BLOCKCHAIN ENABLED DUAL LEVEL SECURITY SCHEME WITH SPIRAL SHUFFLING AND HASHING TECHNIQUE FOR SECRET VIDEO TRANSMISSION

Dr. PL. Chithra (1), R. Aparna (2)*

(1) Professor, University of Madras, Chennai; (2) Research Scholar (UNOM) & Assistant Professor, M.O.P. Vaishnav College, Chennai
India

* Corresponding Author: e-mail: chitrasp2001@gmail.com

Abstract: In the modern digital era, data is considered to be the most valuable asset. Multimedia data includes audio, image and video forms which grabs attention and vulnerable for hacking. Transmission of multimedia data in open network is always unsecure. In this research paper, a novel method to transmit secret video is proposed. First, keyframes are detected by processing the ROI (region of interest) to classify segments. Spiral Shuffling and SHA512 hashing technique are applied to build the cipher blocks. Blockchain technique enhances strength of the Dual Level (Crypto-Stegano) Security Scheme. Discrete cosine transformation with normalization is applied to embed cipher blocks in audio files without any traces of hidden data. Combining the major security techniques such as Cryptography, Steganography and Blockchain enhances the strength of the proposed BDLSS (Blockchain enabled Dual Level Security Scheme). Experimental analysis is carried out with PSNR, SSIM, MSE, NPCR and Correlation coefficient values to prove the efficiency and the proposed method outperforms well over existing methods.

Key words: blockchain, spiral shuffling, hashing, cryptography, steganography, DCT.

1. INTRODUCTION

Sending secret data is always essential in many situations. Multimedia data instantly attracts hackers. The proposed BDLSS is focuses on securely sending secret videos in the unsafe open network. Keyframes are identified for creating the block boundary. The keyframe of a video is normally defined as the frame that contain the action changing key. There are many features to find the keyframe in a video [1]. Here, many such features like Structured Similarity Index Measure (SSIM), entropy, threshold and histogram are considered. Since, many calculations

are involved, it is difficult and time consuming if calculated for the whole image frames of the secret video. Thus, region of interest (ROI) is fixed by calculating the Mean Square Error (MSE) and the variations in the features are calculated for ROI to identify the keyframes. Based on the keyframes in the video, several blocks are formed. Cipher blocks are obtained by applying spiral shuffling and discrete cosine transformation on each block. Image encryption techniques should be strong enough to protect the secret data from the hackers [2,3]. Hiding the secret data in an audio file without any traces of hidden video frames leads to an efficient steganographic technique. Crypto and Stegano schemes are incorporated in the video blocks leads to the efficient Blockchain enabled DLSS.

Standard measures such as correlation coefficients, SNR, PSNR, SSIM and MSE are calculated to portray the efficiency of the proposed BDLSS method. Correlations coefficients are used to show the vast difference between the original and cipher images and the similarity of audio files before and after embedding. Comparative study is done with existing methods and the proposed method outperforms well.

The motivation for this research work is the need for secret video to be communicated in defence sector. Evidence video has to be safeguarded. Thus, a strong secure method is required for accomplishing it. In this research paper, an efficient scheme is proposed to send covet video as cipher blocks hidden in a typical audio file. The combination of crypto and stegano enhances strength to the proposed Blockchain enabled Dual Level Security Scheme (BDLSS).

The remaining part of this paper is organized as follows: Background work or Literature survey is given in Section 2 under the heading Related Works. Proposed Methodology is elaborated in Section 3. Section 4 presents the Blockchain enabled Dual Level Security Scheme. Experimental Results and Performance Analysis are shown in Section 5. Finally, Section 6 concludes this paper.

