

Enhanced Visual Degradation Deep Learning Method for Video Encryption and Decryption

¹ V Jayabharathi, ² Dr. S. Sukumaran

¹ Ph.D., Research Scholar, ² Associate Professor

¹vjayabharathimca@gmail.com, ²prof_suumar@yahoo.com

^{1,2} Department of Computer Science

Erode Arts and Science College (Autonomous), Erode-638009, Tamilnadu, India

DOI: <https://doi.org/10.63001/tbs.2024.v19.i02.S2.pp158-162>

KEYWORDS

Cryptographic,
Video Encryption,
Advance Encryption
Standard,
Enhanced Visual
Degradation,
Digital Security.

Received on:

10-07-2024

Accepted on:

19-10-2024

ABSTRACT

Numerous businesses have developed proprietary or selective encryption techniques for communication and data collection. Because online fraud and cyber theft are on the rise, protecting sensitive data is becoming more and more important. Visual cryptography is a widely used cryptographic technique that involves concealing visual data, such as text, images, videos, and audio, so that only authorized groups with full access to the encrypted data can decrypt it and reveal the original content either collectively or individually. Conduct a number of security tests, including information entropy, mean square error, temporal complexity, histograms, number of pixel change ratio, peak signal-to-noise ratios, and many more, in order to assess the security and resilience of these suggested methods. The study examines video encryption and encoding approaches and uses a variety of assessment metrics to demonstrate that propose method is effective for video encrypting and decrypting.

INTRODUCTION

The wide usage of digital images as well as videos in various applications brings serious attention to security as well as privacy issues today. These days, security and privacy concerns are receiving a lot of attention due to the widespread usage of digital photos and videos in several applications. Data encryption is a useful technique for safeguarding data. Many encryption methods (such as DES, RSA, IDEA, and AES) have been suggested and implemented up to this point; the majority of these are utilized for text and binary data. Since video data are frequently big quantities and demand real-time activities, it is challenging to employ them directly in video encryption. Over the last ten years, a number of video encryption methods have been documented, the majority of them rely on the MPEG ½ codec [2] [3].

Video has emerged as the most common information carrier in visualized communication due to advancements in network technology and the accessibility of multimedia apps. Approximately 80% of data traffic is made up of video, according to statistics. As a result, the military, education, medical, and other areas have all made extensive use of video communication due to its effectiveness and security.

A lot of real-time apps employ video encryption. Although there are many video encryption techniques available today, there are still challenges in the research domain related to time and space complexity, real-time latency, scalability, and vulnerability to a few attacks. Few algorithms have achieved an acceptable computational complexity, though, and in these cases, vulnerability to specific attacks (such as differential, statistical, plain text, and

cipher text attacks) still poses a threat to secure video transmission.

To the best of our knowledge, scientific researchers require a thorough but meticulous methodical video encryption. A fast-paced sequence of still photos, referred to as frames, is played back to create a video, also known as moving pictures. Since the internet is an unsafe medium, it is getting easier and easier to intercept and steal sensitive information (text, photographs, audio, video, etc.) that is being conveyed over it [3,4]. Because sensitive information is frequently contained in multimedia files, its security is crucial. Digital signatures, authentication, and encryption have been used as security mechanisms for data transfer over the internet. Videos may be encrypted using a number of cryptographic algorithms, such as the Advance Encryption Standard (AES), RC4, Simplified Data Encryption Standard (SDES), and Modified, Modified Advance Encryption Standard (MAES), etc.

II. RELATED WORK

AvnishKanungo et al. [3] discuss a wide range of key generation techniques, from using cellular automata and chaotic systems as pseudo-random number generators to using different encryption algorithms (like AES, DES, Rabbit, RSA, Motion Vector, and others) to protect transmitted and stored data. The methodology of the research publications under consideration makes extensive use of the methodologies, key generation procedures, and encryption algorithms discussed above. The study's most compelling topic is how we classified the assessment parameters according to our own criteria and how the technical and practical aspects of the reviewed articles are connected.

The original and encrypted video frames, as well as the original and decrypted video frames, were compared using SSIM by El-Shafai et al. [7]. A total of six distinct videos had their metrics captured. The SSIM values for the encrypted video frame range from 0.0019 to 0.0059, which is quite near to the amount that is advised for adequate distortion. For each of the six videos, the SSIM results between the original and the decrypted versions were 1, indicating a flawless reconstruction of the video.

