International Journal of Advanced Technology and Engineering Exploration
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
Volume-2 Issue-12 November-2015

A meta-analysis of Video Data Security

Abhilasha Yadav[1*] and Kailash Patidar[2]
M.Tech Student, Computer Science, SSSIST, Bhopal[1]
HOD, Computer Science, SSSIST, Bhopal[2]

Abstract

Data Security is important in all field of data communication as it is very important so that any unauthorized access of data can be prevented. There are several ways to secure the data in which cryptography and steganography is the main. Data security is also depends on the data type. As there is not a single universal technique which can secure all the types of data. There is the need to change the proliferation and implementation so that it can be applied to different type of possibilities. In this paper we have discussed about video cryptography and steganography so that we will able to secure the video data.

Keywords

Video Cryptography, Video Steganography, Data Security, Data Type.

1. Introduction

In obsolete age a creating recognizable proof in data stowing without end for picture data has been found in the examination bunch. It is so fundamental as a consequence of data security and transport of data with no copyright infringes The Cryptography, Steganography and Watermarking frameworks can be used to get security and assurance of data [1]. The data hiding system can be used for copy right protection, scene change disclosure [2] besides for message passing. Data hiding strategy can in like manner be used to study the way of compacted video without the first reference. This quality is found out by figuring the defilements of the isolated covered message [3]. Steganography is the one of the genuine techniques in the scope of information concealing [4]. Security is a foremost angle which must be taken into record from the initial steps of the configuration procedure of appropriated databases, particularly in security basic situations [5].

*Author for correspondence

Security and attack detection mechanism are also discussed in [6-9].

Encryption and decoding of the information in the correspondence channel are additionally useful for ensuring the information. For encryption and unscrambling and can utilize DES, RSA, RC4 and RC5 calculations [10]. Square based division can be conceivable with subset superset mining or apportioning strategies [11][12]. It is additionally valuable in the scene where the sending information and the wrapper will be diverse so disarray will be increments and the security in the getting side will be more forced. In cryptography we perform encryption on the first content to make the figure content and unscrambling is only an inverse instrument to frame the plaintext. In steganography we shroud the first plaintext inside of whatever other, content, PDF, pictures and so on. The component of perusing the first content will be independently sent to the beneficiary for information perusing. Cryptography is utilized to change the first plain content to encode or make indistinguishable type of content [13]. The unbearable materials are surreptitious on the sender friend with a specific end goal to have them disengaged and enchanted from unlawful access and after that sent by means of the system. At the point when the information are gotten then the inverse procedure will be utilized for decoding relying upon a calculation. Decoding is the procedure of changing over information from encoded organization back to their unique configuration [14][15][16].

2. Literature Review

In 2010, Vahid alirezaei et al. [17] recommends a proficient video encryption plan is built by picture key and depends on hyperchaos framework. The tumultuous cross sections are utilized to create pseudorandom groupings and after that chose pixel and bitpixel 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 2011, Seohyun Jeong et al. [18] propose 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 2012, Guizani, S. et al. [19] propose 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 tradeoff is between the measure of secretive data being implanted, called stego-information, and that the ensurance 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 likewise powerful against evacuation and location.

In 2012, Baluram Nagaria et al. [20] 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 2012, W. Puech et al. [21] 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. Their expects to help the group in valuing the utility and difficulties of cryptographic strategies in picture and video preparing.

In 2013, Pooja Yadav et al. [22] propose 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. To upgrade more security every piece of mystery casings will be put away in spread casings taking after an example BGRRGBGR.

In 2013, Pritish Bhautmage et al. [23] 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 2013, Anil Kumar et al. [24] 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 2013, Manisha Yadav et al. [25] tries 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 insert 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 2013, Lekha Bhandari et al. [26] propose 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. 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. Problem Domain

The following gaps are identified after the above study and discussion:

1) Symmetric block cipher encryption and decryption techniques are needed for better security.
2) Multiple keys randomization will secure the password breach mechanism.
3) Data steganography can be used to provide better hiding with other data type or the same.
4) As video data is very heavy the data can be handled by data mining techniques with proper data classification.
5) XOR can be operated in the middle to shuffle the data and rearrangements.