2. RELATED WORKS

Sending secret data in private network are highly safe and secure. But it is impossible to depend on creating private network always, as it is not cost effective and the data needs to be transmitted across many devices. Thus, communicating with encrypted data [1-3] improves security. Multimedia data such as image, video and audio are sent as ciphers in open network. Video encryption techniques with AES and ECC [4] holds high strength. Video files are huge and sent as many smaller files. Splitting the video file into smaller blocks [2] are based on the keyframes produces better results. Keyframe identification [1,5] is performed based on numerous features of each video frame images. Embedding the secret data in a multimedia data adds security. Hiding image in an audio file [6] is shown by Tohari Ahmad et al. and embedding secret audio in another cover audio is proposed in our previous work [7]. As the multimedia data are huge and very vulnerable, the amount of data hidden in a cover file is an important measure to

prove the efficiency of the system. Zhiguo Qu et al. elaborated a novel video Steganography protocol [8] with large payload. Blockchain technology is establishing its strength in various fields including video forensics [8], deepfake technologies and IoT [9-11].

Machine learning and deep learning are the latest artificial intelligence (AI) techniques applied in keyframe identification in human action videos [12] of various fields such as sports training [13] videos. Sharing secret data is the reason for the improvement in mobile communications. Sharing secret data in mobile applications by the creation of multiple secure storage dimensions [14] is explained by Mercan, S. et al. and in cloud computing for various mobile devices [15] is clearly described by Lu.X et al. Bhat et al. shown the role of probabilistic public key encryption in secure cloud storage [16]. All these existing methods are the inspiration for the proposing this research work with improved performance.

3. PROPOSED METHODOLOGY

The proposed methodology incorporates three major techniques and are explained as follows:

3.1. Cryptography

1. Read secret video
2. Find the total number of frames in the secret video
3. Keyframe detection
   - 3.1. Calculate the mean squared error (MSE) between each frame
   - 3.2. Identify the region of interest (ROI)
   - 3.3. Calculate structured similarity index measure (SSIM), entropy between ROI on the consecutive frames
   - 3.4. Perform histogram analysis

4. Build the blocks
5. Perform 3X3 spiral shuffling for each frame in the blocks
6. Build Blockchain
7. Apply discrete cosine transformation

3.2. Blockchain

1. Generate hash with SHA512 hashing technique
2. Link cipher blocks

3.3. Steganography

1. Read the cover audio files
2. Normalize the cipher block
3. Embed each cipher block in various audio files
4. Send the files in random order

4. BLOCKCHAIN ENABLED DUAL LEVEL SECURITY SCHEME

In this research work, Blockchain enabled Dual Level Security Scheme (BDLSS) is proposed to enhance security while using open unsecure network for data transmission.