An encryption model with two chaotic systems is used by Kordov and Dimitrov [16] to generate cipher keys in a pseudo-random manner. The suggested technique was applied to five videos, and each video's correlation coefficient was determined. Every encrypted file had values extremely near to zero, suggesting good encryption as it suggests there is no correlation between the values of neighboring pixels.

Karmakar et al. [14] employed skewness to gauge the algorithm's security and utilized hyper chaos and DNA coding for video encryption. Three distinct films were used to test the encryption method on a single original frame, with skewness ranging from -0.2 to +0.2. The original video frame's skewness varied significantly. Following encryption, the skewness variation falls within the range of 0.2 to -0.3, making the security test passable.

Using maps and the Ikeda time delay system, Valli and Ganesan [22] employed a chaos-based video encryption technique. The two plain video frames, P and Q, encrypted with the same key are used to test the suggested strategy. The associated cipher frames are designated as P1 and Q1. XORing P and P1 results in the creation of mask frame M. Valli and Ganesan[24] attempted to recover Q by performing an XOR operation on M and Q1 with the aid of this mask frame. Using the Ikeda DDE and the 12D chaotic map, this is determined to be ineffective.

The entire key space of the proposed encryption technique is about $=1.23794003928538 \times 10^{38}$, which is big enough to withstand an exhaustive search. Waseem& Khan et al. [23] employed a quantum video encryption algorithm based on qubit-planes controlled-XOR operations and enhanced logistic map. With a selective encryption strategy, Gautier et al. [8] obtained an EDR value of 0.87, demonstrating the suggested method's capacity to conceal edges and structural information in the encrypted frames. With an encryption technique based on a cross-coupled chaotic cipher, Weng et al. [25] were able to obtain an EDR value of 0.96, indicating a very little amount of edge information in the cipher text.

The issue of time is addressed by Kelur et al. [15] and Alattar et al. [1]. While Alattar et al. [1] devised a solution by employing I macroblock, Kelur et al. [15] present a way where the size of the original picture is decreased. This is because encrypting each additional I-macroblock takes approximately half the processing time of encrypting all I-macroblocks. The underlying issue of 2D CA mask-based encoding techniques is solved by Li et al. [18].

III. PROPOSED METHODOLOGY

The practice of concealing or encoding data so that only the intended recipient may read it is known as cryptography. Message encoding has been done using cryptography for thousands of years. It is still employed today in e-commerce, bank cards, and computer passwords.

The practice of digitally safeguarding your recordings to avoid unauthorized viewing and interception is known as video encryption. To secure your sensitive digital assets, the technique of video protection entails encrypting videos using specialized software and hardware configuration. Encryption is the process of utilizing an encryption to change plaintext information or a message into ciphertext, a challenging, unintelligible form.

3.1 METHODOLOGY PROPOSED BY MEYER AND GADEGAST

For MPEG videos, this technique is suggested [15]. This technique encrypts the MPEG video stream using the well-known RSA or DES encryption algorithms in CBC mode. It employs four security tiers. (i) Every stream header is encrypted. (ii) Encrypting all stream headers, as well as the intracoded blocks' lower AC and DC coefficients. (iii) Encrypting all I-blocks in P- and B-frames as well as I-frames. (iv) Every bit stream is encrypted. The sequence in which I blocks appear in P or B frames can match that of I blocks in I frames. This significantly lowers the selective encryption scheme's

efficiency [16]. The parameters that are encrypted determine the encryption ratio that can be used.

The encryption ratio is quite low when only headers are encrypted. However, the encryption ratio is 100% when all bit streams are encrypted. Once more, the speed of this technology varies according to the quantity of encrypted parameters and the typical algorithms used, like RSA or DES.

