for five minute video only.

So it is absolutely not feasible to encrypt full video, hence most of video encryption use selective encryption & select appropriate area in video which may be encrypted not full video, however problem is to find that area in video which affect video most. Proposed work is a design which is developed as secure video communication & secure broadcasting for videos & also as security

for private videos in cloud servers & any private networks like MANET[12] or WLAN. As Encryption is all mean that to secure our video & to secure it like it cannot be interpreted by any intruder, easy security may be achieve by using XOR gate along with key however it will be soon recognizable with few easy transform techniques. It is highly required to develop technique that is hard to even recognize with transform or other recursive mathematical solutions. Proposed thesis work is to design an optimized solution to secure data communication as compare with video encryption. Proposed technique is optimized solution to same when data conversion time & encryption time considers as design parameters. Propose work is using IDEA encryption technique instead for AES[3] & using a new formula based Frame pixel finder which rely on KEY given not on type for video.

FRAME & PIXEL FINDER: Proposed work using a new approach to find specific pixels & specific frame from where data need to be fetched let as example 64 bit KEY is

KEY== 1010101110111110111010101100110010110111111000110011110010101111

Than develop a KEY matrix

$$X = \begin{matrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{matrix} \quad \text{.....(1)}$$

The C_k coefficient generation with formula developed given below

$C_k = x(p,1) + x(p+(-1)^k,2) + x(p,3) + x(p+(-1)^k,4) + x(p,5) + x(p+(-1)^k,6) + x(p,7) + x(p+(-1)^k,8)$ (2)

Where

p = 1 as k=0 & p=2 as k=1
p = 3 as k=2 & p=4 as k=3
p = 5 as k=4 & p=6 as k=5
p = 7 as k=6 & p=8 as k=7

When we put k 0,1,…..7 coefficients developed as given below

$C_0 = x(1,1) + x(2,2) + x(1,3) + x(2,4) + x(1,5) + x(2,6) + x(1,7) + x(2,8)$
$C_1 = x(2,1) + x(1,2) + x(2,3) + x(1,4) + x(2,5) + x(1,6) + x(2,7) + x(1,8)$
$C_2 = x(3,1) + x(4,2) + x(3,3) + x(4,4) + x(3,5) + x(4,6) + x(3,7) + x(4,8)$
$C_3 = x(4,1) + x(3,2) + x(4,3) + x(3,4) + x(4,5) + x(3,6) + x(4,7) + x(3,8)$
$C_4 = x(5,1) + x(6,2) + x(5,3) + x(6,4) + x(5,5) + x(6,6) + x(5,7) + x(6,8)$
$C_5 = x(6,1) + x(5,2) + x(6,3) + x(5,4) + x(6,5) + x(5,6) + x(6,7) + x(5,8)$
$C_6 = x(7,1) + x(8,2) + x(7,3) + x(8,4) + x(7,5) + x(8,6) + x(7,7) + x(8,8)$
$C_7 = x(8,1) + x(7,2) + x(8,3) + x(7,4) + x(8,5) + x(7,6) + x(8,7) + x(7,8)$

- C_0 is used as finding RED frame number after each C_0 interval RED frame will be taken.
- C_1 is used as specific pixel in RED frame after each C_1 interval next pixel selected.
- C_2 is used as finding GREEN frame number after each C_2 interval GREEN frames will be taken.
- C_3 is used as specific pixel in GREEN frame after each C_3 interval next pixel selected.
- C_4 is used as finding BLUE frame number after each C_4 interval BLUE frames will be taken.
- C_5 is used as specific pixel in RED frame after each C_5 interval next pixel selected.
- C_6 & C_7 may be used in near future as lot security.

