An Enhanced Multimedia Video Surveillance Security Using Wavelet Encryption Framework

S. Velliangiri

Department of Computer Science and Engineering, CMR Institute of Technology, Hyderabad, Telangana-501401 India
E-mail: velliangiris@gmail.com

Received 21 August 2019; Accepted 07 March 2020;
Publication 30 April 2020

Abstract

Multimedia digital data include medical record and financial documents, which are not guaranteed with security. The concerns for security of multimedia digital data is been a widespread issue in the field of cybernetics. With increasing malwares in video payloads, the proposed study aims to reduce the embedding of malwares using Pseudo Arbitrary Permutation based Cellular Automata Encryption (PAP-CAE) System in video payloads. This method reduces the malware attacks and distortion rate by permuting the secret keys with Pseudo arbitrary permutation. Before the application of PAP-CAE, 2D wavelet transform is applied on the multimedia files that compresses the complex files into different scales and position to be transmitted via a network with reduced size. Simultaneously, it performs the process of decryption and decompression to retrieve the original files. The proposed method is evaluated against existing methods to test its efficacy in terms of detection accuracy, detection time of malwares and false positive rate. The result shows that the proposed method is effective against the detection of malwares in multimedia video files.

Keywords: Wavelet transforms, advanced encryption standard, secured transmission, multimedia video security.

Journal of Mobile Multimedia, Vol. 15_3, 239–254.
doi: 10.13052/jmm1550-4646.1534

1 Introduction

In recent days, the multimedia data including texts, images and videos are transmitted over mobile, internet and cloud [1]. Security is considered as an important constraint on multimedia data transmitted across internet [2]. Hence, it is very necessary to add protection to the files against malware attacks. This should aim at protecting the contents, user privacy and service interaction, etc. For instance, the commercially secret contents has to be secured against the attacks.

Intrusion [3] is regarded as an unwanted behaviour by the intruders to access, manipulate and disable the device through internet services. This may takes several forms of attacks that includes crackers, disgruntled employees or malwares. In general, the behaviour of the intrusion is divided into various types, namely network attacks, data driven attacks, host based attacks, unauthorized logins and sensitive files accessing and malwares. The most vulnerable of which is the malwares that tends to create an executable process to steal, access and tamper the multimedia data.

Hence, it is necessary to consider the intrusion behaviour of unauthorised users to steal the multimedia contents. The study on such behaviour should be carried out effectively by taking in account the complexity of the system. Several existing method focus on protecting the multimedia data against the unauthorized users, interactions between the seller and user or vice versa, or with the third party and non-publishing the private user profiles. Some of the techniques focus on secure interaction, multimedia content security and privacy protection [4]. In last decade, several security technique is proposed to protect the multimedia data and provides support against the security incidents.

Most common technique that can be utilised for the multimedia data security is the encryption technique. However, the encryption should provide resistance against the attacks in recent past. Hence, the use of novel framework that combines the existing encryption techniques with discrete model can improve the encryption process. This helps to glean over massive multimedia data and solves the problems of multimedia data security.

In this paper, pseudo arbitrary permutation with 2D wavelet transform is used to reduce malware in multimedia videos. The security of video frames is increased using pseudo arbitrary permutation combined with CA. In the proposed method, the 2D multi-wavelets is used for compressing the video frames. It is then encrypted using the combined framework of PRP and

CAE with a generated secret key. The proposed system aims at eliminate the malware attacks on multimedia video files.

The main contribution of the proposed work involves the following:

a. The study encrypts the video frames using PAP – CAE system, which is the first encryption technique to be used in video surveillance security.
b. The article develops a novel 2D wavelet transform for compressing the video frames to original video frames and after decryption it performs the decompression to retrieve the original files without loss.
c. The performance of the proposed video surveillance security is compared with other existing methods in terms of several performance metrics. This articulates the efficacy of the proposed work.

The outline of the paper is presented here: Section 2 provides the related works. Section 3 discusses the proposed video surveillance security. Section 4 evaluates the proposed work and Section 5 concludes the entire work with possible directions for future scope.