Algorithm of Enhanced Visual Degradation using Deep Learning Method for Video Encryption and Decryption

<i>Video encryption is accomplished by the use of a modified deformation technique</i>	
Step 1:	<i>vid = (f1, ..., fn) // a series of frames chan // a value (0-2) for the RGB channel Frames K1 is the first key. K2 is the second key</i>
Step 2:	<i>Extract the video frames. V = I1, I2, AVERAGE-ROWS(vid, chan) return Avg-Rows-And-Frames (vid, chan, 'rows')</i>
Step 3:	<i>frame[r][c][chan] signal1 [index1] = sum2 / (nCols * nRows) index2++ Using the key generation technique, generate K1</i>
Step 4:	<i>Starting with frame I2, execute C2 is an abbreviation for imageProcess (I2, K2) D2 is an abbreviation for bitxor (C2, I1) E2 is an abbreviation for video Process (D2, K1)</i>
Step 5:	<i>(frame in video) do nRows = length(frame), sum2 = 0 Repeat the preceding steps for all of the frames.</i>
Step 6:	<i>Combine all of the frames to create an encrypted video.</i>
<i>Decrypted frames from encrypted video. E = E1, E2, ...En</i>	
Step 8:	<i>Using the key generation technique, generate K1 For each E2 frame D2 = Video Process (E2, K1) C2 is an abbreviation for bitxor (D2, I1) Ax = Video Process (C2, K2) AVERAGE-FRAMES(vid, chan) return Avg-Rows-And-Frames (vid, chan, 'cols')</i>
Step 9:	<i>AVG-ROWS-AND-FRAMES(vid, chan, fl) signal1 = {}, index1 = 0, signal2 = {},</i>
Step 10:	<i>index2 = 0 Repeat the preceding steps for all of the frames</i>
Step 11:	<i>for (frame in video) do nRows = length(frame), sum2 = 0 for (r = 0; r < nRows; r++) do nCols = length(frame[r]), sum1 = 0 signal2 [index2] = sum2 / (nCols * nRows) index2++ if (fl == 'rows') then return signal1 Combine all of the frames to create a decrypted video.</i>
Step 12:	<i>for (c = 0; c < nCols; c++) do sum1 += frame[r][c][chan] sum2 += frame[r][c][chan] signal1 [index1] = sum1 / nCols index1++</i>

Numerous security levels can be achieved. Merely encrypting the stream headers is inadequate because this part may be easily seen. Encrypting each bit stream, however, might result in very high security. For this method, there is no proven thorough cryptanalysis. An specialized encoder and decoder are required in order to read an unencrypted SECMPG stream. The recommended encoder is incompatible with MPEG.

Assume that cryptographic operations are being carried out by a target device. The device's user can start the cryptographic operations by, for example, initiating a TLS session to browse an HTTPS website or by using a VPN, an attacker can start the cryptographic operations by sending the device messages intended to activate automatic digital signature. We presume that the target device has a power LED or is linked to another device or peripheral (such as speakers or a USB hub) that has a power LED; the target devices power LED or the connected peripheral is one of the following sorts of LEDs: (1) A regular LED with on/off power.

This is the power LED kind that is most frequently integrated into gadgets. In this instance, the LED only produces light when the

gadget is turned on, and its color remains unchanged. The LED's brightness varies very little depending on the amount of electricity used, but these variations are invisible to the naked eye. (2) An LED for power indication. Smart card readers frequently use this kind of power LED, which changes color in response to cryptographic procedures that are triggered.

3.2 PROPOSED METHOD OF ENHANCED VIDEO DECRYPTION AND ENCRYPTION

The two main kinds of video encryption algorithms are naïve and selective. All of the data, including frames and parameters, that make up a video stream are encrypted using a technique called "naïve encryption". This kind of encryption is very time- and space-consuming, requiring a lot of processing power. The advantage of this is that all relevant data has been encrypted, thus depending on the techniques used, the level of security is rather high. Nevertheless, the same level of security may also be reached if certain frames or informational fragments are encrypted; here is where selective encryption comes into play for movies [8].

Encoding helps decrease the total size of the video file while also accelerating the transmission process. Software that carries out the tasks of encoding (at the source) and decoding (at the receiver) is called a video codec. The video data is decompressed and viewable in its original format when it reaches the decoder at the receiving end. The video codec of the encoder provides the data as a bit stream after compressing it into a common format.

3.3 Dataset

Video Acquisition: For obtaining video footage, we examine two distinct models depending on the type of power LED. One of the steps in the pre-encoding encryption techniques is frame-based encryption, which divides the actual video stream into separate frames and applies encryption to the selected video frames. Mathematical changes based on diffusion, confusion, or both processes are used to alter the images.