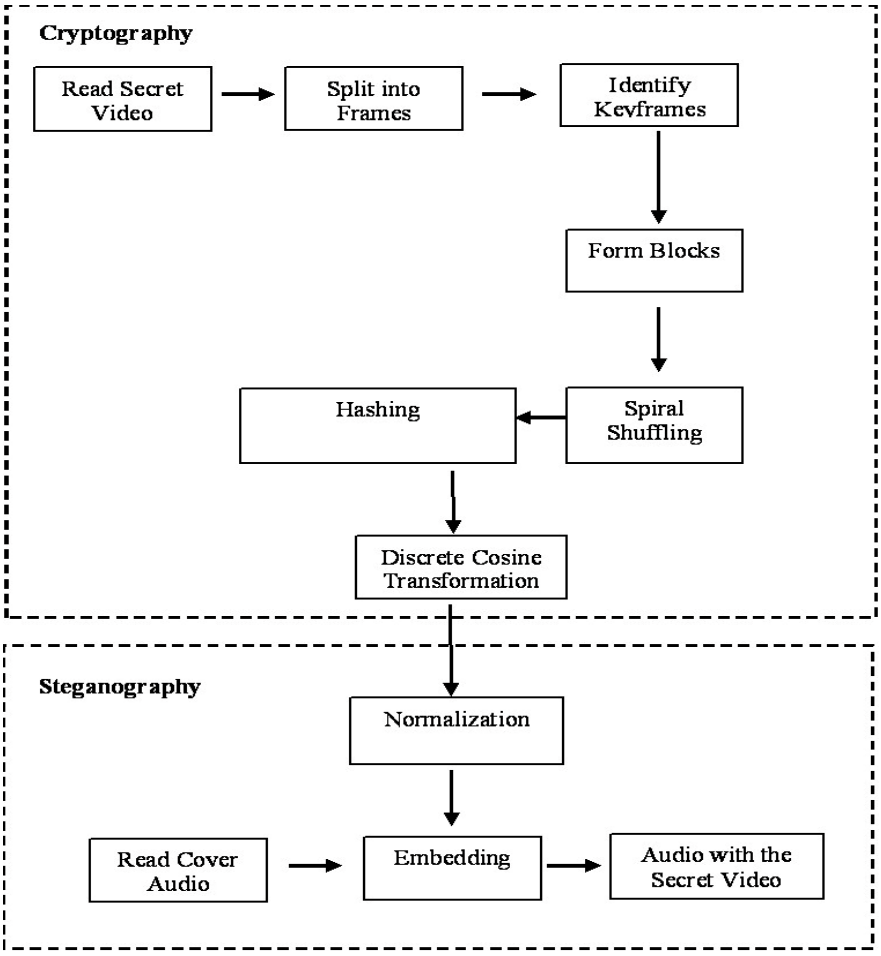

Figure 1. Proposed Blockchain enabled Dual Level Security Scheme (BDLSS)

Cryptography and steganography are the two pillars of secure transmission. Blockchain concept imparted in the dual level security scheme improves extra reign to the method. Sending the cipher blocks embedded in random audio files without any traces of hidden secret data gives strong protection. Figure 1 shows the Blockchain enabled DLSS. Identifying keyframe is the initial step in BDLSS and its algorithm is given below. SSIM, entropy, histogram difference of ROI among

the frames are calculated for keyframe extraction. SSIM & entropy values should be fixed according to the videos used. Here, SSIM between the frames lesser than 0.99 and entropy difference greater than 0.05 is chosen for the secret traffic video.

Algorithm for Keyframe Extraction

1. *Read the video*
2. *Find N the number of Keyframes*
3. *Identify ROI*
    1. *Set i=1 , then F_i=first frame*
    2. *Select three candidate regions R_1, R_2, R_3 on the first frame F_i*
    3. *Calculate the MSE score between the candidate regions*
    4. *Choose the largest MSE score region as ROI*
4. *Keyframe Extraction*
    1. *While (i <=N)*
    2. *For all consecutive frame pairs F_i & F_{i+1}*
    3. *Calculate SSIM, Entropy, Hist_Difference and Standard Deviation*

If (SSIM < 0.99 && Entropy >0.05 && hist-diff > std_deviation)

Add in Keyframe list K[ ]

Else

Add in Non- Keyframe list NK[ ]

End

5. *Keyframes K[ ] identified*

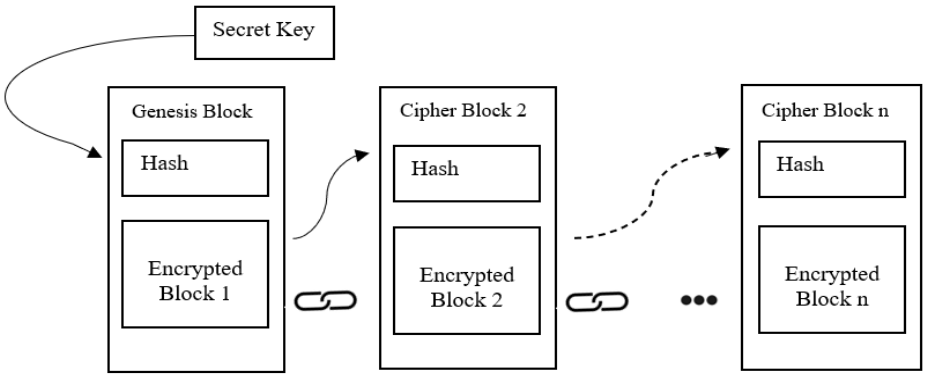

Figure 2. Formation of Blockchain

Including the Blockchain concept to the Crypto-Stegano (DLSS) improves the efficiency of the proposed work. Secret key is known by the sender and receiver. SHA 512 algorithm is used for generating the genesis hash for the secret key. Each block has the previous hash and the encrypted block. Hence, the hash is the link between the cipher blocks. Figure 2 depicts the Blockchain formation. The strong hashing technique makes the proposed method to overcome the risk of deepfake [9]

