International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-4 Number-3 Issue-16 September-2014

An efficient mechanism for Securing Video Data

Akansha Agrawal[1], Virendra Singh[2]

Abstract

Data security is an important concern today. In today's world data has been exchanged in several means like mail, data uploading, video exchange, image exchange etc. In this digital world data exchange and uploading is much more easy and convenient. So there is a chance of data alteration or unauthorized access may possible. There are several security mechanisms for textual data and images but video encryption is different. In this paper we have proposed an efficient video encryption technique. Our encryption technique improves the security with data bins which is validated by the (Red, Green, Blue) RGB comparison.

Keywords

Video Security, encryption and decryption techniques, Video Encryption, RGB Comparison.

1. Introduction

Data Security has been observed as the greater concern today. Data can be send and receive without any data protocol or copyright rules. For security and privacy Cryptography, Steganography and Watermarking techniques can be used [1]. Data hiding techniques are also suggested [2]. It can be used to calculate the quality also. This quality is calculated by the extracted hidden message achived from the next source [3]. In this direction of security mechanism Encryption and decryption of the data is most popular. For encryption and decryption Data Encryption Standard (DES), Rivest, Shamir, and Adleman(RSA), Rivest Cipher4(RC4), Rivest Cipher5 (RC5) and Rivest Cipher6 (RC6) algorithms [4]. Possibility of partition with subset and superset formation is also possible [5][6].

In general cryptography is the mechanism of converting plaintext into cipher text, this mechanism is called encryption and for retrieval of the original text decryption mechanism is performed. By which we can decrypt the cipher text to the plain text [8][9][10]. Means to make text unreadable form to text is the purpose of cryptography [7].

The mechanisms discussed above are well suited for textual data and good in the case of images. But in case of video encryption it becomes tough. As to apply encryption mechanism, all the encryption techniques are not applied on the video data. So first proper encryption techniques with bin calculation is needed. This paper is motivated in this direction to achieve proper security in case video data.

2. Related Work

In 2008, Ganesan, K. et al. [11] suggested the demand of cryptographic techniques. They suggest simple hashing algorithm for making the algorithm more secure, and which can be used for digital signature. Their algorithm is an extension of this algorithm for videos and used multilevel scrambling and hash. In 2009, Zhang Qian et al. [12] suggested three schemes to encrypt parts of video data using permutation code and DES encryption algorithm based on the newest coding standard H.264. In 2010, Vahid alirezaei et al. [13] suggests an efficient video encryption scheme based on hyper chaos system. Pseudorandom sequences are generated by chaotic lattices and then the blocks are encrypted one by one. Analysis and results shows good cryptographic security. In 2011, Seohyun Jeong et al. [14] proposed an error propagation scheme with MPEG2 standard. Their results show that the approach can reduce the execution time without degradation of the security.

In 2012, Guizani, S. et al. [15] suggest the differences of watermarking and steganography. The purpose of steganography algorithms is to hide as much information within the cover object. But in watermarking large amounts of covert information that is also robust against removal and detection is hide in the carrier signal. Security hybridization is also important [16][17][18]. In 2012, W. Puech et al. [19] suggest combination of cryptography and signal processing. Their aim is to solve challenges of

Manuscript received August 04, 2014.

Akansha Agrawal, M. Tech Research Scholar, Department of Computer Science, Indore Institute of Science and Technology-II, Indore.

Virendra Singh, Assistant Professor, Department of Computer Science, Indore Institute of Science and Technology-II, Indore.

cryptographic techniques especially in the case of image and video processing. In 2013, Pooja Yadav et al. [20] suggest that the video is sequential collection of images. So there is a wide space available for hiding information. So the proposed scheme is used to hide a secret video stream in cover video stream. It is encrypted using XOR with secret key and encrypted frames will be hidden in the least significant bit for each frames using encoding of Cover video that is sequential. In 2013, Pritish Bhautmage et al. [21] proposed a new technique for AVI videos data by embedding and extraction. In this method LSB and LSB+3 bits are changed for the cover file. The secret message is encrypted by bit exchange method and then the embedding process starts and an index is generated for the video in the frame. This index save the time of extracting the secret message. In 2013, Anil Kumar et al. [22] proposed image steganography by using Hash-LSB with the combination of RSA algorithm. Hash function is used to generate a pattern for hiding data bits into LSB of RGB pixel values of the cover image. It provides surety of message encryption before hiding it into a cover image. In 2013, Manisha Yadav et al. [23] try to modify the originality of the data files by using Tiny Encryption Algorithm. After encryption, the encrypted data is embedding in a video by using the concept of steganography and then this video file sent via email. In 2013, Lekha Bhandari et al. [24] propose an efficient and secure video encryption algorithm by elliptic curve cryptography (ECC) and RC5 algorithms.

