ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

Securing Video Data: A Critical Review

Akansha Agrawal[1], Virendra Singh[2]

M. Tech Research Scholar, Department of Computer Science, Indore Institute of Science and Technology-II, Indore, India[1]

Assistant Professor, Department of Computer Science, Indore Institute of Science and Technology-II, Indore, India[2]

Abstract: In the era of internet we are using several applications which is used for communication, we are sharing images and videos daily in the friends group or in the social community. So our main motivation of the paper is to discover and study the approaches for securing video files. So that video will be send securely and the data will be protected from any unauthorized access. So we study and discuss in this direction and also suggest some future suggestions.

Keywords: Video Security, encryption and decryption techniques, Video Encryption, Communication Path

I. INTRODUCTION

In ancient epoch a growing enumeration in data hiding for image data has been observed in the research community. It is so crucial because of data security and delivery of data without any copyright infringes The Cryptography, Steganography and Watermarking techniques can be used to obtain security and privacy of data [1]. The data hiding system can be used for copy right protection, scene change detection [2] and also for message passing. Data hiding technique can also be used to assess the quality of compressed video in the absence of the original reference. This quality is calculated by computing the degradations of the extracted hidden message [3].

Encryption and decryption of the data in the communication channel are also helpful for protecting the data. For encryption and decryption we can use DES, RSA, RC4 and RC5 algorithms [4]. Block based division can be possible with subset superset mining or partitioning techniques [5][6] It is also useful in the scene where the sending data and the wrapper will be different so that confusion will be increases and the security in the receiving side will be more imposed. In cryptography we perform encryption on the original text to create the cipher text and decryption is just an opposite mechanism to form the plaintext. In steganography we hide the original plaintext within any other, text, PDF, images etc. The mechanism of reading the original text will be separately sent to the receiver for data reading. Cryptography is used to change the original plain text to encode or make unreadable form of text [7]. The excruciating materials are clandestine on the sender comrade in order to have them secluded and spellbound from illicit access and then sent via the network. When the data are received then the opposite process will be employed for decryption depending on an algorithm. Decryption is the process of converting data from encrypted format back to their original format [8][9][10].

We provide here a brief survey on Video Steganography and Cryptography. Other sections are arranged in the following manner: Section 2 describes about Literature Review; Section 3 discusses about problem domain; section 4 shows the analysis; Section 5 describes Conclusions and future work.

II. LITERATURE REVIEW

In 2008, Ganesan, K. et al. [11] suggest that due to rapid developments in limits and possibilities of communications and information transmissions, there is a growing demand of cryptographic techniques, which has spurred a great deal of intensive research activities in the study of cryptography. They discuss the algorithm for textual data and present the cryptanalysis which can be performed on this algorithm for the recovery of encrypted data. They also describe a simple hashing algorithm for making this algorithm more secure, and which can also be used for digital signature. They propose an extension of this algorithm to images and videos and making it secure using multilevel scrambling and hash.

In 2009, Zhang Qian et al. [12] presented three schemes to encrypt parts of video data using permutation code and DES encryption algorithm based on the newest coding standard H.264. Comparing with encryption effects of three encryption schemes using two encryption algorithms respectively determined one of three schemes as a last encryption scheme. This encryption scheme adopts permutation code encryption algorithm to encrypt parts of motion vector residuals after transform and quantization before entropy encoding, and some codewords of DCT coefficients of residual data in the code stream, which includes TrailingOnes signs Levels and RunBefore. It has high security good real-time lower data expansion rate and good form compatibleness by theory analysis and experiment results, so it can guarantee video data safety and real-time to transmit and has a wide application value.

In 2010, Vahid alirezaei et al. [13] suggests an efficient video encryption scheme is constructed by image key and is based on hyperchaos system. The chaotic lattices are used to generate pseudorandom sequences and then selected pixel and bitpixel of image key encrypt frame blocks one by one. By iterating chaotic maps for certain times, the generated pseudorandom sequences obtain high initial-value sensitivity and good randomness. The

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

pseudorandom-bits in each lattice are used to select pixel and bitpixel of image key and then encrypt the Direct Current coefficient (DC) and the signs of the Alternating Current coefficients (ACs). Theoretical analysis and experimental results show that the scheme has good cryptographic security and perceptual security, and it does not affect the compression efficiency apparently.

In 2011, Seohyun Jeong et al. [14] propose a more efficient selective encryption approach which exploits the error propagation property in MPEG2 standard. Their experimental results show that the proposed approach can reduce the execution time of SECMPEG by a factor of 32 without degradation of the security.

In 2012, Guizani, S. et al. [15] suggest that the optical crypto technique is based on double random phase encoding algorithm to encrypt and decrypt the intended audio/video sequences. The main purpose of steganography algorithms is to hide as much information within the cover media as possible. Therefore, for steganography algorithms, the tradeoff is between the amount of covert information being embedded, called stego-data, and that the ensurance for its presence to remain undetected. While their purposes may seem different, recent advances allow more and more the use of advanced watermarking techniques to embed large amounts of covert information that is also robust against removal and detection. Hybrid security are also discuss in [16][17][18].

