Review Article

ACCENTS Transactions on Information Security, Vol 3(9)
ISSN (Online): 2455-7196
http://dx.doi.org/10.19101/TIS.2018.39003

A survey and analysis for securing video data

Jitendra J. Bonde[1*], Kailash Patidar[2], Manoj Kumar Yadav[3], Narendra Sharma[3] and Rishi Kushwah[3]

M.Tech Scholar, Department of Computer Science, School of Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India[1]

Professor and HOD, Department of Computer Science, School of Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India[2]

Assistant Professor, Department of Computer Science, School of Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India[3]

Abstract

Information security is essential in all field of information correspondence as it is vital so that any unapproved access of information can be anticipated. There are few approaches to secure the information in which cryptography and steganography is the fundamental. Information security is additionally relies upon the information sort. As there is not a solitary general strategy which can secure every one of the sorts of information. There is the need to change the expansion and usage with the goal that it can be connected to various kinds of conceivable outcomes. In this paper we have discussed about the video cryptography and steganography with the goal to secure the video information. For this a detail survey and analysis have been presented followed by detail discussion to find out the advantages and disadvantages.

Keywords

Video cryptography, Video steganography, Data security, XOR.

1.Introduction

In this age a making unmistakable verification in information stowing without end for picture information has been found in the examination group. It is as major as an outcome of information security and transport of information with no copyright encroaches The Cryptography, Steganography and Watermarking systems can be utilized to get security and confirmation of information [1]. The information concealing framework can be utilized for duplicate right insurance, scene change divulgence [2] other than for message passing. Information concealing system can in like way be utilized to ponder the method for compacted video without the principal reference. This quality is discovered by figuring the pollutions of the separated secured message [3]. Steganography is the one of the honest to goodness methods in the extent of data disguising [4]. Security is a principal edge which must be taken into record from the underlying strides of the setup technique of appropriated databases, especially in security essential circumstances [5].

*Author for correspondence

Security and attack discovery component are likewise talked about in [6−9].

Encryption and unraveling of the data in the correspondence channel are also helpful for guaranteeing the data. For encryption and unscrambling and can use DES, RSA, RC4 and RC5 estimations [10].

Square based division can be possible with subset superset mining or distributing methodologies [11, 12]. It is moreover important in the scene where the sending data and the wrapper will be various so confuse will be additions and the security in the getting side will be more constrained. In cryptography we perform encryption on the primary substance to make the figure substance and unscrambling is just a converse instrument to outline the plaintext. In steganography we cover the main plaintext within whatever other, content, PDF, pictures etc. The part of scrutinizing the principal substance will be autonomously sent to the recipient for data examining. Cryptography is used to change the main plain substance to encode or make unclear kind of substance [13]. The terrible materials are surreptitious on the sender companion with a

particular true objective to have them withdrawn and captivated from unlawful get to and after that sent by method for the framework. Exactly when the data are gotten then the reverse methodology will be used for disentangling depending upon a computation. Translating is the strategy of changing over data from encoded association back to their special setup [14−16].

The objective of this paper is to analyze the study based on the related works.

2.Literature review

In 2010, Alirezaei and Yaghbi [17] prescribes a capable video encryption plan is worked by picture key and relies on upon hyperchaos system. The tumultuous cross segments are used to make pseudorandom groupings and after that picked pixel and bitpixel of picture key scramble edge squares one by one. By rehashing wild maps for particular times, the made pseudorandom groupings obtain high beginning quality affectability and incredible inconsistency. The pseudorandom-bits in each cross area are used to pick pixel and bitpixel of picture key and a while later encode the Direct Current coefficient (DC) and the signs of the Alternating Current coefficients (ACs). Theoretical examination and exploratory results exhibit that the arrangement has incredible cryptographic security and perceptual security, and it doesn't impact the weight efficiency clearly.

In 2011, Jeong et al. [18] propose a more profitable particular encryption approach which abuses the misstep spread property in MPEG2 standard. Their test outcomes exhibit that the proposed strategy can diminish the execution time of SECMPEG by a part of 32 without debasement of the security.