3. Proposed Work

In this paper an efficient symmetric key encryption is presented for video data. The approach is better understood by the flowchart shown in figure 1. First the video data is selected and convert the video data in the binary file. Then we achieve the binary data which is used as the plaintext. The plaintext is then forwarded to symmetric key encryption block. The same key is used for encryption and decryption. After encryption we calculate the data bins of RGB that is calculated for checking the data bins for the original data and encrypted data. This is shown in figure 2. For this we have calculated Video Histograms. Histogram is used when the data or the set is very large and it is calculated based on the values in case we consider RGB values and the values are replicated in terms of bar.

A histogram is a plot deviate consists of a surrounded by of "bins", or organize bars, into which the imitate self-possession are sorted. The high point of unendingly histogram prohibition indicates but odd of your observations episode jump into divagate Canada luggage compartment, associate to the perfect expanse of matter values, so this kind of chart is also called the relative frequency histogram.

The roguish stance is to fake the expanse of bins, or classes, into which your data will be sorted. Encircling are a handful of influence to execute this, and match up of the outdo time again hand-me-down methods is to delimit the number of bins based on the total number of observations: k = 1 log2N, where N is the total number of data values, and k is the resulting number of bins. If you bring off non-integer k usefulness this formula, you should round it to the nearest integer. Without delay using EasyFit, you fundamentally either have the number of bins calculated automatically, or manually specify it through the Options|Map. The devote oneself to stand is to apportion the manifest courtyard of your text from xmin to xmax into k intervals of equal width, and calculate how many values fall into in perpetuity interval. And definitely, the crest of each embargo is planned as the in the midst of text points falling into rove interval, divided by the total number of observations. Value that directly displaying the attendant bars, they must be adjacent - there mustn't be any space between the neighboring bars. Histograms are many times imperfectly surrounding "bar charts" second-hand to ventilate veritable data, meaning that you can have non-numerical values on the x-axis, so the distance between the bars, as well as their particular order, is not really important, which is not the case for histograms.

After encryption we then apply decryption mechanism with the same key. It is protected by the encryption password. After applying the correct password we will achieve the final data. Then the histogram is gain calculated and shown in the form of data bin and represented in terms of graph and compares the result.

Then finally information entropy is calculated to check the distraction in the information before and after encryption.