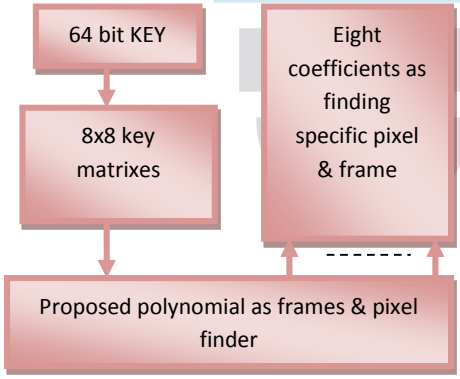

Figure 1 Propose Frame & Pixel finder

CIPHER VIDEO GENERATOR: Figure 2 shown below is overall explanation for proposed work flow of work may be explained as below:

Step 1: Browse any video from laptop or any other source to MATLAB[18] environment & develop it as a MATLAB[18] file & open that file in MATLAB[18] as further accessing.

Step 2: Isolate frames & also isolate Red green & blue form individual frames, every value in that pixel may be considered as a data as encryption.

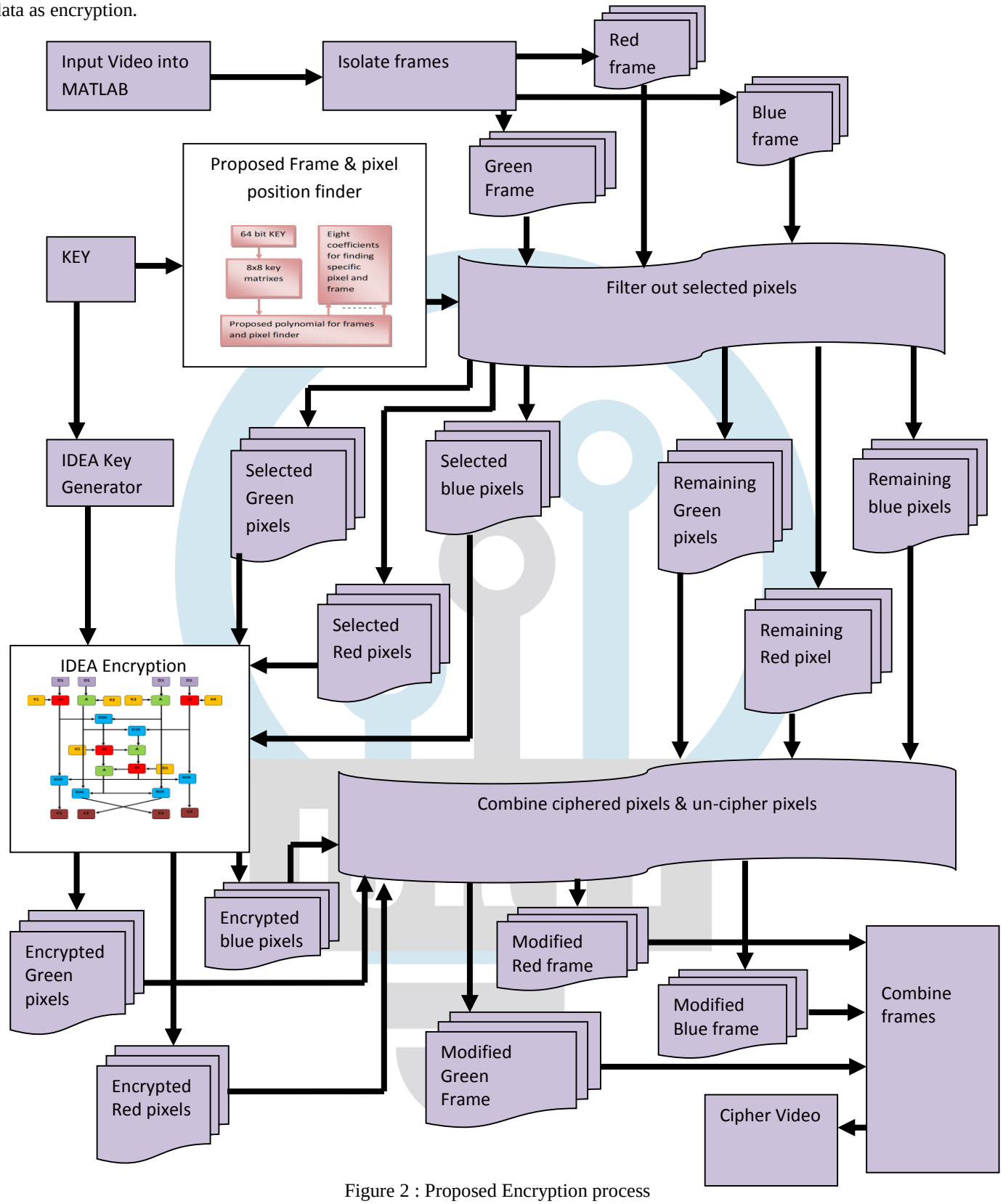

Figure 2 : Proposed Encryption process

Step 3: Select any random 64 bit key & pass it into proposed frame & pixel finder, there that key will further converted into eight various coefficients as red, green & blue frames & pixel.
Step 4: Filter out selected pixels from selected frames & isolate remaining unselected pixel for unselected frames.
Step 5: Develop 52 Sub-keys as IDEA encryption generation.
Step 6: Pass selected pixels for selected frames from IDEA cipher generator & develop cipher as all selected pixels.
Step 7: Combine cipher pixels of selected frames & unselected pixels for unselected frames again with help for those eight coefficients which is been discussed in step 3.
Step 8: Combine all red, green & blue modified frames & develop cipher video

Figure 4 below shows that after developing cipher video it is highly necessary matching original video & developed cipher video on basis for standard parameters, here SNR, MSE & BER are standard parameters taken.

