International Journal of Advanced Technology and Engineering Exploration, Vol 3(16)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2016.316007

Review Article

An efficient video data security mechanism based on RP-AES

Abhilasha Yadav[1*] , Manoj Verma[2] and Kailash Patidar[3]
M.Tech Student, Computer Science, SSSIST, Bhopal, India[1]
Assistant Professor, Computer Science, SSSIST, Bhopal, India[2]
HOD, Computer Science, SSSIST, Bhopal, India[3]

Abstract
Video security is an important aspect of communication now days. As the area is complex due to the nature of video and its file format. So there is a wide scope in this area. Cryptography can be applied for the data protection but in case of video all cryptography algorithms are not suitable as the video encoding scheme is different for different file formats. So in this paper an efficient Advanced Encryption Standard (AES) based algorithm has been proposed. This is hybridizing with random process. So this algorithm is random process- Advanced Encryption Standard (RP-AES). Our process improve the security mechanism due to this random process, the random process can efficient in generating runtime passwords every time. This algorithm has been checked by two parameters first by information loss and by checking the histogram comparison. In case of first parameter our results show less information entropy change so the data loss is minimum. In the second case the deviation in histogram shows that the RGB combinations have sufficient deviation for the encryption and decryption process.

Keywords
Video encryption, Information loss, RGB, AES.

1.Introduction
In old age a making conspicuous confirmation in information stowing without end for picture information has been found in the examination bundle. It is as major as an outcome of information security and transport of information with no copyright encroaches The Cryptography, Steganography and Watermarking structures can be utilized to get security and certification of information [1]. The information concealing framework can be utilized for duplicate right security, scene change revelation [2] other than for message passing. Information concealing methodology can in like way be utilized to consider the method for compacted video without the first reference. This quality is discovered by figuring the contaminations of the disengaged secured message [3]. Steganography is the one of the real methods in the extent of data disguising [4]. Security is a principal point which must be taken into record from the introductory strides of the arrangement method of appropriated databases, especially in security fundamental circumstances [5]. Security and assault recognition instrument are additionally talked about in [6-9].

*Author for correspondence

Encryption and deciphering of the data in the correspondence channel are also valuable for guaranteeing the data. For encryption and unscrambling and can use DES, RSA, RC4 and RC5 counts [10]. Square based division can be possible with subset superset mining or allotting systems [11][12]. It is moreover significant in the scene where the sending data and the wrapper will be different so confuse will be augmentations and the security in the getting side will be more constrained. In cryptography we perform encryption on the first substance to make the figure substance and unscrambling is just a backwards instrument to outline the plaintext. In steganography we cover the first plaintext within whatever other, content, PDF, pictures et cetera. The part of examining the first substance will be freely sent to the recipient for data scrutinizing. Cryptography is used to change the first plain substance to encode or make vague sort of substance [13]. The unendurable materials are surreptitious on the sender companion with a particular deciding objective to have them separated and charmed from unlawful access and after that sent by method for the framework. Right when the data are gotten then the reverse method will be used for interpreting depending upon a count. Interpreting is the method of changing over data from encoded

association back to their special arrangement [14][15][16].