Close video acquisition:

Using the smartphone camera, the attacker captures the footage. We believe that there is a device or connected peripheral that leaks data since the power LED in this case matches the cryptographic protocols. We also suppose that the attacker can enter into the room where the target device is housed and record video of the power LED on the victim device. (or the associated peripheral) using a smartphone while the target device is doing cryptographic operations.

Over the Internet video acquisition:

Fractional Fourier Transform and the input signal is rotated by any angle into the necessary phase as part of the transform space domains using the 2D-Fractional Fourier Transform, which is a linear transformation. It is thought of as a simplified version of the conventional Fourier Transform (FT) method. The Fractional Fourier Transform is employed in the recommended video cryptography approaches because it is widely used in the field of optics, namely in optical statistics and signal processing applications. As a result, it is essential in the field of image and video encryption and decryption.

SVD (Singular Value Decomposition):

Three matrices (U, S, and V) are produced by the singular value decomposition of a matrix X of size $m \times n$. S is a diagonal matrix with values known as "the singular values," whereas U and V are orthogonal matrices of size $m \times m$ [5]. The SVD equation is displayed in the equation below:

$$U \times S \times V^t = X \text{ (Include variables)}$$

The S matrix's diagonal values represent the most important values, which are taken into account for additional encryption and processing in order to hide data.

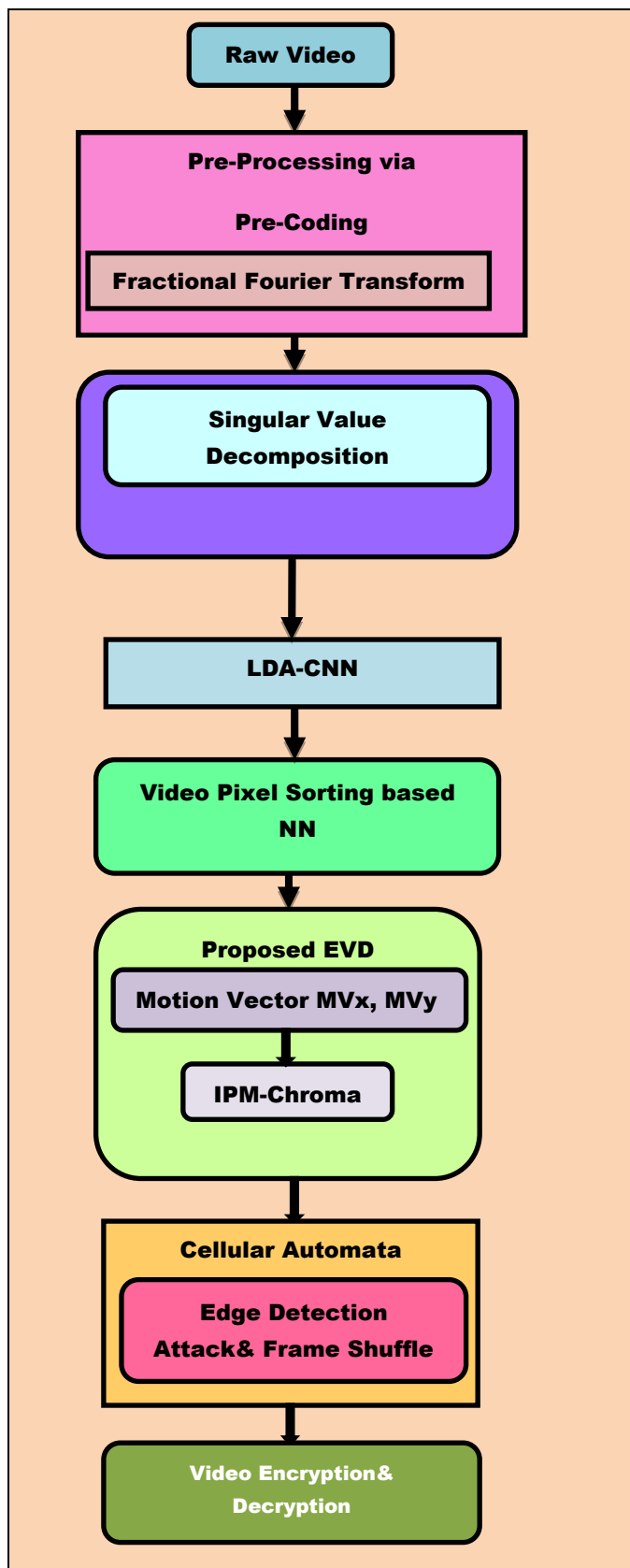


Fig.1.1 Flow Diagram of EVD-DLM

Linear Discriminant Analysis (LDA) and Convolutional Neural Network (CNN):

The following are the approach's two main parts. Linear Discriminant Analysis (LDA) is used in the first phase for frame-level

video labelling. LDA is used to find a projection that maximizes the distance between distinct action movies and reduces the distance between the same action films after two CNNs have extracted spatial and temporal information.