mechanisms. Since the all the cipher blocks are independent, they can be embedded in different conventional audio files and sent in random order. As the cipher blocks are sent hidden in various audio files, missing any of the blocks will not support the decryption process. And hence the secrecy is maintained. Each cipherblock is applied with discrete cosine transformation (DCT) prior to embedding. Normalization factor [7] is derived from the short-term energy calculation of the audio signal. Normalized cipherblock is hidden in the audio file without leaving any traces of the secret data. Any audio file can be used to hide the cipherblock. The only constraint for choosing the audio file is, it has to be lengthier enough to hold the secret cipherblock.

5. EXPERIMENTAL ANALYSIS AND PERFORMANCE ANALYSIS

Secret video and the cover audio files are digitalized in the pre-processing step for keyframe extraction [1,2]. On digitalization, cover audio generates 1D scalar dataset and the secret video generates 2D or 3D vector dataset. Hence, it is the major constraint for embedding the vast secret data in audio file. The Blockchain concept provides solution for this problem. The cipher block is converted into 1D scalar dataset and embedded in the normal audio file. Spiral shuffling generates the confusion matrix, for which the DCT is applied in sender's side and Inverse DCT in receiver's end supports in the retrieval of original secret data. Those calculations are given in the equations (1,2).

$$dct(u,v) = \alpha(u)\alpha(v) + \sum_{y=0}^{N-1} \sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2x+1)v}{2N}\right] \quad (1)$$

for $u,v = 0,1,2\ldots\ldots..N\text{-}1$

$$f(x,y) = + \sum_{y=0}^{N-1} \sum_{y=0}^{N-1} \alpha(u)\alpha(v)dct(u,v)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2x+1)v}{2N}\right] \quad (2)$$

where, *N* is the data sequence

$$\alpha(u) = \begin{cases} \sqrt{\frac{1}{N}} & for\ u = 0 \\ \sqrt{\frac{1}{N}} & for\ u \neq 0 \end{cases} \quad \& \quad \alpha(v) = \begin{cases} \sqrt{\frac{1}{N}} & for\ v = 0 \\ \sqrt{\frac{2}{N}} & for\ v \neq 0 \end{cases}$$

5.1. Cryptanalysis

Peak Signal to Noise Ratio (PSNR), Correlation coefficients, and Structural Similarity Index Measure (SSIM) calculation are, given in equations (3-5), used to perform cryptanalysis by comparing the differences between the original secret image and the encrypted image.

$$PSNR = 10\, log_{10}\left(\frac{max^2}{MSE}\right) \tag{3}$$

$$r_{xy} = \frac{\sigma_{xy}}{\sqrt{\sigma_x^2 \sigma_y^2}} \tag{4}$$

where x and y are the two datasets for which the cross-correlation (r) is calculated.

$$SSIM(D,S) = \frac{(2\mu_x\mu_y + P_1)(2\sigma_{xy} + P_2}{(\mu_x^2 + \mu_y^2 + P_1)(\sigma_x^2 + \sigma_y^2 + P_2)} \tag{5}$$

Various videos such as a sample Traffic video, standard Akiyo video and a Cartoon video are considered for our experimental analysis, as shown in the Table 1, to prove that the proposed method is applicable for any type of videos.

Table 1. Keyframe Analysis

Video	***Video Name***	***Information bits***	***Resolution***	***No. of frames***	***No. of Keyframes***
Video1	*Traffic*	*1434 KB*	*360 X 270*	*322*	*10*
Video2	*Akiyo*	*460 KB*	*264 X 352*	*300*	*8*
Video3	*Cartoon*	*805 KB*	*1920 X 1440*	*311*	*8*

Table 2 depicts the cryptanalysis to prove that the proposed method successfully resists differential attacks. For each of the cipherblocks in the sample traffic video, the experiment is carried out by calculating the Structured Similarity Index(SSIM), Correlation Coefficients and Peak-Signal-Noise Ratio(PSNR) and the results obtained are tabulated in the Table 3.