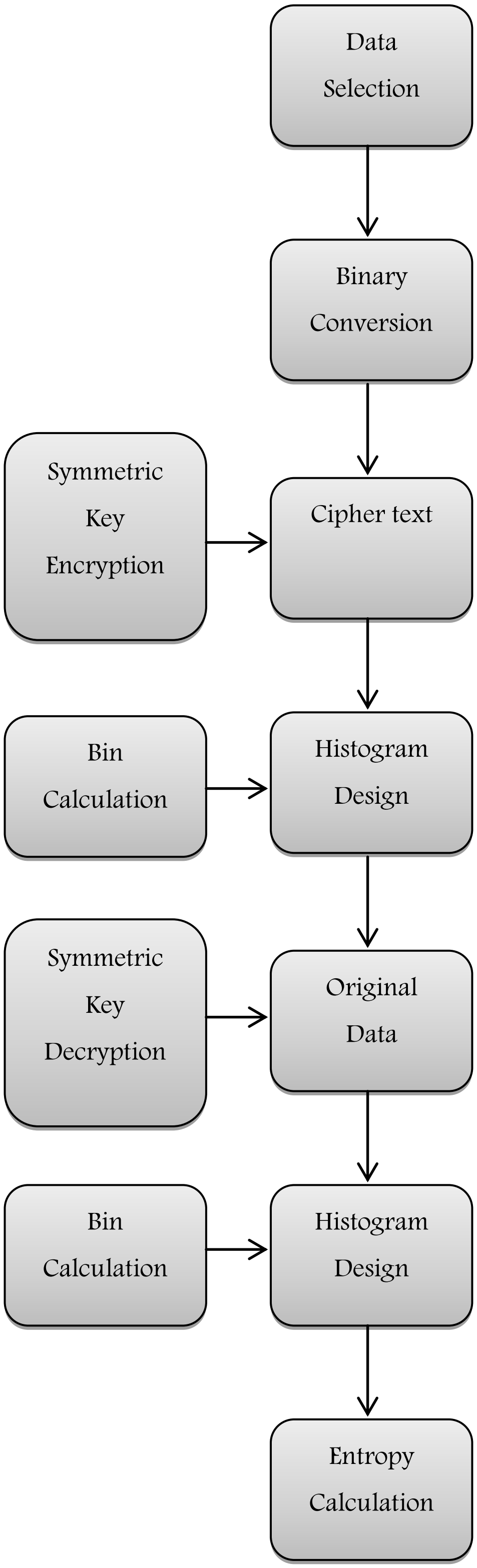

Figure 1: Flowchart

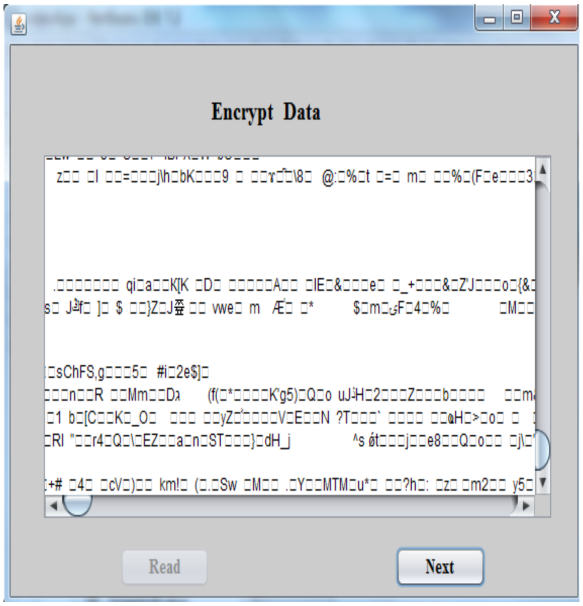

Figure 2: Data Encryption

Algorithm:
Assumptions:
VF→ Video File
PT→ Plain Text
K→Key
CT→Cipher Text
H→ Histogram
FD→Frequency Distribution
P (S_i)→ Cumulative Probability

Step 1: Accept the Video File
Step 2: Binary data has been send for the cipher text creation.

PT= binary (VF)
Step 3: Create the cipher text by the help of symmetric 128 bit key.

CT=Encryption (PT, K)

It is subdivided according to the binary data.

C_1= Encryption (PT_1 + Initial Vector)
C_2= Encryption (PT_2 + Initial Vector)
……..
……..
……..
C_n= Encryption (PT_n + Initial Vector)
Step 4: Histogram Calculation for the encrypted data

$$H = \frac{FD}{W}$$

Step 5: Get the plain text by the help of symmetric 128 bit key.

PT=Decryption (CT, K)
It is subdivided according to the binary data.

PT_1= Decryption (CT_1 + Initial Vector)
PT_2= Decryption (CT_2 + Initial Vector)
……..
……..
……..
PT_n= Decryption (CT_n + Initial Vector)
Step 6: Histogram Calculation for the decrypted data

$$H = \frac{FD}{W}$$

Step 7: Entropy Calculation

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

4. Result Analysis

The results shown below show the effectiveness of our approach. We first consider the sample video image and create the bin Histogram after performing symmetric encryption as shown in figure 3. The Histogram of the original video or after decryption is different which is shown in figure 4. The detraction clearly shows the bin differences are very high so that it will be more secure in comparison to the previous technique. Then we have considered five different sample videos and calculated the information entropy which is also different in all cases. So the results show the security is enhanced in our technique.