2 Related Works

Secured protection of multimedia files and copyrights management is regarded as the core enabling technology that enables newer technologies in processing of multimedia files while it surprises the limitations due to data intrusions. In order of the industry to deploy successfully the multimedia video services, it is very necessary to ensure that the data holds integrity, confidentiality and availability.

Several scientists, engineers, practitioners and researchers works in the similar field to design and develop a secure systems to secure the multimedia data to benefit the user privacy. There are several video protection techniques like multimedia encryption, protection architectures, fingerprinting watermarking, and authentication. Among these techniques, multimedia encryption stands as a state-of-the-art encryption methods that adopts fast, secure cryptosystem and encryption scheme to protect the multimedia data. Further, it offers end-to-end security to the video files transmitted across the network or distributing system.

Some of the recent techniques related to the present study includes: Feistel Encryption Scheme for multimedia big data files [5, 6], image-scrambling encryption algorithm [7], chaotic encryption [8, 9], quantization parameter based encryption [10]. These studies operates with enhancement

on basic encryption algorithm. Further, chaos as in [8, 9] is combined with for confusion and diffusion.

Xiao et al. (2016) [16] used a compression based encryption framework using an improved adjustable lightweight encryption scheme with resource-efficient encryption optimization model.

Xiao et al. (2016) [19] provides an analysis model for multimedia data encryption optimization. This method uses general-purpose lightweight speed tunable video encryption scheme with series of intelligent selective encryption control models.

Peng et al. (2017) [17] uses quantization parameter on the encryption of the sign of T1 s and the impact of encrypting inter-macroblock non-zero coefficients, the sign of intra-macroblock non-zero DCT coefficients, the sign of trailing ones, the intra prediction modes (IPMs) and the sign of motion vector difference (MVD) are encrypted to protect the texture and motion information of H.264/AVC.

Thanki et al. (2017) [18] developed a hybrid watermarking scheme in multimedia data using image processing transforms and Compressive Sensing to achieve fragility and security for multimedia data. The compressive sensing is applied on the singular value of wavelet coefficients of watermark image to get the CS measurements. These CS measurements are embedded with embedding factor into the hybrid coefficients of the host medium.

Alsmirat et al. (2017) [21] provides mutual authentication, session key management, data confidentiality, and data integrity in multimedia video streaming. Consequently, only authenticated cameras and authenticated cloud devices are capable of providing the encrypted video frames that are also subject to verification of the entirety of such frames. Since video streaming is a very late-sensitive application, we are investigating various variations of the proposed frame to find safety options that best match the added delay with system security.

Joshi et al. (2017) [22] uses compression of video frames using DCT and DWT multiresolution technique. The security is improved using Arnold transformation technique that enhances the security level and provides larger embedding capacity with improved robustness against attacks.

Thiyagarajan et al. (2019) [20] developed a low-overhead high efficiency video coding encryption scheme in Internet of Multimedia Things (IoMT). This is adopted on low energy frame, where all the syntax elements are encrypted and alternate coefficients are encrypted after the frame correlation with neighboring coefficients to achieve better encryption with low key overhead.

Hence, the proposed system is inspired from the encryption technique used in [11, 20] and [22], where random sequence is used for seeking an optimal solution and simulated annealing algorithm is used to obtain optimal pseudorandom sequences.

Jeong et al. (2019) [15] recently tested the efficacy of a deep learning method called Convolution Neural Network (CNN) against the detection of adversarial samples. Inspired from this, the proposed system uses cellular automaton to encrypt the video frames and provides resistance against all attacks.