In 2012, Guizani and Nasser [19] suggest that the optical crypto framework relies on upon twofold self-assertive stage encoding figuring to scramble and decipher the normal sound/video groupings. The essential inspiration driving steganography figurings is to stow away however much information within the spread media as could be normal. Along these lines, for steganography figurings, the tradeoff is between the measure of hidden information being embedded, called stego-data, and that the ensurance for its region to remain undetected. While their reasons may seem, by all accounts, to be changed, late advances allow progressively the usage of front line watermarking systems to embed a considerable measure of mystery information that is in like manner intense against clearing and area.

In 2012, Nagaria et al. [20] proposed a DCT based steganography arrange for which gives higher impenetrability to picture taking care of attacks, for instance, JPEG weight, fuss, upheaval, elucidation et cetera. For securing the data, this will be mystery key guaranteed. For arrangement this test framework we have encoded our data and after that without watchword we won't unscramble the data. The differentiation between the two is in the appearance in the readied yield; the yield of Steganography operation is not unmistakably recognizable yet rather in cryptography the yield is blended with the objective that it can draw thought. They have endeavored to elucidate the particular approachs towards utilization of Steganography using "sight and sound" archive (content, static picture, sound and video) and Network IP datagram as spread.

In 2012, Puech et al. [21] prescribe a growing number of picture and video planning issues, cryptographic systems are used to approve substance get to control, character check and confirmation, and security affirmation. The mix of cryptography and sign get ready is an invigorating creating field. This at an early stage paper gives a survey of systems and troubles that exist in applying cryptographic primitives to basic picture and video taking care of issues, including (mostly) content encryption, secure face affirmation, and secure biometrics. Their hopes to help the gathering in esteeming the utility and challenges of cryptographic methodologies in picture and video get ready.

In 2013, Yadav et al. [22] recommend that the Video is essentially a gathering of pictures; in this way much space is open amidst for covering information. In proposed arrange video steganography is used to cover a secret video stream in spread video stream. Each edge of riddle video will be broken into individual sections then changed over into 8-bit twofold values, and encoded using XOR with puzzle key and mixed edges will be concealed at all immense bit of each housings using continuous encoding of Cover video. To redesign more security each bit of riddle housings will be secured in spread housings taking after a case BGRRGBGR.

In 2013, Bhautmage et al. [23] proposed another procedure for data embedding and extraction for high assurance AVI recordings. In this framework rather than changing the LSB of the spread report, the LSB

and LSB+3 bits are changed in exchange bytes of the spread record. The riddle message is mixed by using a clear piece exchange technique before the genuine embedding system starts. A rundown can in like manner be made for the riddle information and the rundown is placed in a packaging of the video itself. With the help of this rundown, they can without a lot of an extend focus the puzzle message, which can lessen the extraction time.

In 2013, Kumar and Sharma [24] have proposed another arrangement of picture steganography i.e. Hash-LSB with RSA computation for giving more security to data and our data hiding strategy. The proposed system uses a hash ability to make a case for covering data bits into LSB of RGB pixel estimations of the spread picture. This technique confirms that the message has been mixed before hiding it into a spread picture. In case in any case the figure content got revealed from the spread picture, the widely appealing individual other than recipient can't get to the message as it is in mixed structure.

In 2013, Yadav et al. [25] tries to adjust the advancement of the data archives into mixed structure using Tiny Encryption Algorithm .This Algorithm is to be planned for ease and better execution. In an encryption arrange, information is mixed using little encryption estimation that movements it into a distorted figure content. After encryption, the mixed data is embedding in a video by using the possibility of steganography and after that this video record sent through email. The application should have a reversal procedure as of which should be in a position to unscramble the data to its one of a kind association upon the right requesting by the customer.