2.Related work

In [17] authors recommend a proficient video encryption plan is built by picture key and depends on hyper chaos framework. The tumultuous cross sections are utilized to create pseudorandom groupings and after that chose pixel and bit pixel of picture key scramble edge squares one by one. By repeating riotous maps for specific times, the created pseudorandom groupings acquire high starting quality affectability and great irregularity. The pseudorandom-bits in every cross section are utilized to choose pixel and bitpixel of picture key and afterward encode the Direct Current coefficient (DC) and the indications of the Alternating Current coefficients (ACs). Hypothetical examination and exploratory results demonstrate that the plan has great cryptographic security and perceptual security, and it doesn't influence the pressure productivity obviously. In [18] authors proposed a more productive specific encryption approach which misuses the mistake spread property in MPEG2 standard. Their test results demonstrate that the proposed methodology can decrease the execution time of SECMPEG by a component of 32 without corruption of the security. In [19] authors proposed that the optical crypto system depends on twofold arbitrary stage encoding calculation to scramble and decode the expected sound/video groupings. The fundamental motivation behind steganography calculations is to stow away however much data inside of the spread media as could be expected. In this way, for steganography calculations, the trade-off is between the measure of secretive data being implanted, called steno-information, and that the insurance for its vicinity to stay undetected. While their reasons may appear to be changed, late advances permit more the utilization of cutting edge watermarking procedures to implant a lot of secret data that is like powerful against evacuation and location. In [20] authors proposed a DCT based steganography plan which gives higher imperviousness to picture handling assaults, for example, JPEG pressure, clamor, revolution, interpretation and so on. For securing the information, this will be secret key ensured. For configuration this test system we have encoded our information and after that without watchword we won't unscramble the information. The contrast between the two is in the appearance in the prepared yield; the yield of Steganography operation is not clearly noticeable but rather in cryptography the yield is mixed with the goal that it can draw consideration. They have attempted to clarify the distinctive methodologies towards usage of Steganography utilizing "sight and sound" document (content, static picture, sound and video) and Network IP datagram as spread. In [21] authors recommend an expanding number of picture and video preparing issues, cryptographic strategies are utilized to authorize substance access control, character check and verification, and security assurance. The blend of cryptography and sign preparing is an energizing developing field. This early on paper gives a review of methodologies and difficulties that exist in applying cryptographic primitives to critical picture and video handling issues, including (halfway) content encryption, secure face acknowledgment, and secure biometrics. They expect to help the group in valuing the utility and difficulties of cryptographic strategies in picture and video preparing. In [22] proposed that the Video is basically a grouping of pictures; thus much space is accessible in the middle of for concealing data. In proposed plan video steganography is utilized to shroud a mystery video stream in spread video stream. Every edge of mystery video will be broken into individual segments then changed over into 8-bit double values, and encoded utilizing XOR with mystery key and scrambled edges will be covered up at all huge piece of every casings utilizing consecutive encoding of Cover video. In [23] authors have proposed another strategy for information implanting and extraction for high determination AVI recordings. In this system as opposed to changing the LSB of the spread document, the LSB and LSB+3 bits are changed in interchange bytes of the spread record. The mystery message is scrambled by utilizing a straightforward piece trade strategy before the real implanting procedure begins. A list can likewise be made for the mystery data and the list is put in a casing of the video itself. With the assistance of this list, they can without much of a stretch concentrate the mystery message, which can diminish the extraction time. In [24] authors have proposed another system of picture steganography i.e. Hash-LSB with RSA calculation for giving more security to information and our information concealing technique. The proposed strategy utilizes a hash capacity to create an example for concealing information bits into LSB of RGB pixel estimations of the spread picture. This method verifies that the message has been scrambled before concealing it into a spread picture. On the off chance that regardless the figure content got uncovered from the spread picture, the middle of the road individual other than beneficiary can't get to the message as it is

in scrambled structure. In [25] authors have tried to modify the innovation of the information documents into scrambled structure utilizing Tiny Encryption Algorithm .This Algorithm is to be intended for effortlessness and better execution. In an encryption plan, data is scrambled utilizing little encryption calculation that progressions it into a garbled *figure* content. After encryption, the scrambled information is inserting in a video by utilizing the idea of steganography and after that this video document sent through email. The application ought to have an inversion process as of which ought to be in a position to unscramble the information to its unique organization upon the correct solicitation by the client. In [26] authors proposed a computationally proficient and secure video encryption calculation. This makes secure video encryption doable for continuous applications with no additional devoted equipment. What's more, unique and solid security away and transmission of computerized pictures and recordings is required in numerous advanced applications, for example, private video conferencing and medicinal imaging frameworks, and so on. Tragically, the established methods for information security are not proper for the present interactive media utilization [27]. Accordingly, they have to grow new security conventions or adjust the accessible security conventions to be material for securing the interactive media applications. They have actualized elliptic bend cryptography (ECC) and RC5 calculations are said. RSA based encryption has critical issues as far as key size. At present, the RSA calculation requires the key length of no less than 1024 bits for long haul security, while it appears that 160 bits are adequate for elliptic bend cryptographic working.