Table 2. Cryptanalysis

Video	***No. of Frames***	***Frame Aspect Ratio***	***SSIM***	***Correlation Coefficients***	***PSNR***
Video1	*322*	*360 X 270*	*-1.3545e-03*	*-0.00022*	*-44.0899*
Video2	*300*	*264 X 352*	*-2.9545e-04*	*-0.00028*	*-47.0632*
Video3	*311*	*1920 X 1440*	*-1.6621e-04*	*0.00004*	*-42.9190*

Where *cf1, cf2* are the cipherframes, '*n*' is the number of pixels and used to calculate the NPCR & UACI values. Comparative analysis is carried with existing methods and the results are highlighted in Table 4 & Table 5. Net Pixel Change Rate (NPCR) and. Unified Average Changing Intensity (UACI) [1,11,14] are calculated as per the equations (6-8) and the results are shown in the Table 5 with time complexity and correlation coefficients. The proposed BDLSS shows higher performance rate than the existing methods [1,4,14]. Figure 3 shows the original and cipher keyframe of sample surveillance video and the standard Akiyo video.

The experimental simulation is carried out in MATLAB R2022B with various secret videos and its compatible audio files. As there are no major restrictions in choosing the video & audio files, the proposed BDLSS can be applied in various fields easily. Here, surveillance video, standard Akiyo video and cartoon videos are considered as secret videos and song audio files (eg. 'despacito' song) in mp4 format are used as cover files.

$$NPCR(cf1, cf2) = \sum_{i,j} \frac{c(i,j)}{n} X\ 100\% \tag{6}$$

$$c(i,j) = \begin{cases} 0, & \text{if } (cf1(i,j)\ equals\ \ cf2(i,j) \\ 1, & \text{Otherwise} \end{cases} \tag{7}$$

$$UACI(cf1, cf2) = \sum_{i,j} \frac{cf1(i,j) - cf2(i,j)}{255\ x\ n} X\ 100\ \% \tag{8}$$

Table 3. Cipher block

Video	***Block No.***	***No. of Frames***	***SSIM***	***Correlation Coefficients***	***PSNR***
Traffic Video1	*1*	*25*	*-0.0029*	*-0.00027*	*-44.0899*
	2	*21*	*-0.0018*	*-0.00024*	*-44.0664*
	3	*27*	*-0.0013*	*-0.00037*	*-44.0162*
	4	*33*	*-0.0018*	*-0.00018*	*-44.0387*
	5	*53*	*-0.0026*	*-0.00012*	*-44.0429*
	6	*30*	*-0.0013*	*-0.00046*	*-44.0320*
	7	*35*	*-0.0022*	*0.00002*	*-43.9877*
	8	*25*	*-0.0022*	*-0.00035*	*-44.0375*
	9	*60*	*-0.0071*	*-0.00019*	*-44.0697*
	10	*12*	*-0.0035*	*-0.00044*	*-44.0840*

Table 4. Comparative Analysis 1

#	***Video***	***SSIM***
Proposed Method	*Akiyo*	*0.00078*
Qingqing Han et al. [4]		*0.0012*

Table 5. Comparative Analysis 2

#	***Frame Image Size***	***Speed (ms)***	***Correlation***	***NPCR***	***UACI***
Proposed Method	*[264, 352, 3]*	*504*	*-0.00022*	*99.67*	*33.46*
R. Hamza et.al [1]	*[640, 480, 3]*	*790*	*0.0035*	*99.62*	*33.47*
X. Huang [14]	*[256. 256, 1]*	*547*	*0.0722*	*>99*	*33.43*

Figure 3. Original and Cipher Keyframes

5.2. Steganalysis

Steganalysis is performed to ensure the secret cipher data is hidden effectively in an audio at sender's side and lossless retrieval at the receiver's end. SSIM, PSNR, Correlation, SNR, MSE, histogram analysis is performed as steganalysis and the results are given in the following Table 6.