3 Proposed Methodology

In the proposed architecture, the main process is shown in following steps:

Step 1: Collect the embedded video payload and segment the video file into video frames.
Step 2: Partition the segmented video frames into several sub-frames.
Step 3: Apply 2D multi-wavelets on sub-frames for compression.
Step 4: Encrypt the compressed pixel and lines of sub-frames using PAP – CAE.

a. Generate a secret key generator
b. Create Cipher text using PAP-CA

Step 5: Transmit the encrypted video frames over the network
Step 6: Reception of encrypted video frames at the receiver
Step 7: Decryption of the video frames at the receiver end
Step 8: Decompression of video sub-frames using inverse 2D multi-wavelets.
Step 9: Combine the subframes to form video frames
Step 10: Combine partitioned video frames to form the video

3.1 Encryption Using Pseudo Arbitrary Permutation with Cellular Automata Encryption System

The PAP-CAE is used for enhancing the multimedia video security that avoids the malware attacks. The PAP is applied on PAP-CAE method is to select a specific permutation with the help of a generated secret key (S). The architecture of PAP is given in Figure 1. The security is given to each video frame by the application of PAP for a specific pixel as in Figure 1.

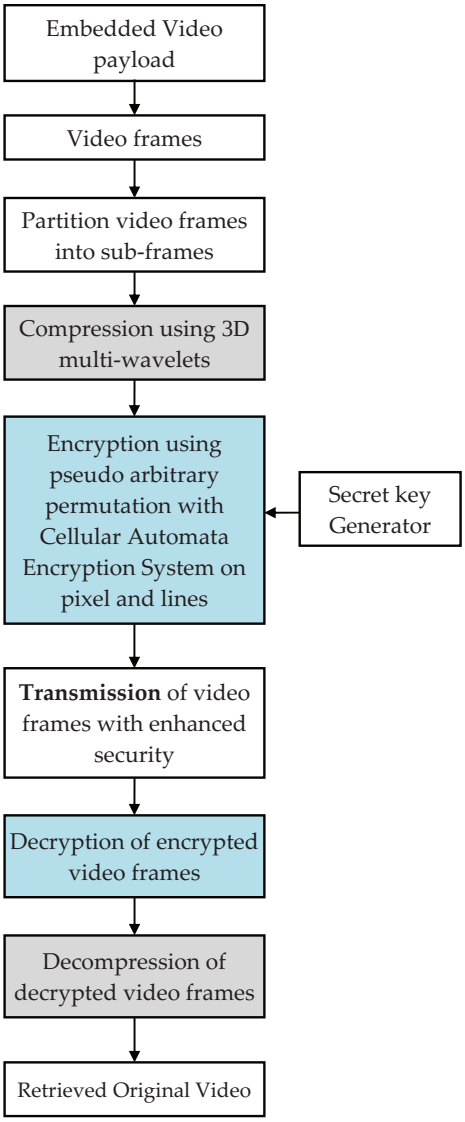


Figure 1 Proposed system architecture.

The video frames are segmented into subframes, where each video frame is encrypted using PAP on a specific lines and pixel of each frames. Each video frame is made of pixel and line. The video frame is applied with random permutation using a secret key generation (S).

Here, each pixel of every column and row is permutated. The random PAP of each pixel is given as follows:

$$\mathrm{X} = \mathrm{Sp}(\mathrm{P}) \tag{1}$$

In Equation (1), P is referred as the value of the pixel of a line in a video frame, X in a video frame is the value of the pixel from different positions and Sp is considered as the secret key of permutation of a pixel. After the application of permutation of PAP on each line, the entire video segment is combined.

In PAP process the random frame permutation function is applied with secret key that tends to create the encrypted video frame. The encryption process using the random permutation with secret key is given as:

$$\mathrm{Y} = \mathrm{Sb}(\mathrm{q}). \tag{2}$$

As specified in Equation (2), Y is refereed as the encrypted frame, Sb is considered as the secret key of the permutation of each line, and q is refereed as the line.

The PAP process is considered as multilevel encryption process that tends to reduce the probability rate of malware detection and it tends to reduce the rate of distortion of video frames. The degree of permutation is fast, however, the security is increased to higher degree by the state transition of each encrypted pixel using CA [12].

CA Phase Transition Encryption

The CA [12, 14] consists of encryption and decryption process, which is given below:

Encryption

Input: Encrypted overall image pixel I of a video frame from PAP
Output: Phase Transition Encrypted Matrix U

Step 1: Apply CA for each pixel of each pixel of a video frame I
Step 2: Repeat Step 1 for all the pixels of a video frame I
Step 3: Convert the phase transition value of CA into 8-bit binary value
Step 4: The first four bits applies the rule 150 of CA
Step 5: The second four bits are applied with rule 60 of CA
Step 6: Save the phase transition results into new video frame values of phase transition pixel Ia

Step 7: Repeat between step 2 to step 5 for each pixel value of I
Step 8: Transmit the matrix that contains the encrypted and phase transition value over the distributed network.