In 2012, W. Puech et al. [19] suggest an increasing number of image and video processing problems, cryptographic techniques are used to enforce content access control, identity verification and authentication, and privacy protection. The combination of cryptography and signal processing is an exciting emerging field. This introductory paper gives an overview of approaches and challenges that exist in applying cryptographic primitives to important image and video processing problems, including (partial) content encryption, secure face recognition, and secure biometrics. Their aims to help the community in appreciating the utility and challenges of cryptographic techniques in image and video processing.

In 2013, Pooja Yadav et al. [20] suggest that the Video is simply a sequence of images; hence much space is available in between for hiding information. In proposed scheme video steganography is used to hide a secret video stream in cover video stream. Each frame of secret video will be broken into individual components then converted into 8-bit binary values, and encrypted using XOR with secret key and encrypted frames will be hidden in the least significant bit of each frames using sequential encoding of Cover video. To enhance more security each bit of secret frames will be stored in cover frames following a pattern BGRRGBGR.

In 2013, Pritish Bhautmage et al. [21] proposed a new technique for data embedding and extraction for high resolution AVI videos. In this method instead of changing the LSB of the cover file, the LSB and LSB+3 bits are changed in alternate bytes of the cover file. The secret message is encrypted by using a simple bit exchange method before the actual embedding process starts. An index can also be created for the secret information and the index is placed in a frame of the video itself. With the help of this index, they can easily extract the secret message, which can reduce the extraction time.

In 2013, Anil Kumar et al. [22] have proposed a new technique of image steganography i.e. Hash-LSB with RSA algorithm for providing more security to data as well as our data hiding method. The proposed technique uses a hash function to generate a pattern for hiding data bits into LSB of RGB pixel values of the cover image. This technique makes sure that the message has been encrypted before hiding it into a cover image. If in any case the cipher text got revealed from the cover image, the intermediate person other than receiver can't access the message as it is in encrypted form.

In 2013, Manisha Yadav et al. [23] tries to alter the originality of the data files into encrypted form using Tiny Encryption Algorithm .This Algorithm is to be designed for simplicity and better performance. In an encryption scheme, information is encrypted using tiny encryption algorithm that changes it into an unreadable cipher text. After encryption, the encrypted data is embed in a video by using the concept of steganography and then this video file sent via email. The application should have a reversal process as of which should be in a position to decrypt the data to its original format upon the proper request by the user.

In 2013, Lekha Bhandari et al. [24] propose a computationally efficient and secure video encryption algorithm. This makes secure video encryption feasible for real time applications without any extra dedicated hardware. In addition, special and reliable security in storage and transmission of digital images and videos is needed in many digital applications such as confidential video conferencing and medical imaging systems, etc. Unfortunately, the classical techniques for data security are not appropriate for the current multimedia usage. As a result, they need to develop new security protocols or adapt the available security protocols to be applicable for securing the multimedia applications. They have implemented elliptic curve cryptography (ECC) and RC5 algorithm are mentioned. RSA based encryption has significant problems in terms of key size. Currently, the RSA algorithm requires the key length of at least 1024 bits for long term security, whereas it seems that 160 bits are sufficient for elliptic curve cryptographic functioning.

III. PROBLEM DOMAIN

In [25] authors present a new method of real-time steganography using video bit streams. The basis of this method is using the combination of video, audio, text. In order to hide information in the output message, they suggest making use of other methods of image steganography, which is impartial to the provided furtively. By improving this method, they can get the video files without any noise distraction. Change of the spatial pixel values variance can be estimated in the

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

compressed domain, and the embedding payload is allotted according to the variance of each cover frame. Therefore the correlation of the continuous frames is unchanged. But more security will be applied at the pixel level can provide proper variance also.

Table 1: PSNR Values of Different Video Sequences [13]

Videos	y component	u component	Yuv component
Stefan	13.4369	12.1670	9.9660
Foreman	11.5638	11.0838	10.4427
Akiyo	16.4143	13.2990	11.3551
Salesman	17.5727	13.8912	11.7581

Table 2: Test of Time Efficiency [13]

Videos	Encryption/compression	Decryption/decompression
Stefan	1.1	2.3
Foreman	0.95	1.9
Akiyo	1.0	2.1
Salesman	1.5	3.7

In [13] authors measure the quality of the encrypted content, the peak signal-to-noise ratio (PSNR) is tested. PSNR was calculated for video's presented in Table1. Additionally they presented the time ratio in table 2. In [13] the results show that the proposed stream cipher satisfies the requirement of secure encryption principles, the encrypted videos are secure in perception, the encryption operation does not change the compression ratio apparently.

But the performance of the encryption system can be improved by applying some standard encryption scheme.