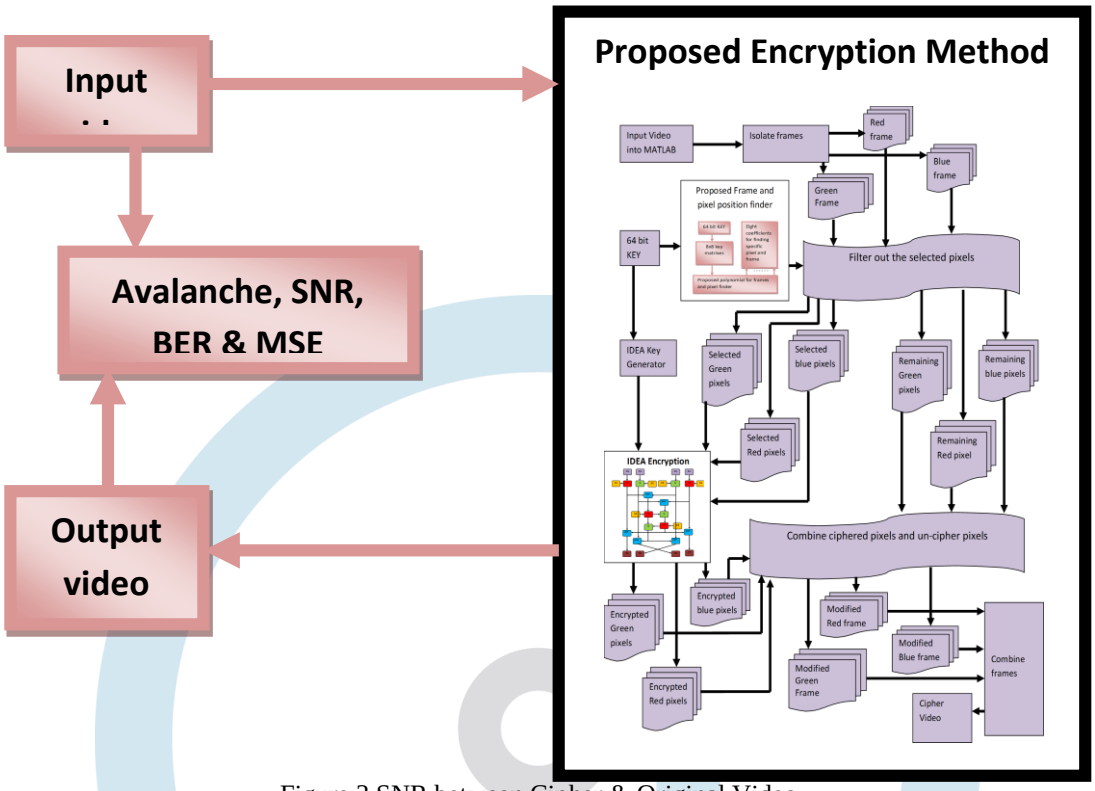

Figure 3 SNR between Cipher & Original Video

Proposed work is a Design of Secure Video Encryption module with a new Key based Frame Isolation technique & IDEA Encryption may be named MFSMI. figure above explains working flow of encryption & decryption. it may be observe that total computational requirement of MFSMI is very less due to IDEA Encryption & Key base frame finder, Haojie Shen et al [1] were using AES which has heavy computational requirement as compare to IDEA & for finding pixels in image Haojie Shen et al [1] ware using Discrete Cosine Transform (DCT) for identifying high & low frequencies & encrypt high frequencies again DCT require heavy computation & again IDCT also necessary heavy computation, however proposed work MFSMI is using a light key based computation to find frame & pixel in it. Hence it may be conclude that proposed work is much faster than Haojie Shen [1] work & lot suitable for Real time video encryption.