Decryption

Input: Encrypted and Phase transition video frame Ia
Output: Decrypted matrix U

Step 1: Convert the binary value of 8-bit number of encrypted and phase transition video frame
Step 2: The first four bits applies the rule 150 of CA
Step 3: The second four bits are applied with rule 60 of CA
Step 4: Save the phase transition results into video frame values of phase transition pixel
Step 5: Repeat the process of step 2 and step 3 over each pixel
Step 6: Output the pixel matrix with decrypted value = I
Step 7: Apply inverse PAP to remove see the original video frames

3.2 2D Wavelet Transform for Compression and Decompression

The 2D DWT is used mainly for denoising, image compression, etc. It provides superior features than existing DCT, KLT and FFT, since the DWT divides the images into different sub-bands in terms of time and frequency domain. This helps to attain higher compression ratio and eliminates the blockiness artifacts during image rendering process.

The 2D DWT is treated to be a chain of decomposition levels that is evaluated through the application of 1D DWT over an image in both horizontal and vertical directions at each levels. From the Figure 2, it is seen that the input signal is sent to two different filter stages for analysis. Initially, it is computed using a low-pass horizontal filter and then with a high pass horizontal filter. Finally, it is down-sampled by the factor of 2. This helps to obtain the one dimensional output i.e. 1L and 1H. Similarly, 1L and 1H computed using a low-pass vertical filter and then with a high pass vertical filter. Finally, it is down-sampled by the factor of 2. This helps to obtain the four 2D sub-bands, which includes 1HH, 1HL, 1LH and 1LL. This provides the information of original image pixel values. Again if the 2D DWT is applied on any one of the four 2D sub-bands, the image obtains four other new sub-bands, which includes 2HH, 2HL, 2LH and 2LL. The process continues until the entire image sub-band sequence is decomposed into n-levels.

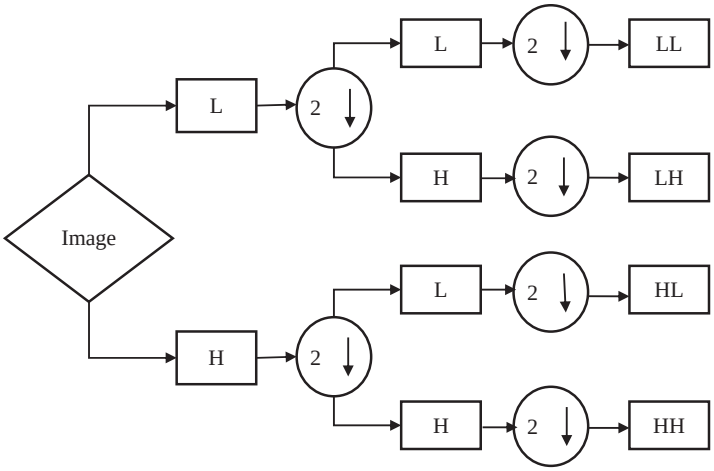


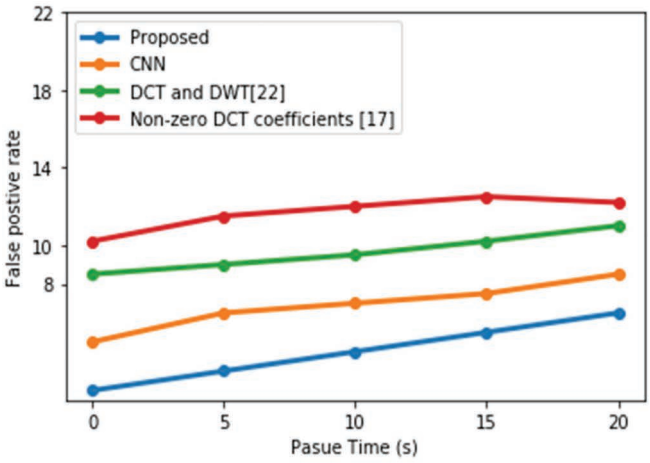
Figure 2 2D DWT decomposition.