3.Proposed work

In this paper an efficient Advanced Encryption Standard (AES) based algorithm has been proposed. This is hybridizing with random process. So this algorithm is random process- Advanced Encryption Standard (RP-AES). It can be understood with the help of *Figure 1*.

The whole process can be categorized in five different parts:

Data Preprocessing: In this process the video data is selected first and then it is converted in the encrypted supported file that is a binary file. This data is the plaintext for the next processing.

Data Encryption: Then AES algorithm is applied for data encryption process. This process is applied according to the algorithm 1. In this process the plain text is applied to AES algorithm. The key that is given as data is ventured into a cluster of 44 words (32-bits each), w[i]. 4 distinct words (256 bits) serve as a round key for each round. Then data substitution is applied. Then value is calculated according to the finite field that is Galois field. Then XOR is applied to the added round key. Then key randomization is applied with the help of random algorithm.

Algorithm 1: AES Algorithm
In this algorithm we have used 256-bit key. It is ordered in the similar matrix by column.

Step 1:Plain text as an input.
Step 2:The key that is given as data is ventured into a cluster of 44 words (32-bits each), w[i]. 4 distinct words (256 bits) serve as a round key for each round.
Step 3: 4 distinct stages are utilized, 1 change and 3 of substitution:

-Substitute bytes–Uses a S-box to perform a byte-to-byte substitution of the piece
-Shift lines–A basic change
-Mix sections–A substitution that makes utilization of number juggling.
-Add round key–A straightforward bitwise XOR of the present square with the bit of the extent.

Step 4: It shows the encryption round uses arithmetic in the finite field that is Galois field GF (2^8), with the irreducible polynomial.
Step 5: Just the Add Round Key stage utilizes the key. Whatever other stage is reversible without learning of the key.
Step 6: The Add Round Key is a type of Vernam cipher and independent from anyone else would not be imposing. The other 3 organizes together give disarray, dispersion, and nonlinearity, however without anyone else would give no security in light of the fact that they don't utilize the key. Then the data is adjusting according to the XOR encryption with the added round key. The stage is also completely reversible
Step 7: Then encryption process is applied with the same keys.

Algorithm 2: Random algorithm
INPUT: (Text, character, Random-Seed)
OUTPUT: random_data, (Final-Seed)
random_data = F(Text, character, Random-Seed)
Key' = Math.random(Text, character, Random-Seed)

Final-Seed' = F(Key', Random-Seed)
Return random_data

Histogram Generation: After encryption we figure the information canisters of RGB that is ascertained for checking the information receptacles for the first information and scrambled information. For this we have ascertained the data Histograms. Histogram is utilized when the information or the set is substantial and it is ascertained in view of the qualities on the off chance that we consider RGB qualities and the qualities are reproduced as far as bar.

Algorithm 3: Histogram Generation
Step 1: Bin wise arrangement makes a matrix mapping.
Step 2: It is divided in 16-16 pair bins.
Step 3: Then RGB information is extracted
Red[x1, y1], Green[x1,y1], Blue[x1,y1]
Step 4: For mapping Euclidean distance is calculated based on the coordinates (x, y) and (a, b) is given by:
dist((x, y), (a, b)) = $\sqrt{(x - a)^2 + (y - b)^2}$
Step 5: It is allocated to the histogram shading mark of a casing based upon its shading histogram. The clarification is that progressive comparative edges will contain around the same shading data and comparable edges will have a comparative histogram.