In 2013, Bhandari and Wadhe [26] propose a computationally capable and secure video encryption count. This makes secure video encryption feasible for nonstop applications with no extra gave gear. Besides, and strong security away and transmission of automated pictures and recordings is required in various propelled applications, for instance, private video conferencing and restorative imaging structures, etc. Heartbreakingly, the set up techniques for data security are not appropriate for the present intuitive media use. Likewise, they need to develop new security traditions or change the open security traditions to be material for securing the intuitive media applications.They have completed elliptic curve cryptography (ECC) and RC5 estimations are said. RSA based encryption has basic issues similarly as key size. At present, the RSA estimation requires the key length of no less than 1024 bits for whole deal security, while it creates the impression that 160 bits are sufficient for elliptic twist cryptographic working.

In 2017, Naveen et al. [27] suggested that the video compression and security is important for reliable and fast communication. They have proposed a combination of embedded zero wavelet (EZW) and chaotic logistic map. It emphasizes both compression and security. In the primary stage, video is encoded utilizing decoupled 3D-DWT design and after that compacted utilizing EZW. The information acquired from EZW is given as contribution to the turbulent calculated guide, which gives security. Disordered rationale delineate utilized for giving security as it is straightforward and that's just the beginning delicate towards the adjustments in the underlying conditions. The time taken to give security is effectively lessened by tumultuous calculated outline. To give a dependable security two keys are utilized at the transmitter and three keys are utilized at the recipient. The planning prerequisite of the clamorous calculated guide calculation is analyzed with the AES in the outcomes area and observed to be vastly improved.

In 2017, Elshamy et al. [28] suggested that the multimedia data security has become very important for the government and military fields. They have applied a video encryption technique and compared it with Henon chaotic map system, phase modulation system and the proposed technique.

In 2016, Iyer et al. [29] suggesting the video encryption is important as the communication based on video data is increasing. The video information that movements back and forth between the sender and the beneficiary needs to go through the most unsecure medium of correspondence, the web. The current strategies for giving security to the video information depends fundamentally on overwhelming sign handling calculations which require a ton of data transmission and sets aside a considerable measure of opportunity to complete the encryption bringing about slacks in correspondence. Then again, no single encryption calculation is sufficiently secure to give a totally impeccable and lossless outcome. Their proposed approach has the advantages of hybrid technique of encryption with less time.

3.Problem domain

Based on the above analysis in the related work section the following gaps have been identified:

1) Standard encryption and decryption techniques can be applied.
2) Key should be secure with the random prioritization.
3) AES and Blowfish algorithms can be used for developing better security framework.
4) Pixel shuffling can be done with XOR operation for proper data rearrangement.
5) Data encryption can be applied in such manner that it takes less time also means it should be efficient in computation.

4.Analysis

For comparing the quality of encryption standard peak signal-to-noise ratio (PSNR) has been compared in [17]. 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.

In [18] encryption times for 610kb video data have been compared and analyzed. It is observed that the proposed "slice level" approach has reduce execution time in comparison to the secure MPEG (SECMPEG) and full encryption. They have affirmed that the proposed strategy could reduce the execution time of SECMPEG by a component of 32 without defilement of the security. There is a degree of utilizing in order to improve the security any standard security structure. In [30] compared the video encryption. Their decision is based on multiple aspects. There are preparing time, execution, security, dynamism of framework, and affect from mistake engendering. AES/CTR/PKCS5Padding have preparing time around 125, 4781 millisecond to encode 2 KB hex information from test video. Their approach produce up to 256-bit key, which is secure enough. Their framework is dynamic means hard to foresee the ciphertext and if ciphertext mistake occured while proliferating, it just influences those mistake bits, not different bits.

In [31] they have posed the I and P frames encryption. The encryption is key based encryption of edges. Plans for encryption effectively considered in writing. Their encryption is connected on information other than movement vectors that is I edges and specific P outlines. The key with which encryption is prepared is encoded utilizing RSA. Hence open key encryption conspire which is utilized for key trade while the real encryption is finished utilizing private key encryption with traded key. We trust this plan will be productive and hearty because of particular edge encryption.

In [32] AES have been used for video encryption. They have compared their approach with the DES algorithm. In [33] they have proposed a new selective encryption. It is used for encryption of the compressed video frames from each group of pictures (GOP). They have used indexed based chaotic sequence. They have suggested that there is not any confidential information leakage possible.