4 Experimental Results and Discussions

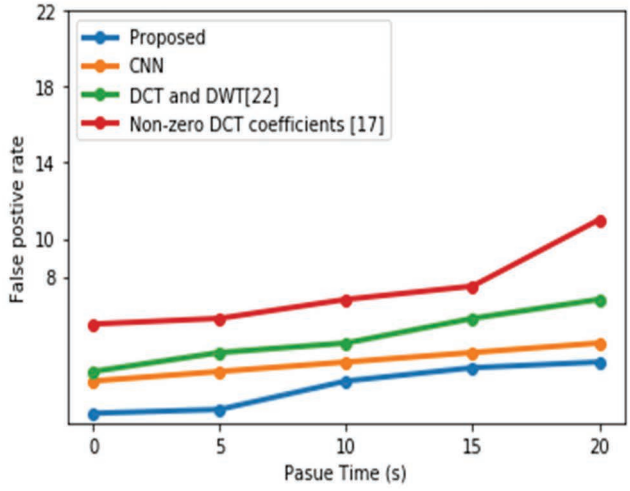
This section presents the results of video encryption system for multimedia video surveillance with different performance metrics. The performance of encryption with compression and decryption with decompression using the proposed method is evaluated against an existing method. The performance of compression and encryption is tested based on the execution of H.264 JM 10.2 in AVC mode. The experimental setup uses eight different benchmark videos for the analysis. This includes Bus, City and Tempete videos of CIF format and Ice, Foreman, Mobile, Salesman and Soccer videos of QCIF format. These videos represent various combinations like camera motion (Bus and City videos), still background (foreman and salesman videos), complex texture (Tempete and Mobile videos) and fast motion (Soccer and Ice videos).

The Figure 3(a) provides the results of false positive rate between proposed detection and conventional lightweight and cryptographic model. The proposed and conventional system is tested between 0 and 20 pause time. The simulation scenario is set as follows: the total Malware nodes in the simulation scenario is eight and it is made fixed, and eight other Malware nodes are made dynamic.

The Figure 3(b) provides the results of false positive drop rate between proposed model with CA and conventional malware detection systems. The proposed and conventional system is tested between 0 and 20 pause time. The simulation scenario is set as follows: the total malware nodes in the



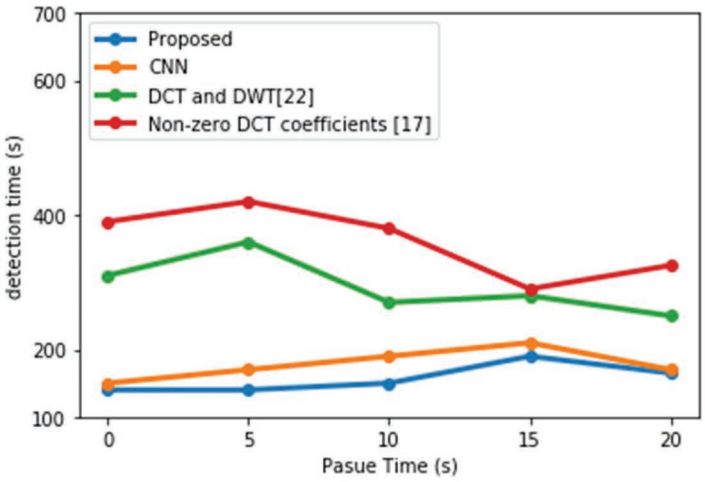
(a) 50 malwares is introduced in the system