In this case we can assume c for image characteristics and h (a) for its histogram for image a with n number of bars.

$$hd1(a,b) = \sum_{i=1}^{k} | h_i(a) - h_i(b) |$$

$$hd2(a,b) = \sum_{i=1}^{k} (h_i(a) - h_i(b))^2$$

$$hds(a,b) = \sum_{i=1}^{k} \frac{(h_i(a) - h_i(b))^2}{\max(h_i(a), h_i(b))}$$

Data Decryption: The reversible process is applied for retrieving the data after encryption for decoding component with the same key. It is secured by the encryption secret key. In the wake of applying the right secret word we will accomplish the last information. At that point the histogram is addition figured and appeared as information contained in form of different RGB bars and produced in terms of the outcome.

Information loss
The information loss is checked for the purpose of checking the information in terms of entropy to calculate the distraction in the information which is prior to encryption.

$$\sum_{i=1}^{n} - p(s_i) \log_2 p(s_i)$$

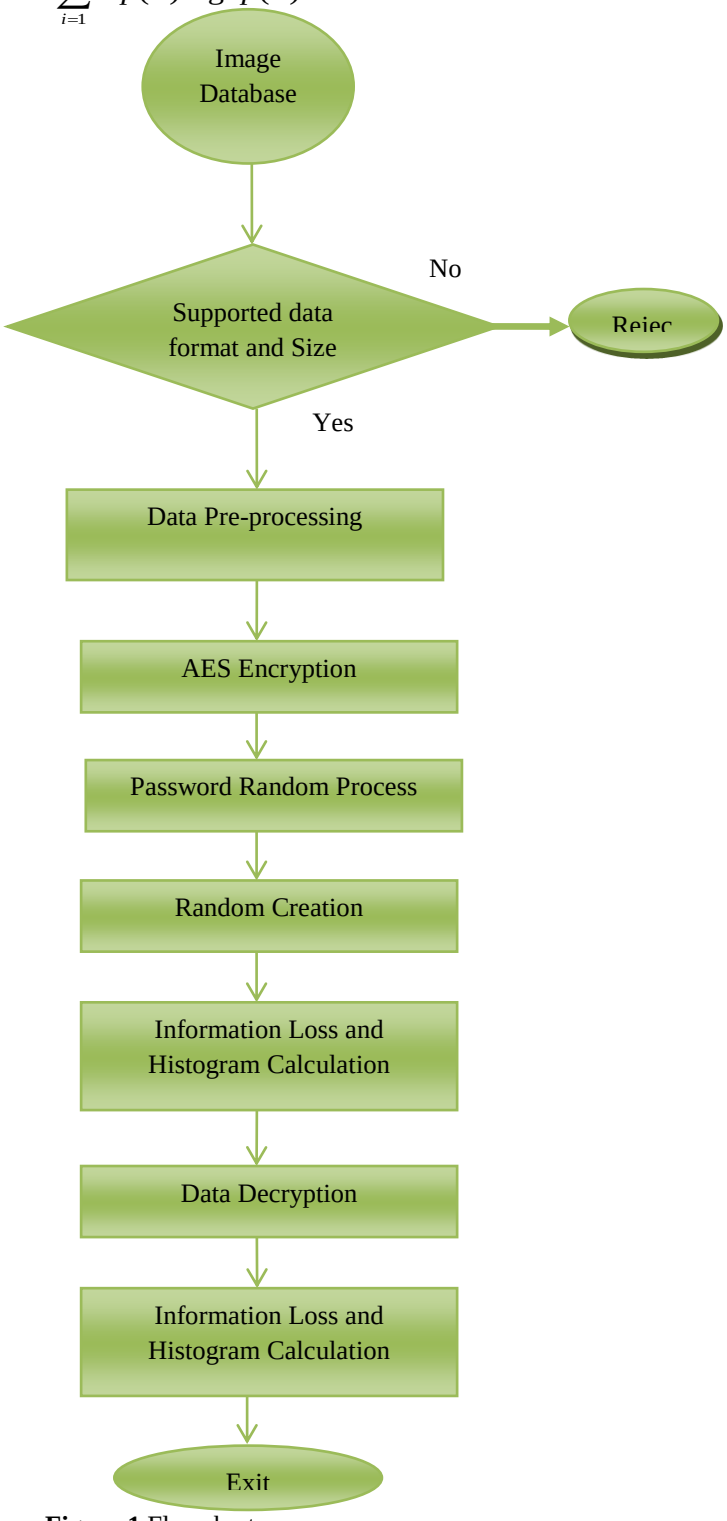

Figure 1 Flowchart

4.Result analysis

The outcomes appeared underneath demonstrate the viability of our efficient RP-AES method. This method demonstrates the results in two forms first by the histogram comparison and deviation. Second by the calculation of information loss. We first consider the example video picture and make the container Histogram in the wake of performing AES encryption. The Histogram of the first video after decoding is distinctive which is appeared in *Figure 2*. The same is shown for the original image as shown in *Figure 3*. The derogation plainly demonstrates the container contrasts are high with the goal that it will be more secure in correlation to the past method. It is proved by the RGB variation obtained. At that point we have considered seven diverse examples for the information loss which is additionally distinctive in all cases. The outcomes demonstrate the information loss is minimum as shown in *Table 1*and the security is improved in our strategy. Due to java virtualization and key generation separation the encryption time is also reduced. It is shown in *Table 2*.

Table 1 Information loss comparison

S. no	Name	Main image	Encrypted image
1	Video1	7.78	7.99
2	Video2	7.80	7.99
3	Video3	7.74	7.99
4	Video4	7.70	7.99
5	Video5	7.91	7.99
6	Video6	7.84	7.99
7	Video7	7.96	7.99