Table 6. Steganalysis

Audio File	***Video Cipher Block***	***SSIM***	***Correlation Coefficients***	***PSNR***	***SNR***	***MSE***
audio1. wav	*vc1*	*0.9999*	*1.0000*	*57.1329*	*-1.2528e-04*	*1.9351e-06*
audio2. wav	*vc2*	*0.9998*	*1.0000*	*55.4627*	*-1.8328e-04*	*2.8427e-06*
audio3. wav	*vc3*	*0.9998*	*1.0000*	*56.8727*	*-1.3377e-04*	*2.0546e-06*

SSIM values are closer to 1, which shows that there is only a minimal difference in the structure of the cover audio even after embedding the secret video

cipherblock. Value for correlation is 1, proves the strength of stegano method proposed. PSNR of the secret image frame obtained in the receiver's end is always >55 shows the competence [6-8]. Mean Square Error (MSE) is the average squared difference between the estimated values and the actual value [8] which is calculated with the following equation (9). Lesser the value better the result. Hence, the proposed BDLSS is efficient.

$$MSE = \frac{1}{m\,x\,n}\sum_{x=1}^{m} - \sum_{y=1}^{n}(D(x,y) - S(x,y))^{2} \quad (9)$$

Thus, the cryptanalysis and steganalysis are performed to show the efficiency of the proposed work. Also, comparative analysis is carried with some of the existing work to highlight BDLSS. Furthermore, in our future work Deep learning, machine learning and CNN [12,13] concepts can be utilized to automize the keyframe detection for reducing the time complexity.

5.3. Significance of BDLSS

a. Integrating the benefits of Blockchain with Crypto-Stegano adds new zest to the proposed methodology.
b. In the proposed BDLSS the cipherblocks are sent in any random order, makes it stronger.
c. SHA512 hashing algorithm is used to produce the 64bit linking key, which connects the randomly sent cipherblocks, in the receiver end.
d. Discrete cosine transformation is performed and then the resultant is dynamically normalized with the short-term energy value of the cover audio to hide the cipherblock without any traces.
e. Any audio signal, including music, songs, conversational audio files, can be selected as cover audio provided it should be equal or lengthier than the cipherblock.
f. Different cover audios can be used to send each cipherblocks, so that the hacker cannot suspect.
g. It is a lossless method; hence the secret video reaches the receiver without any modifications or loss.
h. Many standard measures are calculated and compared to prove the efficacy. Proposed method is incorporated with standard video to state its performance over existing methods.

6. CONCLUSION

This research work addresses the problem of confidentiality. Multimedia data are vulnerable and seeks additional protection than ordinary data, as it attracts intruder easily. Blockchain enabled Crypto-Stegano DLSSM outperforms well and achieves good result in transferring video data in the open network. Correlation coefficients are derived to prove the similarities between original secret video & decrypted video and cover audio signals before & after embedding. SNR, PSNR, SSIM, MSE and histogram measures prove the lossless transmission of secret

video. Experimental results are carried with the surveillance video and standard akiyo video for comparative analysis to prove the performance of proposed Blockchain enabled Dual Level Security Scheme over existing methods.

ACKNOWLEDGEMENT

Sincere thanks to the Department of Computer Science, UNOM and M.O.P. Vaishnav College for the consistent support and motivation for carrying on the research work.

REFERENCES

[1] R. Hamza, K. Muhammad, A. N. and G. RamíRez-GonzáLez, Hash Based Encryption for Keyframes of Diagnostic Hysteroscopy. *IEEE Access*, vol. 6, 2018, pp. 60160-60170, DOI: 10.1109/ACCESS.2017.2762405.

[2] Minjun Zhou, Chunhua Wang, A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks. *Signal Processing*, vol. 171, 2020, 107484, ISSN 0165-1684, DOI: 10.1016/j.sigpro.2020.107484.

[3] X. Huang, Image encryption algorithm using chaotic Chebyshev generator. *Nonlinear Dya*., vol. 67, no. 4, 2012, pp. 2411-2417.