5.Conclusion and future suggestions

This paper provides detail insights on video data encryption to secure it in the manner that it is feasible in time and covering the latest security also. For this a detail survey and analysis have been presented followed by the discussion. The discussion suggests that there is a need of standard encryption technique along with the bit wise shuffling of pixel data. It can be suggested that by the help of RGB color distribution randomly along with the entropy calculation the methods have been checked also for their effectiveness.

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 international conference on multimedia and expo 2008 (pp. 277-80). IEEE.
[3] Lathikanandini M, Suresh J. Steganography in MPEG video files using MACROBLOCKS. International Journal of Advanced Computer Research. 2013; 3(8):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. 2013; 3(1):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 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. CONSEG-2012 (pp.1-4).
[11] Khare P, Gupta H. Finding frequent pattern with transaction and occurrences based on density minimum support distribution. International Journal of Advanced Computer Research. 2012; 2(5):165-9.
[12] Lakhtaria KI. Protecting computer network with encryption technique: a study. In international conference on ubiquitous computing and multimedia applications 2011 (pp. 381-90). Springer, Berlin, Heidelberg.
[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).
[14] William S. Cryptography and network security: principles and practice. Prentice-Hall, Inc. 1999:23-50.
[15] Shannon CE. Communication theory of secrecy systems. Bell System Technical Journal. 1949; 28(4):656-715.
[16] Ganesan K, Singh I, Narain M. Public key encryption of images and videos in real time using chebyshev maps. In international conference on computer graphics, imaging and visualisation 2008 (pp. 211-6). IEEE.
[17] Alirezaei V, Yaghbi M. Efficient video encryption by image key based on hyper-chaos system. In international conference on multimedia communications 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 2011 (pp. 54-7). IEEE.
[19] Guizani S, Nasser N. An audio/video crypto-adaptive optical steganography technique. In international wireless communications and mobile computing conference 2012 (pp. 1057-62). IEEE.
[20] Nagaria B, Parikh A, Mandliya S, Shrivastav N. Steganographic approach for data hiding using LSB techniques. International Journal of Advanced Computer Research. 2012; 2(6):441-5.
[21] Puech W, Erkin Z, Barni M, Rane S, Lagendijk RL. Emerging cryptographic challenges in image and video processing. In international conference on image processing 2012 (pp. 2629-32). IEEE.
[22] Yadav P, Mishra N, Sharma S. A secure video steganography with encryption based on LSB technique. In international conference on computational intelligence and computing research 2013 (pp. 1-5). IEEE.
[23] Bhautmage P, Jeyakumar A, Dahatonde A. Advanced video steganography algorithm. International Journal of Engineering Research and Applications. 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).
[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] Naveen C, Raza SF, Satpute VR. Multi key algorithm for performance enhancement of video encryption. In international conference on industrial and information systems 2016 (pp. 666-71). IEEE.
[28] Elshamy AM, Abdelghany MA, Alhamad AQ, Hamed HF, Kelash HM, Hussein AI. Secure implementation for video streams based on fully and permutation encryption techniques. In international conference on computer and applications 2017 (pp. 50-5). IEEE.
[29] Iyer SC, Sedamkar RR, Gupta S. A novel idea of video encryption using hybrid cryptographic techniques. In international conference on inventive computation technologies 2016 (pp. 1-5). IEEE.
[30] Mustafa A. Calculation of encryption algorithm combination for video encryption using two layers of AHP. In international conference on telecommunication systems services and applications 2016 (pp. 1-7). IEEE.
[31] Hole RN, Kolhekar M. Robust video encryption and decryption using selective encryption. In international conference on nascent technologies in engineering 2017 (pp. 1-4). IEEE.
[32] Dumbere DM, Janwe NJ. Video encryption using AES algorithm. In international conference on current trends in engineering and technology 2014 (pp. 332-7). IEEE.
[33] Batham S, Yadav VK, Mallik AK. ICSECV: an efficient approach of video encryption. In international conference on contemporary computing 2014 (pp. 425-30). IEEE.