Table 1: Entropy Comparison

S. No	Name	Original	Encrypted
1	Sample 1	7.8087	7.9999
2	Sample 2	7.7069	7.9999
3	Sample 3	7.7497	7.9499
4	Sample 4	7.752	7.99993

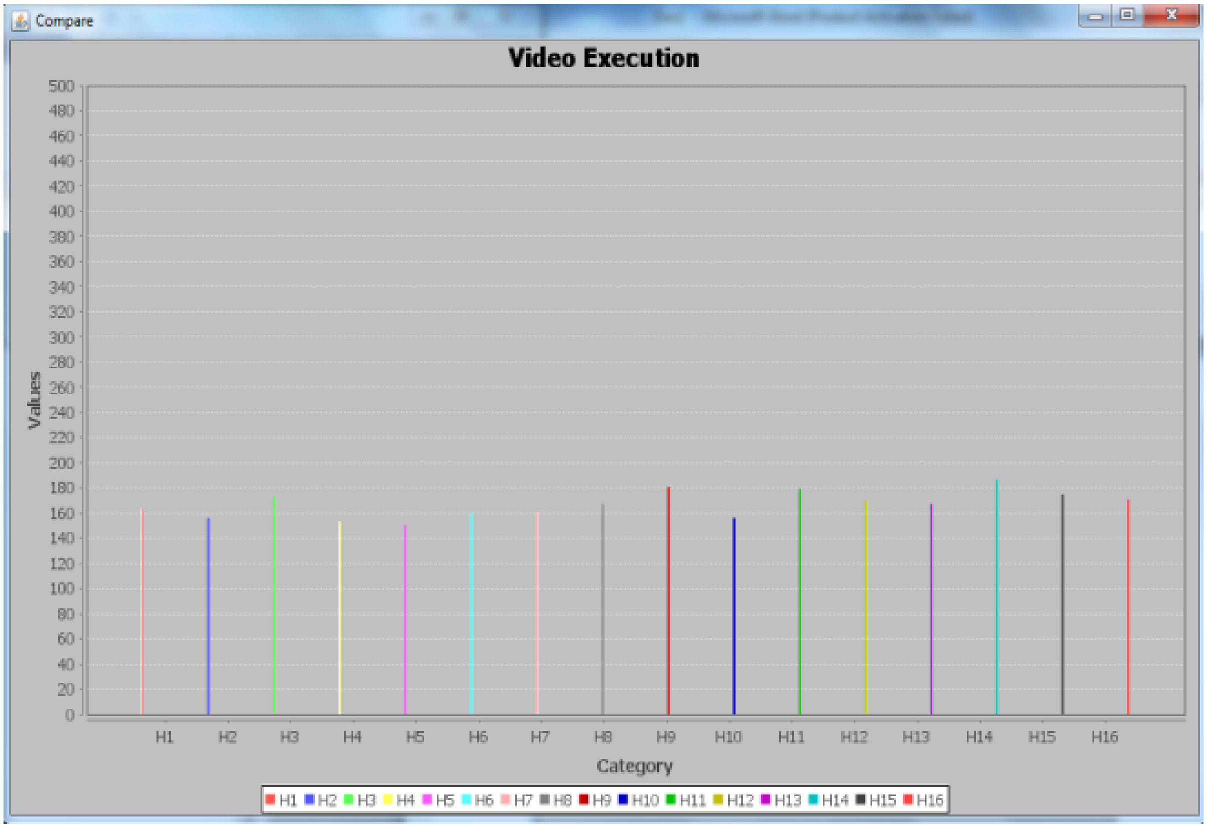

Figure 3: Histogram (After Encryption)