Motion Vector (MVx, MVy):

HEVC defines a signed 16-bit range for both horizontal and vertical motion vectors, or along the X and Y axis; these are referred to as the MVx and MVy vectors. It is a two-dimensional vector used for inter-prediction that provides an offset between the coordinates in the decoded frame and the reference frame of a video.

Cellular automata

A cellular automaton is a discrete model made up of a neighborhood specification for every cell in an arbitrary-sized regular grid with a finite number of states. Certain principles control how these cells interact and transform into the next generation (state). Most of the rules are mathematical functions or calculable that depend on the state of the cell and its environment at any given moment. Here, a pseudorandom number generator is used to produce keys for the encryption process utilizing cellular automata.

Assumedly, the attacker gains access to the video camera using its API, enabling them to record, enlarge, and focus on the target device's power LED and any related peripherals before sending the content to themselves via the Internet. In this video acquisition model, we further assume that the device contains an indicative power LED and that the color fluctuations in the device's power LED induced by cryptographic processes may be observed from a distance.

IV. RESULTS AND DISCUSSIONS

By altering an original video frame and then encrypting both the original and modified original video frames using the same encryption technique, an attacker might speculate about information about the video frame. The adversary looks for correlations between the two encrypted frames and the plain frame by comparing them. As a result, for each little alteration made to the original, the encryption system ought to produce a new encrypted frame. For this purpose, the measures UACI (Unified Average Changing Intensity) and NPCR (Number of Pixels Change Rate) are utilized to assess algorithm performance. The metrics' mathematical computations are as follows:

$$NPCR = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N D(i, j) \times 100 (\%)$$

$$D(i, j) = \begin{cases} 0 & \text{if } C_1(i, j) = C_2(i, j); \\ 1 & \text{if } C_1(i, j) \neq C_2(i, j); \end{cases}$$

$$UACI = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N \frac{|C_1(i, j) - C_2(i, j)|}{255} \times 100 (\%)$$

where the encrypted video frames (plain and modified video frames) are represented by C1 and C2. One pixel from the original video frame is altered to create the modified frame. The video frame sizes are M and N.

Fusion of video and multi-method assessment:

A perceived quality score for a video sequence may be predicted using VMAF, a perceptual video quality metric. Number of zero indicates a very low perceived video quality, while a score of 100 indicates a high perceptual video quality. The range of VMAF values is 0 to 100. Employed a selective encryption method and VMAF to assess the encrypted video's quality [10]. The proposed method resulted in a notable decline in the perceived quality of the video. The VMAF score for encrypted frames from various video classes was recorded using five different QPs. QP 17 had the lowest average score of 9.32, while QP 32 had the highest average score of 10.66.

Table 1.1 Flow Diagram of EVD-DLM

Algorithms	NPCR	UACI	FSIM	VMAF
AES	93.45	93.61	92.91	92.28
RSA	91.41	91.71	91.81	93.43

MPEG	93.85	93.14	93.26	92.58
EVD	95.67	95.27	94.43	95.56

In Table 1.1 describes the enhanced visual degradation using deep learning method for video encryption compared with existing methods like AES, RSA MPEG with the video metrics are NPCR, UACI,FSIM,VMAF.