III-RESULTS

To implement proposed work software used is MATLAB[18] all program are written in MATLAB[18] & also tested on MATLAB. Hence to get understanding software it is a compulsory element for proposed work.

SIMULATION RESULTS: Proposed work simulation is done on various video file, MATLAB standard HEVC [5][1] file 'fil_cat.avi' & MATLAB standard MPEG[9][3] file 'atrium.mpg' simulated, shown & explained.

Results obtain as 'fil_cat.avi': figure 4 below show few frames for video

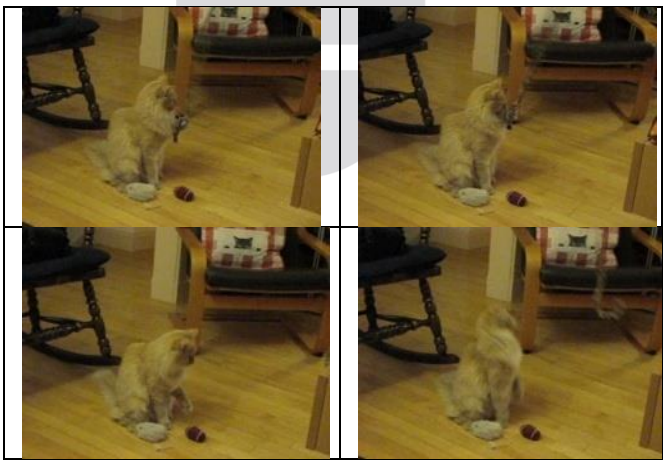

Figure 4 frame separation for HEVC video 'fil_cat.avi'

figure 5 shown below are frames for cipher video for 'fil_cat.avi' developed after execution for whole code.

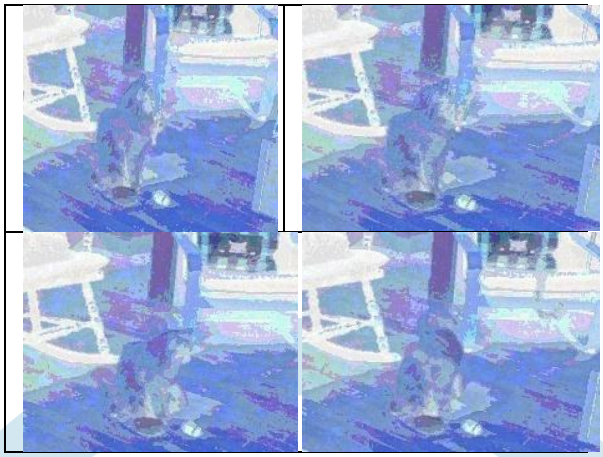

figure 5 Cipher video frame for 'fil_cat.avi'