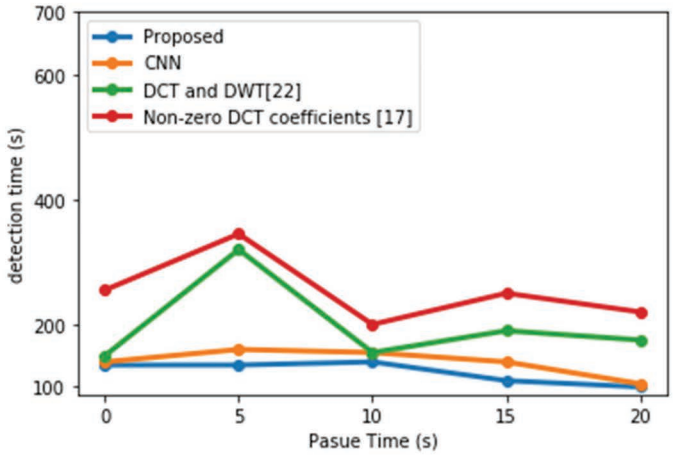
(b) 20 malwares is introduced in the system

Figure 3 False positive rate.

simulation scenario is two and it is made fixed, and two other malware nodes are made dynamic. Finally, it is found that proposed system acquires reduced Malware detection time than conventional model with Malware nodes in the simulation scenario.



(a) 50 malwares is introduced in the system



(b) 50 malwares is introduced in the system

Figure 4 Malware detection time.

The Figure 4(a) provides the results of total packet drop rate between proposed Compression and PAP-CAE and conventional malware detection system. The proposed and conventional system is tested between 0 and 20 pause time. The simulation scenario is set as follows: the total malware nodes

in the simulation scenario is two and it is made fixed, and two other malware nodes are made dynamic.

The Figure 4(a) provides the results of total packet drop rate between proposed Compression and PAP-CAE and conventional malware detection system. The proposed and conventional system is tested between 0 and 20 pause time. The simulation scenario is set as follows: the total malware nodes in the simulation scenario is eight and it is made fixed, and eight other malware nodes are made dynamic. Finally, it is found that proposed system acquires reduced malware detection time than conventional model with 20 malware nodes in the simulation scenario.

The result shows that the use of Cellular Automata Encryption increases the encryption in multimedia video streams than other methods. It is seen that if performs marginally better than the other methods. Hence, the proposed method intends to use improved encryption technique in future to increase the robustness of the encryption in multimedia video frames.

5 Conclusions and Future Scope

In this paper, we present a multimedia security framework to secure the data traversed across mobile, internet and cloud access against the malware attacks. The framework applies pseudo arbitrary permutation on pixel and lines over video frames at initial instant. It then encrypts the video frames using Cellular Automata Encryption System. The encrypted video frames are then combined to acquire high security. Finally, the malwares are reduced using 2D wavelet transform by compressing the complex files to reduce the file size for effective transmission across distributed systems. The experimental result shows that the proposed method is effective against existing methods in terms of higher detection accuracy, reduced detection time and false positive rate. In future, the study tends to be extended with deep learning strategies to possibly encrypt the video frames and pseudo arbitrary permutation.

References

[1] Langelaar, G., Setyawan, I., and Lagendijk, R. (2000). Watermarking of digital image and video data – A state of art review. *IEEE Signal Process. Mag.*, 20–46.

[2] Rahman, S. M. (2001). Design and management of multimedia information systems: Opportunities and challenges. *IGI Global*.

[3] Yahalom, R., Steren, A., Nameri, Y., Roytman, M., Porgador, A., and Elovici, Y. (2019). Improving the effectiveness of intrusion detection systems for hierarchical data. *Knowledge-Based Systems*, 168, 59–69.

[4] Lian, S., Kanellopoulos, D., and Ruffo, G. (2009). Recent advances in multimedia information system security. *Informatica*, 33(1).

[5] Aljawarneh, S. and Yassein, M. B. (2017). A resource-efficient encryption algorithm for multimedia big data. *Multimedia Tools and Applications*, 76(21), 22703–22724.

[6] Aljawarneh, S. and Yassein, M. B. (2018). A multithreaded programming approach for multimedia big data: Encryption system. *Multimedia Tools and Applications*, 1–20.

[7] Li, C., Lin, D., and Lü, J. (2017). Cryptanalyzing an image-scrambling encryption algorithm of pixel bits. *IEEE MultiMedia*, 24(3), 64–71.