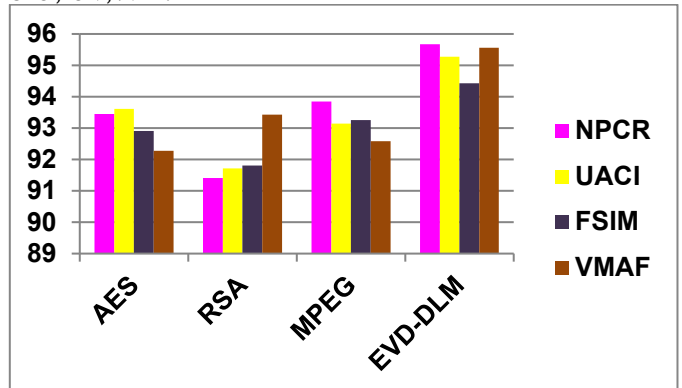


Fig 1.2 Evaluation of EVD-DLM

The performance of Enhanced Visual Degradation using Deep Learning Method for Video Encryption is described in Fig.1.2 NPCR, UACI,FSIM,VMAF metrics. While comparing the existing methods the proposed enhanced visual degradation is gives better result when encrypt and decrypt the video.

CONCLUSION

The many video encryption methods may be divided into two main categories. The first involves dividing the video data into its most crucial parts using hardware-based methods, mathematical transformations, or traditional encoding techniques. Assessing the effectiveness of these various methods is crucial since it enables the practitioner to assess the approach taken and whether or not best outcomes were attained. In order to help practitioners choose which encryption approaches would be most appropriate for their particular set of needs, our study attempts to offer guidance. The discussion of performance metrics creates the foundation for them to assess the effectiveness of their approach, and the bifurcation of the techniques can assist them in analysing their use case and choosing a procedure that satisfies their pass criteria for optimum encryption. The study thoroughly discusses several assessment criteria to validate the current approaches, as well as ways for video encryption and encoding. When compared to current methods for encrypting and decrypting videos, the suggested solution performs better.



REFERENCES

- Alattar AM, Al-Regib GI, Al-Semari SA. Improved selective encryption techniques for secure transmission of MPEG video bit-streams. In: Proceedings 1999 International Conference on Image Processing (Cat. 99CH36348); 24-28 October 1999; Kobe, Japan. pp. 256-260.
- Alhassan S, Iddrisu MM, Daabo MI. Perceptual video encryption using orthogonal matrix. International Journal of Computer Mathematics: Computer Systems Theory 2019; 4(3-4): 129-139. doi: 10.1080/23799927.2019.1645210.
- AvnishKanungo, AyushiSrivastava, SaniyaAnklesaria, PrathameshChur, "A systematic review on video encryption algorithms: A future research", Journal of Autonomous Intelligence (2023) Volume 6 Issue 2 doi: 10.32629/jai.v6i2.665.
- Benrhouma O, Alkhodre AB, AlZahrani A, et al. Using singular value decomposition and chaotic maps for selective encryption of video feeds in smart traffic management. Applied Sciences 2022; 12(8): 3917. doi: 10.3390/app12083917
- Dr.S.Brindha, Dr.S.Sukumaran, Dr.S.Ravichandran, "Effective Taxonomy of Advanced Mobile Edge Computing of Long-Term

- Dr.S.Brindha,Dr.S.Sukumaran,Dr.S.Ravichandran, “Deployment Liabilities of Deep Learning Based on 5G Mobile Applications Using Advanced Mobile Edge Computing Taxonomy”, International Journal Of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume 9, Issue 11, Pp: 567-571,UGC Approved Journal No: 49023(18), 30thNovember 2021.
- El-Shafai W, Almomani IM, Alkhayer A. Optical bit-plane-based 3D-JST cryptography algorithm with cascaded 2D-FrFT encryption for efficient and secure HEVC communication. IEEE Access 2021; 9: 35004-35026. doi: 10.1109/ACCESS.2021.3062403.
- Gautier G, FarajAllah M, Hamidouche W, et al. Selective encryption of the versatile video coding standard. IEEE Access 2021; 10: 21821-21835. doi: 10.48550/ARXIV.2103.04203.
- Go K, Lee I-G, Kang S, Kim M. Secure video transmission framework for battery-powered video devices. IEEE Transactions on Dependable and Secure Computing 2022; 19(1): 275-287. doi: 10.1109/TDSC.2020.2980256.
- Hassan HE-R, Tahoun M, ElTaweel G. A robust computational DRM framework for protecting multimedia contents using AES and ECC.
- Kordov K, Dimitrov G. A new symmetric digital video encryption model. Cybernetics and Information Technologies 2021; 21(1): 50-61. doi: 10.2478/cait-2021-0004.
- Lee MK, Jang ES. Start code-based encryption and decryption framework for HEVC. IEEE Access 2020; 8: 202910-202918. doi: 10.1109/ACCESS.2020.3036023.
- Li H, Gu Z, Deng L, et al. A fine-grained video encryption service based on the cloud-fog-local architecture for public and private videos. Sensors 2019; 19(24): 5366. doi: 10.3390/s19245366.
- Li X, Xiao D, Wang QH. Error-free holographic frames encryption with CA pixel-permutation encoding algorithm. Optics and Lasers in Engineering 2018; 100: 200-207. doi: 10.1016/j.optlaseng.2017.08.018.
- Long M, Peng F, Li H. Separable reversible data hiding and encryption for HEVC video. Journal of Real-Time Image Processing 2018; 14(1): 171-182. doi: 10.1007/s11554-017-0727-y.
- Peng F, Zhang X, Lin ZX, Long M. A tunable selective encryption scheme for H.265/HEVC based on chroma IPM and coefficient