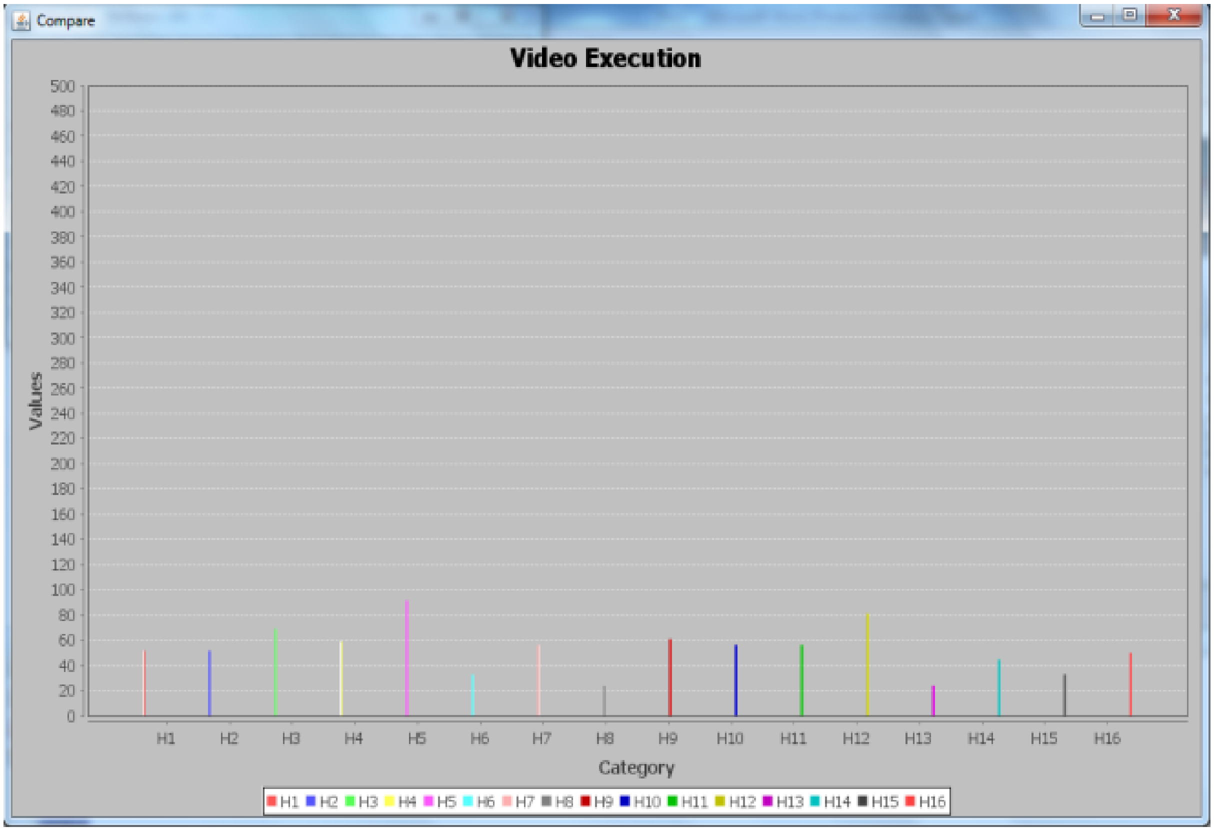

Figure 4: Histogram (After Decryption)

5. Conclusion

In this paper several methodologies have been discussed and proposed an efficient video encryption technique. Our methodology has significant difference in the bins as in the encrypted data and in the original video. The entropy difference also shows the encryption mechanism provide better security in terms of previous method.

References

[1] Vipula Madhukar Wajgade, Dr. Suresh Kumar," Enhancing Data Security Using Video Steganography", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 4, April 2013.

[2] Spyridon K. Kapotas and Athanassios N. Skodras, "A New Data Hiding Scheme for Scene Change Detection in H.264 Encoded Video Sequences" in Proc. IEEE Int. Conf. Multimedia Expo ICME, pp. 277–280, Jun. 2008.

[3] Lathikanandini. M, Suresh. J," Steganography in MPEG Video Files using MACROBLOCKS", International Journal of Advanced Computer Research (IJACR), Volume-3, Number-1, Issue-8 March-2013.

[4] Ashutosh Kumar Dubey, Animesh Kumar Dubey, Mayank Namdev, Shiv Shakti Shrivastava,"Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment", CONSEG 2012.

[5] Ashutosh Kumar Dubey, Animesh Kumar Dubey, Vipul Agarwal, Yogeshver Khandagre, "Knowledge Discovery with a Subset-Superset Approach for Mining Heterogeneous Data with Dynamic Support", CONSEG 2012.

[6] Preeti Khare, Hitesh Gupta, "Finding Frequent Pattern with Transaction and Occurrences based on Density Minimum Support Distribution", International Journal of Advanced Computer Research (IJACR), Volume-2, Number-3, Issue-5 September-2012.

[7] Lakhtaria, Kamaljit I. "Protecting computer network with encryption technique: A Study." In Ubiquitous Computing and Multimedia

Applications, pp. 381-390. Springer Berlin Heidelberg, 2011.

[8] Chan, Aldar CF, and Claude Castelluccia. "A security framework for privacy-preserving data aggregation in wireless sensor networks." ACM Transactions on Sensor Networks (TOSN) 7, no. 4 (2011): 29.