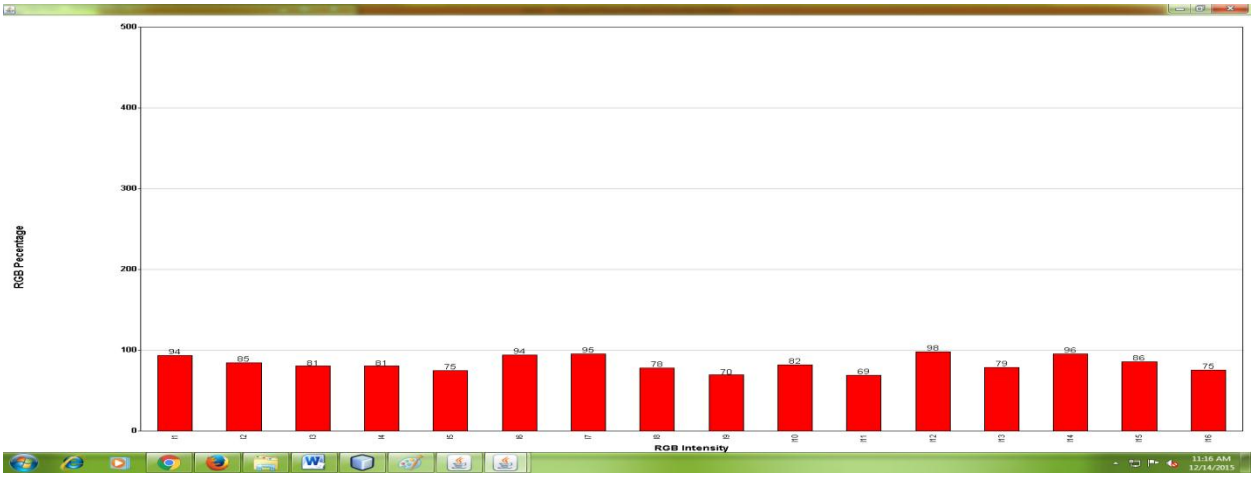

Figure 2 RGB video encryption histogram

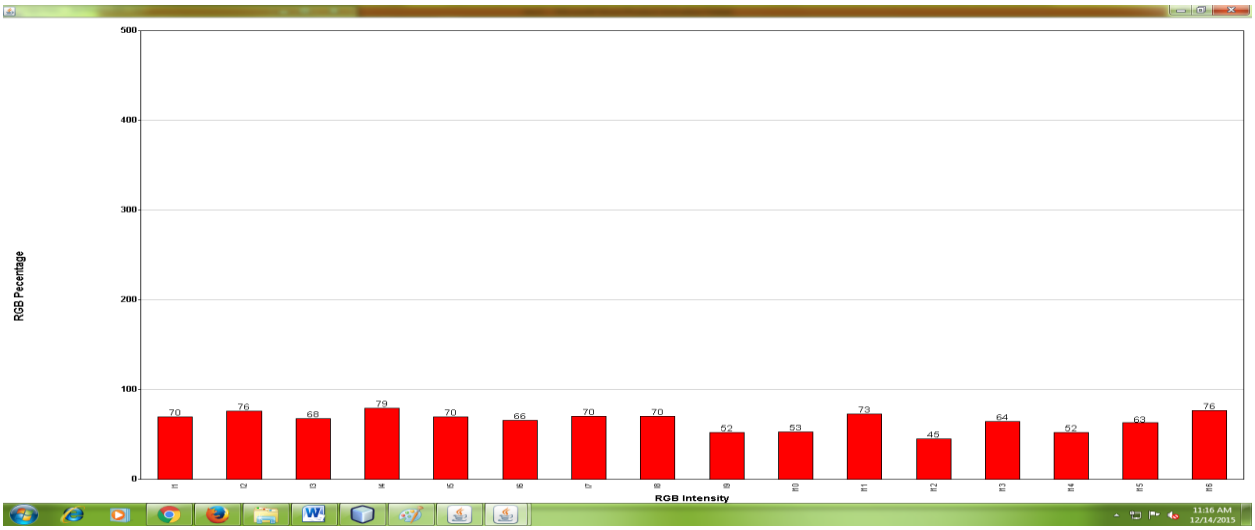

Figure 3 RGB video decryption histogram

Table 2 Time comparison

S. No	Video length (second) [28]	Encryption time (second) [28]	Video length (second)	Encryption time (second)
1	32	270	311	8.68
2	52	318	310	8.88
3	33	270	246	6.48
4	23	215	247	7.19
5	20	201	255	7.21
6	18	190	30	6.04

5.Conclusion

Based on the analysis and discussion in this paper it can be concluded that the video security is an important and challenging research era. In this paper we have proposed an efficient RP-AES method which is based on advanced encryption standard. It is capable of providing 256 bit key encoding and decoding. The randomization process can be helpful as it provide different keys for the same file if it is selected again in this framework. It is compared based on two parameters; the first parameter is the RGB histogram which shows the variations in the RGB it leads to the improved security. Second is the information los comparison which allows checking the loss in information in the cryptography process. Based on these parameters our approach has been outperformed.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Wajgade VM, Kumar DS. Enhancing data security using video steganography. International Journal of Emerging Technology and Advanced Engineering. 2013; 3(4):549-52.

[2] Kapotas SK, Skodras AN. A new data hiding scheme for scene change detection in H. 264 encoded video sequences. In IEEE international conference on multimedia and expo 2008(pp. 227-280). IEEE.

[3] Lathikanandini M, Suresh J. Steganography in MPEG video files using MACROBLOCKS. International Journal of Advanced Computer Research. 2013; 3(1):18-21.

[4] Bhalshankar S, Gulve AK. Audio steganography: LSB technique using a pyramid structure and range of bytes. International Journal of Advanced Computer Research. 2015; 5(20):233-48.

[5] Sengupta A. Dynamic fragmentation and query translation based security framework for distributed databases. International Journal of Advanced Computer Research. 2015; 5 (20):249-63.

[6] Kaushik M, Ojha G. Attack penetration system for SQL injection. International Journal of Advanced Computer Research. 2014; 4(2):724-32.

[7] Dubey A, Gupta R, Chandel GS. An efficient partition technique to reduce the attack detection time with web based text and PDF files. International Journal of Advanced Computer Research (IJACR). 2013; 3(9):80-6.