- Haridas D, Kiran DS, Patel S, et al. Real-Time compressed video encryption: Based on quasigroup on System on Chip (SOC). SN Computer Science 2021; 2(5): 408. doi: 10.1007/s42979-021-00793-4.
- Huang M, Yang C, Li H, Shen J. Sparse selective encryption for HEVC 4K video using spatial error spread. Journal of Internet Technology 2019; 20(5): 1589-1600.
- Huang Q, Zhao X, Li G. Research on the application of video encryption technology based on 7 dimensional CNN hyper chaos. In: 2018 10th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA); 10-11 February 2018; Changsha, China. pp. 448-451.
- Karmakar J, Pathak A, Nandi D, Mandal MK. Sparse representation based compressive video encryption using hyper-chaos and DNA coding. Digital Signal Processing 2021; 117: 103143. doi: 10.1016/j.dsp.2021.103143.
- Kelur S, HS RK, K R. Selective area encryption using machine learning technique. In: 2019 Innovations in Power and Advanced Computing Technologies (i-PACT); 22-23 March 2019; Vellore, India. pp. 1-7.
- scrambling. IEEE Transactions on Circuits and Systems for Video Technology 2020; 30(8): 2765-2780. doi: 10.1109/TCSVT.2019.2924910.
- Valli D, Ganesan K. Chaos based video encryption using maps and Ikeda time delay system. The European Physical Journal Plus 2017; 132(12): 542. doi: 10.1140/epjp/i2017-11819-7.
- Waseem HM, Khan M. A new approach to digital content privacy using quantum spin and finite-state machine. Applied Physics B 2019; 125(2): 27. doi: 10.1007/s00340-019-7142-y.
- Wen H, Ma L, Liu L, et al. High-quality restoration image encryption using DCT frequency-domain compression coding and chaos. Scientific Reports 2022; 12(1): 16523. doi: 10.1038/s41598-022-20145-3.
- Wen H, Liu Z, Lai H, et al. Secure DNA-coding image optical communication using non-degenerate hyperchaos and dynamic secret-key. Mathematics 2022; 10(17): 3180. doi: 10.3390/math10173180.

BIOGRAPHIES OF AUTHORS

	<p>V. Jayabharathi was born in Erode, Tamil Nadu (TN), India, in 1990. She received the Bachelor of Computer Science (B.Sc.) degree from the Bharathiar University, Erode, TN, India, in 2010 and the Master of Computer Applications (M.C.A.) degree from the University of Madras, Chennai, TN, India, in 2013. She also received the M.Phil degree from the Bharathiar University, Coimbatore, in 2014. She is pursuing Ph.D degree in computer science at Bharathiar University. Her research interests include Cryptography.</p>
	<p>Dr. S. Sukumaran graduated in 1985 with a degree in Science. He obtained his Master Degree in Science and M.Phil in Computer Science from the Bharathiar University. He received the Ph.D degree in Computer Science from the Bharathiar University. He has 35 years of teaching experience starting from Lecturer to Associate Professor. At present he is working as Associate Professor of Computer Science in Erode Arts and Science College, Erode, Tamilnadu. He has guided for more than 55 M.Phil research Scholars in various fields and guided 20 Ph.D Scholars. Currently he is Guiding 2 Ph.D Scholars. He is member of Board studies of various Autonomous Colleges and Universities. He published around 80 research papers in national and international journals and conferences. His current research interests include Image processing, Network Security and Data Mining.</p>