[9] William, Stallings, and William Stallings. Cryptography and Network Security, 4/E. Pearson Education India, 2006.

[10] Shannon, Claude E. "Communication Theory of Secrecy Systems*." Bell system technical journal 28, no. 4 (1949): 656-715.

[11] Ganesan, K.; Singh, I.; Narain, M., "Public Key Encryption of Images and Videos in Real Time Using Chebyshev Maps," Computer Graphics, Imaging and Visualisation, 2008. CGIV '08. Fifth International Conference on, pp.211,216, 26-28 Aug. 2008.

[12] Zhang Qian; Wu Jin-mu; Zhao Hai-xia, "Efficiency Video Encryption Scheme Based on H.264 Coding Standard and Permutation Code Algorithm," Computer Science and Information Engineering, 2009 WRI World Congress on , vol.1, no., pp.674,678, March 31 2009-April 2 2009.

[13] Alirezaei, V.; Yaghbi, M., "Efficient Video Encryption by Image Key Based on Hyper-chaos System," Multimedia Communications (Mediacom), 2010 International Conference on , pp.141,144, 7-8 Aug. 2010.

[14] Seohyun Jeong; Eunji Lee; Sungju Lee; Youngwha Chung; Byoungki Min, "Slice-level selective encryption for protecting video data," Information Networking (ICOIN), 2011 International Conference on pp.54,57, 26-28 Jan. 2011.

[15] Guizani, S.; Nasser, N., "An audio/video crypto Adaptive optical steganography technique," Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International, pp.1057,1062, 27-31 Aug. 2012.

[16] Manjunath S Gabasavalagi, Sanjeevakumar M. Hatture, Nalinakshi B. G, Rashmi P. Karchi," Hybrid Level Integration of Biometric Traits for Security Applications" , International Journal of Advanced Computer Research (IJACR),Volume-3, Number-3, Issue-12, September-2013.

[17] R. Tamijetchelvy, P. Sankaranarayanan," An Optimized Multikeying Chaotic Encryption for Real Time Applications ", International Journal of Advanced Computer Research (IJACR),Volume-3, Number-4, Issue-13, December-2013.

[18] Pushpender Prasad Chaturvedi, Amit Singh Rajput, Aabha Jain," Video Object Tracking based on Automatic Background Segmentation and updating using RBF neural network", International Journal of Advanced Computer Research (IJACR),Volume-3, Number-2, Issue-10, June-2013.

[19] Puech, W.; Erkin, Z.; Barni, M.; Rane, S.; Lagendijk, R.L., "Emerging cryptographic challenges in image and video processing," Image Processing (ICIP), 2012 19th IEEE International Conference on , pp.2629,2632, Sept. 30 2012-Oct. 3 2012.

[20] Yadav, P.; Mishra, N.; Sharma, S., "A secure video steganography with encryption based on LSB technique," Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on, pp.1, 5, 26-28 Dec. 2013.

[21] Pritish Bhautmage, Amutha Jeyakumar, Ashish Dahatonde," Advanced Video Steganography Algorithm", International Journal of Engineering Research and Applications (IJERA) Vol. 3, Issue 1, January -February 2013, pp.1641-1644.

[22] Anil Kumar, Rohini Sharma," A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", International Journal of Advanced Research in Computer Science and Software Engineering", Volume 3, Issue 7, July 2013.

[23] Manisha Yadav, Mauli Joshi, Akshita," Improved Secure Data Transfer Using Tiny Encryption Algorithm and Video Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 12, December 2013.

[24] Lekha Bhandari, Avinash Wadhe,"Speeding up Video Encryption using Elliptic Curve Cryptography (ECC)", International Journal of Emerging Research in Management &Technology Volume-2, Issue-3, March 2013.

Akansha Agrawal completed my B.E from Takshshila Institute of Engineering & Technology, Jabalpur, Madhya Pradesh in Computer Science and Engineering Branch. Currently I am pursuing my M.Tech degree from Indore Institute of Science & Technology, Indore, Madhya Pradesh in Computer Science and Engineering Branch. Working as Guest Faculty at Government Engineering College Nowgong, Madhya Pradesh. My Interest areas are Video security, Image processing and Data Mining.