[4] Qingqing Han, Liejun Wang, Yongming Lee, and Jiwei Qin.2020. Video encryption scheme using hybrid encryption technology. *Int. J. Internet Protoc. Technol.* vol.13, no.1 2020, pp. 1–8. DOI: 10.1504/ijipt.2020.105046

[5] Savran Kızıltepe, R., Gan, J.Q. & Escobar, J.J. A novel keyframe extraction method for video classification using deep neural networks. *Neural Computing & Applications*, 2021, DOI: 10.1007/s00521-021-06322-x

[6] Tohari Ahmad, Muhammad Hanif Amrizal, Waskitho Wibisono, Royyana Muslim Ijtihadie, Hiding data in audio files: A smoothing-based approach to improve the quality of the stego audio. *Heliyon*, vol. 6, no.3, 2020, DOI: 10.1016/j.heliyon.2020.e03464.

[7] Chithra, Pl., and R. Aparna. "Voice Signal Encryption Scheme Using Transformation and Embedding Techniques for Enhanced Security." *2018 IEEE, 2nd International Conference on Imaging, Signal Processing and Communication (ICISPC)*, 2018, pp. 149–54, DOI: 10.1109/ICISPC44900.2018.9006681.

[8] Qu, Z., Chen, S. & Ji, S. A Novel Quantum Video Steganography Protocol with Large Payload Based on MCQI Quantum Video. *International Journal of Theoretical Physics*, vol.56, pp. 3543–3561, 2017, DOI: 10.1007/s10773-017-3519-z.

[9] Mercan, Suat & Cebe, Mumin & Aygun, Ramazan & Akkaya, Kemal & Toussaint, Elijah & Danko, Dominik., Blockchain-based video forensics and integrity

verification framework for wireless Internet-of-Things devices. *Security and Privacy,* vol. 4, no.2, 2021, DOI: 10.1002/spy2.143.

[10 Thorat, Chandrama; Inamdar, Vandana; Jadhav, Bhagvat, TED: A Lightweight Block Cipher for IoT Devices With Side-Channel Attack Resistance. *International Journal on Information Technologies & Security*, vol. 12, no. 2, p83-96, 2020.

[11] Khan, P.W.; Byun, Y. A Blockchain-Based Secure Image Encryption Scheme for the Industrial Internet of Things. *Entropy*, vol.22, no.2,175, 2020, DOI: 10.3390/e22020175.

[12] Gawande, Ujwalla, et al. Deep Learning Approach to Key Frame Detection in Human Action Videos. *Recent Trends in Computational Intelligence*, 2020, DOI: 10.5772/intechopen.91188.

[13] Lv, C., Li, J., & Tian, J. Key frame extraction for sports training based on improved deep learning. *Scientific Programming*, 2021, pp.1-8.

[14] Glet, Michał; Kaczyński, Kamil, Secret Sharing Scheme for Creating Multiple Secure Storage Dimensions for Mobile Applications. *International Journal on Information Technologies & Security*. vol. 12, no. 4, 2020, p83-102.

[15] Lu, X., Pan, Z. & Xian, H. An efficient and secure data sharing scheme for mobile devices in cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications (JoCCASA)*, vol. 9, no. 60, 2020, DOI: 10.1186/s13677-020-00207-5.

[16] Bhat, R., Sunitha, N.R. & Iyengar, S.S. A probabilistic public key encryption switching scheme for secure cloud storage. *International Journal of Information Technology*, 2022, DOI: 10.1007/s41870-022-01084-8

Information about the authors:

Dr. PL. Chithra is working as a Professor in the Department of Computer Science, University of Madras. The main areas of research include 3D Digital Image Processing, Pattern Recognition, Artificial Intelligence, Signal Processing, Network Security, and Video Processing. She is passionate about teaching, imparting, training, motivating and helping young minds with knowledge and discipline. She has 30 years of teaching and 20 years of research experience in Computer Science.

Aparna R. is a research scholar in the Department of Computer Science, University of Madras and working as Assistant Professor in the Department of Information Technology at M.O.P. Vaishnav College, Chennai. Her areas of research interest are Signal & Image Processing. She has presented and published papers in National and International conferences and journals.

Manuscript received on 12 December 2022
Revised version resubmitted on 07 February 2023