MSE between Original frame for 'fil_cat.avi' & ciphered frame for 'fil_cat.avi' is 6683
SNR between Original frame for 'fil_cat.avi' & ciphered frame for 'fil_cat.avi' is 7.9321
BER between Original frame for 'fil_cat.avi' & ciphered frame for 'fil_cat.avi' is 0.6725
Time delay needed as developing cipher is 1.736 seconds

The work is been compare with similar work for secure video encryption, P. Deshmukh et al [3]reduce time with significant amount however could not maintain security level they were using easy XOR between selected frames to develop cipher frame. In work by M li et al [2] they were doing AES[3] all almost every 3rd frame which makes their procedure very strong against any attack by intruders however also reduces total time with a big amount & also necessary many for computations Haojie Shen et al [1] perform encryption on high frequencies only that make many for change in original videos if any video has many for high frequency component hence their procedure is huge dependent on type of video. Base works are also uses MATLAB standard HEVC & MPEG video so proposed work is also done simulation on MATLAB standard HEVC & MPEG video. Table 1 shown below shows comparative results obtain as proposed work & other work which used HEVC [5][1] standard Video as their simulation.

Results obtain as HEVC [5][1] video			
Parameter	**Proposed**	**Ahmed I. Sallam et al [1]**	**Ch. Naveen et al [2]**
MSE	0.6683	0.311	-
SNR	7.9321	8.77	10
BER	0.6725	0.54	-
Time	1.736	-	-

Table 5 Comparative results as HEVC Videos

Table 6 shown below shows comparative results obtain as proposed work & other work which used MPEG[9][3] standard Video as their simulation.

Results obtain as MPEG[9][3] video		
Parameter	**Proposed**	**Haojie Shen et al [3]**
MSE	0.5895	
SNR	8.36	45.63
BER	0.7219	
Time	2.552	1.124

Table 2: Comparative results as MPEG Videos

IV-CONCLUSION

Thesis is to propose a security scheme which reduces latency overhead by modifying existing approaches as encrypting video data using a probabilistic encryption for frames. Proposed work is also useful when we store our confidential video or image on cloud server it so it will be secure we just have to save an encrypted videos & images on cloud servers. Proposed work is a new key based algorithm to find out frame & specific pixel in video & use IDEA encryption instead for AES. Proposed methods causes significant

speed enhancement for video encryption with similar security. In addition, it is best suited as communication between hand-held devices such as mobile phones, palmtops etc. algorithm may be used between sites where processing capacity & battery power are limited & efficient encryption is main necessity. Proposed work has achieved lowest SNR among all available work & high MSE than all available work. The future aspect for proposed algorithm is designed as decryption process. This thesis work may be implemented design to military purpose as implemented design to high secure video communication. This thesis work has been done using MATLAB. Proposed work is simulated on MATLAB[18] in future work may be implemented on much advance software tool with high computational capable hardware & reduced memory to make working fast, in near future much stages to encryption may be add however it should be very careful because much stage will increase time delay & reduce throughput.

REFERENCES

[1] Ahmed I. Sallam, El-Sayed M. EL-Rabaie, Osama S. Faragallah, HEVC Selective Encryption Using RC6 Block Cipher Technique, 10.1109/TMM.2017.2777470, IEEE Transactions on Multimedia

[2] Ch. Naveen, Saiyma Fatima Raza, V. R. Satpute,Multi key Algorithm for Performance Enhancement of Video Encryption, 2016 11th international conference on industrial and information systems (ICIIS), India, pp 50-55

[3] Haojie Shen, Li Zhuo, Yingdi Zhao, An efficient motion reference structure based Selective Encryption algorithm as HEVC videos, Published in IET Information Security , IET Inf. Secur., 2014, Vol. 8, Iss. 3, pp. 199–206, Institution for Engineering & Technology 2014, doi: 10.1049/iet-ifs.2012.0349