[8] Li, C. (2016). Cracking a hierarchical chaotic image encryption algorithm based on permutation. *Signal Processing*, 118, 203–210.

[9] Ye, G. and Huang, X. (2018). Spatial image encryption algorithm based on chaotic map and pixel frequency. *Science China Information Sciences*, 61(5), 058104.

[10] Peng, F., Gong, X. Q., Long, M., and Sun, X. M. (2017). A selective encryption scheme for protecting H. 264/AVC video in multimedia social network. *Multimedia Tools and Applications*, 76(3), 3235–3253.

[11] Wang, X., Liu, C., Xu, D., and Liu, C. (2016). Image encryption scheme using chaos and simulated annealing algorithm. *Nonlinear Dynamics*, 84(3), 1417–1429.

[12] Wolfram, S. (2018). *Cellular Automata and Complexity: Collected Papers*. CRC Press.

[13] Zhang, X., Seo, S. H., and Wang, C. (2018). A Lightweight Encryption Method for Privacy Protection in Surveillance Videos. *IEEE Access*, 6, 18074–18087.

[14] Clarke, K. C. (2018). Cellular automata and agent-based models. *Handbook of Regional Science*, 1–16.

[15] Jeong, J., Kwon, S., Hong, M. P., Kwak, J., and Shon, T. (2019). Adversarial attack-based security vulnerability verification using deep learning library for multimedia video surveillance. *Multimedia Tools and Applications*, 1–15.

[16] Xiao, C., Wang, L., Zhu, M., and Wang, W. (2016). A resource-efficient multimedia encryption scheme for embedded video sensing system based on unmanned aircraft. *Journal of Network and Computer Applications*, 59, 117–125.

[17] Peng, F., Gong, X. Q., Long, M., and Sun, X. M. (2017). A selective encryption scheme for protecting H. 264/AVC video in multimedia social network. *Multimedia Tools and Applications*, 76(3), 3235–3253.

[18] Thanki, R., Dwivedi, V., and Borisagar, K. (2017). A hybrid watermarking scheme with CS theory for security of multimedia data. Journal of King Saud University-Computer and Information Sciences.

[19] Xiao, C., Wang, L., Jie, Z., and Chen, T. (2016). A multi-level intelligent selective encryption control model for multimedia big data security in sensing system with resource constraints. In 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud) (pp. 148–153). IEEE.

[20] Thiyagarajan, K., Lu, R., El-Sankary, K., and Zhu, H. (2019). Energy-Aware Encryption for Securing Video Transmission in Internet of Multimedia Things. *IEEE Transactions on Circuits and Systems for Video Technology*, 29(3), 610–624.

[21] Alsmirat, M. A., Obaidat, I., Jararweh, Y., and Al-Saleh, M. (2017). A security framework for cloud-based video surveillance system. *Multimedia Tools and Applications*, 76(21), 22787–22802.

[22] Joshi, A. M., Gupta, S., Girdhar, M., Agarwal, P., and Sarker, R. (2017). Combined DWT–DCT-based video watermarking algorithm using Arnold transform technique. In Proceedings of the International Conference on Data Engineering and Communication Technology (pp. 455–463). Springer, Singapore.

Biography

S. Velliangiri obtained his Bachelor's in Computer Science and Engineering from Anna University, Chennai. Master's in Computer Science and Engineering from Karpagam University, Coimbatore and Doctor of Philosophy in Information and Communication Engineering from Anna University, Chennai. He is working as an Associate Professor in CMR Institute of Technology, Hyderabad, Telangana. He is a member of Institute of Electrical and Electronics Engineers (IEEE) and International Association of Engineers (IAENG). He is specialized in Network security and Optimization techniques. He has published twenty five International journals and presented ten International conferences. He has authored and co-author of several books. He served as Area Editor in EAI Endorsed journal of Energy Web (Scopus) and Journal of computer science Bentham (Scopus).He was the reviewer of IET Communication, Elseiver, Taylor and Francis, Springer, Inderscience and other reputed scopus indexed journals.