Table 3: Encryption Times for 610kb Video Data [14]

	Full Encryption	SECMPEG	Slice-Level
Total Data Size	610KB	610KB	610KB
I-frame Size	129KB	129KB	129KB
Size of Encryption	610KB	207KB	7KB
Execution Time	0.73sec	0.25sec	0.008sec

Table 4: Relative Confusion Degree of Selective Encryptions Measured With MSE [14]

Security	SECMPEG	Slice-Level
RCD	99.9%	99.7%

In [14] Table 3 shows the encryption times for 619KB with each encryption approaches. We can see, the proposed "slicelevel" approach can reduce significantly the execution time of SECMPEG. In [14] authors confirmed that the proposed approach could reduce the execution time of SECMPEG by a factor of 32 without degradation of the security. There is a scope of improving the security by using any standard security system.

In [26] authors have attempted to follow random frame skipping. But the very first I-frame in each frameset is always set aside to exploit as the reference frame. The implementation scheme applying MPEG-21 DIA is purely a temporal one, so the quality degradation of the adapted video is due to frame dropping only, especially when the target frame rate is less than 15 fps. So this procedure can be adopted also.

In [27] author suggests that increasing the number of rounds to at least 16 will increase security against differential cryptanalysis. This was in-fact suggested by Rivest [28] that security will increase when the number of rounds of encryption is increased. Even though we used a 32 bit version of RC5, authors increased the number of rounds to 20 so as to have good computational security. From [27] we have found a new insight in the direction of increasing the video security. The security can be applied on Mobile devices with proper management of data by data mining [29].

Table 4: Encryption Overhead on Compression and Encryption Time per Frame [27]

Name	Size of Frames	Original Size(KB)	Total Number of Frames	Number of I-Frames	Encrypted Video Size	HIT	MISS
Pond	352x244	5144	611	61	7400	997977	65072
Cat	704x576	19692	737	62	28048	909737	24169
Professor	352x240	10164	703	47	11040	159564	10925
Satelitevieww	720x576	22252	2528	141	41472	2121612	50519
Street	640x480	9196	819	546	19865	2083735	143082
Table Tennis	352x240	1224	150	26	3196	215534	5042
Training	352x240	34168	7292	456	41148	997977	65072
Iceland	384x288	7668	1108	74	10376	180207	16182

IV. ANALYSIS

After studying several research papers we come with the following analysis:

1. There is a significant requirement of applying standard encryption and decryption techniques.
2. Encryption and Decryption techniques are combined for providing more encryption strength.
3. Need of reducing the encryption and decryption time which will not affect the strength of security.
4. There is some security mechanism which can protect the password leakage.
5. We can use partition based encryption to provide more impact.
6. To improve the confusion the data should be changed in different format.

V. CONCLUSION AND FUTURE SUGGESTIONS

In this paper we have studied and discussed different methodologies presented in the previous research work as well as different cryptography and steganography mechanism. We also discuss the merits and some of the

findings which will be incorporated to improve the security and reduces the time. Based on our study we will suggest hybrid framework with proper encryption /decryption technique and steganography. Slice based division and securing the division is also helpful for improving the security in future. Data confusion will be an added advantage in this security phenomenon.

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 K. (2011) Protecting computer network with encryption technique: A Study. International Journal of u- and e-service, Science and Technology 4(2).

[8] Chan, A. (2011) A Security framework for privacy preserving data aggregation in wireless sensor networks. ACM transactions on sensor networks 7(4).

[9] Stalling, W. (2005) Cryptography and network security principles and practices ,4th edition Prentice Hall.

[10] Shannon, C. E. (1948) Communication Theory of secrecy systems. Bell System Technical Journal.

[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 , vol., no., 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 , vol., no., 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 , vol., no., 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 , vol., no., 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 , vol., no., 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 , vol., no., 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.

[25] S. Suma Christal Mary," Improved Protection In Video Steganography Used Compressed Video Bit streams", International Journal on Computer Science and Engineering ,Vol. 02, No. 03, 2010, 764-766.

[26] Iqbal, Razib, Shervin Shirmohammadi, and Abdulmotaleb El Saddik. "Compressed-domain encryption of adapted H. 264 video." Multimedia, 2006. ISM'06. Eighth IEEE International Symposium on. IEEE, 2006.

[27] Raju, Chigullapally Narsimha, et al. "Fast and secure real-time video encryption." Computer Vision, Graphics & Image Processing, 2008. ICVGIP'08. Sixth Indian Conference on. IEEE, 2008.

[28] R. L. Rivest. The RC5 encryption algorithm. In Proc. of the Second International Workshop on Fast Software Encryption (FSE), pages 86–96, 1994.

[29] Ashutosh K. Dubey and Shishir K. Shandilya," A Novel J2M E Service for M ining Incremental Patterns in Mobile Computing", Communications in Computer and Information Science, 2010,Springer LNCS.