[4] M. Li, C. Yang, J. Tian, Video Selective Encryption Based on Hadoop Platform, 978-1-4799-6022-4/15/ 2015 IEEE

[5] Modified AES based algorithm as MPEG video encryption, P. Deshmukh, V. Kolhe, 978-1-4799-3835-3/14/2014 IEEE

[6] kai huang, di ma, hi tong gi, ron ging yang, High throughput VLSI architecture as HEVC/AVC context based adaptive binary arithmetic coding (CABAC) decoding, Springer link, Journal for Zhejiang University SCIENCE, June 2013, Volume 14, problem 6, pp 449463

[7] W. Puech, A. Bors & J.M. Rodrigues, Protection for Color Images by Selective Encryption, IEEE Trans. on Circuits & Systems as Video Technology, 10(7):1116–1120, Oct. 2013

[8] Ajay Kulkarni, Saurabh Kulkarni, Ketki Haridas, Aniket More, Proposed Video Encryption Algorithm v/s Other Existing Algorithms: A Comparative Study, International Journal for Computer Applications (0975 – 8887) Volume 65– No.1, March 2013

[9] Li Weng, Karel Wouters & Bart Preneel, Extending Selective MPEG Encryption Algorithm PVEA, In Proc. IEEE Workshop on Multimedia Signal Processing, 2009.

[10] William Puech, José Rodrigues, Adrian Bors, Analysis & Cryptanalysis for a Selective Encryption procedure as JPEG Images, HAL Id: lirmm-00192604, http://hal-lirmm.ccsd.cnrs.fr/lirmm-00192604 Submitted on 28 Nov 2007

[11]Patil Ganesh G & Madhumita A Chatterjee, Selective Encryption Algorithm as Wireless Ad-hoc Networks, International Journal on Advanced Computer Theory & Engineering (IJACTE), ISSN (Print) : 2319 – 2526, Volume-1, Issue-1, 2012

[12] Ajay Kushwaha, Enhancing Selective Encryption Algorithm as Secured MANET, 2012 Fourth International Conference on Computational Intelligence, Modelling & Simulation, 2166-8531/2012 IEEE,DOI 10.1109/CIMSim.2012.16

[13] Pavithra. C Vinod. B. Durdi, Analization & Comparison for Selective Encryption Algorithms with Full Encryption as Wireless Networks, International Journal for Engineering Trends & Technology (IJETT) – Volume 4 problem 5- May 2013, ISSN: 2231-5381 Http://www.ijettjournal.org Page 2083

[14] Deepti Ranaut, Madal Lal, A Review on Security Issues & Encryption Algorithms in Mobile Ad-hoc Network, International Journal for Science & Research (IJSR) ISSN (Online): 2319-7064, Volume 3 problem 6, June 2014 www.ijsr.net, Paper ID: 0201442

[15] Roman Pfarrhofer, Andreas Uhl, Selective Image Encryption Using JBIG, CMS 2005, LNCS 3677, pp. 98–107, 2005, IFIP International Federation as Information Processing 2005

[16] Tom Lookabaugh, Douglas C. Sicker, Selective Encryption as Consumer Applications, SPIE Multimedia Systems & Applications VI, Orlando, FL, Sept 7-9, 2009.

[17] Saurabh Sharma Pushpendra Kumar Pateriya, A Study on various Approaches for Selective Encryption technique, International Journal for Computer Science & Communication Networks, Vol 2(6), 658-662

[18] MATLAB help browser, Math-works.

[19] Saranya. P, Varalakshmi. L.M, HEVC based Selective Video Encryption as Mobile Applications, International Journal for Computer Applications (0975 – 8887) Volume 17– No.4, March 2011

[20] A Massoudi, F Lefebvre, C De Vleeschouwer, B Macq & JJ Quisquater, Overview on Selective Encryption for Image & Video: Challenges & Perspectives, EURASIP Journal on Information Security, eurasipjournals.com/content/2008/1/179290

.