[8] Chhajed U, Kumar A. Detecting cross-site scripting vulnerability and performance comparison using C-time and E-time. International Journal of Advanced Computer Research. 2014; 4(2):733-40.

[9] Dubey AK, Dubey AK, Namdev M, Shrivastava SS. Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment. In CSI sixth international conference on software engineering (CONSEG) 2012 (pp. 1-8). IEEE.

[10] Dubey AK, Dubey AK, Agarwal V, Khandagre Y. Knowledge discovery with a subset-superset approach for mining heterogeneous data with dynamic support. In In CSI sixth international conference on software engineering (CONSEG) 2012 (pp. 1-6). IEEE.

[11] Khare P, Gupta H. Finding frequent pattern with transaction and occurrences based on density minimum support distribution. International Journal of Advanced Computer Research (IJACR). 2012; 2(3):165-9.

[12] Lakhtaria KI. Protecting computer network with encryption technique: a study. International Journal of u- and e- Service, Science and Technology. 2011; 4(2): 43-52.

[13] Chan AC, Castelluccia C. A security framework for privacy-preserving data aggregation in wireless sensor networks. ACM Transactions on Sensor Networks. 2011; 7(4):29-45.

[14] Stallling W. Crypthography and Network Security Priciples and Practices. Prentice Hall; 2005.

[15] Shannon CE. Communication theory of secrecy systems*. Bell system technical journal. 1949; 28(4):656-715.

[16] Yadav A, Patidar K. A meta-analysis of video data security. International Journal of Advanced Technology and Engineering Exploration. 2015; 2(12):152-6.

[17] Alirezaei V, Yaghbi M. Efficient video encryption by image key based on hyper-chaos system. In 2010 international conference on multimedia communications (Mediacom) 2010(pp. 141-4). IEEE.

[18] Jeong S, Lee E, Lee S, Chung Y, Min B. Slice-Level selective encryption for protecting video data. In international conference on information networking (ICOIN), 2011(pp. 54-7). IEEE.

[19] Guizani S, Nasser N. An audio/video crypto-adaptive optical steganography technique. In wireless 8th international on communications and mobile computing conference (IWCMC) 2012(pp. 1057-62). IEEE.

[20] Nagaria B, Parikh A, Eep M, Shrivastav N. Steganographic approach for data hiding using LSB

techniques. International Journal of Advanced Computer Research.4(6);441-5.

[21] Puech W, Erkin Z, Barni M, Rane S, Lagendijk RL. Emerging cryptographic challenges in image and video processing. In 19th IEEE international conference on image processing (ICIP) 2012(pp. 2629-32). IEEE.

[22] Yadav P, Mishra N, Sharma S. A secure video steganography with encryption based on LSB technique. In IEEE international conference on computational intelligence and computing research (ICCIC) 2013 (pp. 1-5). IEEE.

[23] Bhautmage P, Jeyakumar A, Dahatonde A. Advanced video steganography algorithm. International Journal of Engineering Research and Applications (IJERA). 2013; 3(1):1641-4.

[24] Kumar A, Sharma R. A secure image steganography based on RSA algorithm and hash-LSB Technique. International Journal of Advanced Research in Computer Science and Software Engineering. 2013; 3(7):363-72.

[25] Yadav M, Joshi M. Akshita," Improved secure data transfer using tiny encryption algorithm and video steganography". International Journal of Advanced Research in Computer Science and Software Engineering. 2013; 3(12):547-50.

[26] Bhandari L, Wadhe A. Speeding up video encryption using elliptic curve cryptography (ECC). International Journal of Emerging Research in Management &Technology. 2013; 2(3):24-9.

[27] Raju CN, Umadevi G, Srinathan K, Jawahar CV. Fast and secure real-time video encryption. In sixth Indian conference on computer vision, graphics & image processing 2008 (pp. 257-64). IEEE.

[28] Dumbere DM, Janwe NJ. Video encryption using AES algorithm. In 2nd international conference on current trends in engineering and technology (ICCTET) 2014 (pp. 332-7). IEEE.