4. Analysis

In [18] Table 1 demonstrates the encryption times for 619KB with every encryption approaches. We can see, the proposed “slice level” methodology can diminish altogether the execution time of SECMPEG. In [14] authors confirmed that the Proposed methodology could lessen the execution time of SECMPEG by an element of 32 without corruption of the security. There is an extent of using so as to enhance the security any standard security framework.

Table 1: 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
Security	Null	99.9%	99.7%

The result comparison from [27] is shown below.

Table 2: 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
Satelitеview	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

For comparing the quality of encryption standard peak signal-to-noise ratio (PSNR) are compared in [17] which is shown below.

Table 3: Video PSNR Comparison [17]

Videos	PSNR(db)		
	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

Based on the above analysis we can understand that the parameters and methods used for video security is cryptography and steganography and the methods are compared based on the PSNR, Mean Square Error (MSE), RGB Histogram comparison and entropy calculation.

5. Conclusion and Future Suggestions

This paper provides the analysis on video encryption based on the previous related research. In this paper we have first explores the previous research with their advantages and disadvantages. Then we suggest the gaps and the analysis. We have also discussed the parameters for the comparison. Based on the discussion we can suggest standard encryption technique with histogram comparison and entropy evaluation which will be better security option.

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] Satish Bhalshankar and Avinash K. Gulve, " Audio Steganography: LSB Technique Using a Pyramid Structure and Range of Bytes ", International Journal of Advanced Computer Research (IJACR), Volume-5, Issue-20, September-2015, pp.233-248.

[5] Arunabha Sengupta, "Dynamic fragmentation and query translation based security framework for distributed databases", International Journal of Advanced Computer Research (IJACR), Volume-5, Issue-20, September-2015, pp.249-263.

[6] Manju Kaushik, Gazal Ojha , " Attack Penetration System for SQL Injection " , International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-15, June-2014 ,pp.724-732.

[7] Dubey, Animesh, Ravindra Gupta, and Gajendra Singh Chandel. "An Efficient Partition Technique to reduce the Attack Detection Time with Web based Text and PDF files." International Journal of Advanced Computer Research (IJACR) 3.1 (2013): 9.

[8] Urmi Chhajed, Ajay Kumar, "Detecting Cross-Site Scripting Vulnerability and performance comparison using C-Time and E-Time", International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-15, June-2014, pp.733-740.

[9] 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.

[10] 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.
[11] 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.
[12] Lakhtaria K. (2011) Protecting computer network with encryption technique: A Study. International Journal of u- and e-service, Science and Technology 4(2).
[13] Chan, A. (2011) A Security framework for privacy preserving data aggregation in wireless sensor networks. ACM transactions on sensor networks 7(4).
[14] Stalling, W. (2005) Cryptography and network security principles and practices, 4th edition Prentice Hall.
[15] Shannon, C. E. (1948) Communication Theory of secrecy systems. Bell System Technical Journal.
[16] 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.
[17] 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.
[18] 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.
[19] 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.
[20] Baluram Nagaria, Ashish Parikh ,Sandeep Mandliya ,Neeraj shrivastav," Steganographic Approach for Data Hiding using LSB Techniques", International Journal of Advanced Computer Research (IJACR),Volume-2 Number-4 Issue-6 December-2012.
[21] 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.
[22] 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.
[23] 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.
[24] 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.
[25] 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.
[26] 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.
[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.

Abhilasha Yadav, received her Bachelor's degree in computer science engineering from Gautam Buddh Technical University, Uttar Pradesh .She pursue her master degree in software engineering from, SSSIST, Sehore, M.P., India.
Email: abhilashay0@gmail.com

Mr. Kailash Patidar, HOD of computer science engineering /information technology, SSSIST, Sehore, M.P., India.