https://afrjcict.net

A Comparative Study of Video Cryptographic Algorithms and the Performance Metrics used in the Literature to Measure the Algorithms

Adetokunbo Abayomi Adenowo[1*] and Latifat Folake Oderinu[2]

[1,2]Department of Electronic and Computer Engineering,
Lagos State University, Lagos,
Nigeria.
Email: [1]adetokyom@yahoo.com, [2]lateefahoderinu@gmail.com

[*]Corresponding Author: Adetokunbo A. Adenowo (Email: adetokyom@yahoo.com)

ABSTRACT

The pervasiveness of internet and low-cost mobile computing devices has made video communication the preferred option for several information archival and transmission in recent times. However, this growth has come with issues such as security and privacy. Restricting unauthorized access measure can be adopted to protect multimedia information, but does not guarantee the integrity and security of information. A better and more secure cryptography-based approach is required. Cryptography is the art of keeping data in a secure form to prevent unauthorized attackers or to encrypt the information by scrambling its contents, such as image, audio, video; to make it invisible or unintelligible during storage or transfer. Thus, a systematic literature review (SLR) was carried out to determine various video encryption algorithms/techniques (VEA) proposed in previous literature and the performance metrics measured by the authors within the last ten years. This study reveals that the percentage of VEA techniques authors adopted are 17% Naïve/Full encryption, 9% Permutation-based encryption, 51% Selective Encryption(most-adopted), 17% Perceptual Encryption and 6% Hybrid encryption(least-adopted). Furthermore, two or more performance metrics are measured by authors of various proposed VEA and their percentages are 93% Cryptography Security (most-measured metrics), 71% Encryption/Decryption ratio, 51% Format-Compliance, 71% Encryption/Decryption Time, 61% Perceptual Security/Visual Degradation, 53% Mean Square Error (MSE), 53% Peak Signal to Noise Ratio (PSNR) and 27% Structural Similarity Index Measure (SSIM) (least-measured metrics)

Keywords: Cryptography, Encryption Performance Metrics, Peak-Signal-to-Noise-Ratio, Structural Similarity, Systematic Literature Review, Video Encryption Algorithm

African Journal of Computing & ICT Reference Format:

Adetokunbo Abayomi Adenowo and Latifat Folake Oderinu (2020),
A Comparative Study of Video Cryptographic Algorithms and
the Performance Metrics used in the Literature to Measure the
Algorithms. *Afr. J. Comp. & ICT, Vol. 13, No. 4, pp. 43– 61.*

© Afr. J. Comp. & ICT, December 2020; P-ISSN 2006-1781

I. INTRODUCTION

The geometric growth in the generation and use of digital videos is massive and undetermined. The pervasiveness of internet and low-cost mobile computing devices has made video communication the preferred option for several information archival and transmission in recent times. However, this growth has come with issues such as security and privacy. There has been an increase in unauthorized access, piracy, hacking and other digital attack every year. Some multimedia contents (consists of text, image, audio, and video), especially video applied in entertainment, politics, economics, militaries, industries or education, etc., are necessary to be protected by providing confidentiality, integrity, and ownership or identity. Restricting unauthorized access measure can be adopted to protect multimedia information, but does not guarantee the physical security of information.

Thus, cryptography which is a better and more secure approach is required. Cryptography involves encryption (encoding) and decryption (decoding) of information. It is the art and science of safe-guarding information from undesirable people by converting it into a different form difficult to recognize by its attackers during storage and transmission The main goal of cryptography is keeping data secure from unauthorized attackers or to encrypt the information by scrambling its contents (such as text, image, audio, and video). This aim to make the contents unreadable, unintelligible or invisible during storage or transmission [1].

In view of the foregoing, this paper shall explore studies on video encryption during the year 2010 to 2020. The objectives of this paper shall be to: (i) determine existing video encryption techniques adopted by authors; and (ii) identify performance metrics used for video encryption algorithms in the literatures

II. RELATED WORKS

2.1 Video Encryption Techniques

Several video encryption techniques have been proposed in past studies by modifying the standard cryptography algorithms as shown in Figure 1 below, due to complex nature of videos (see [8-9], [25-26], [29], [57], and [74]). However, proposed techniques in the literature can be categorized based on naïve algorithms [91], selective algorithms [92], permutation algorithms [47], perceptual algorithm [7] [23], among others.

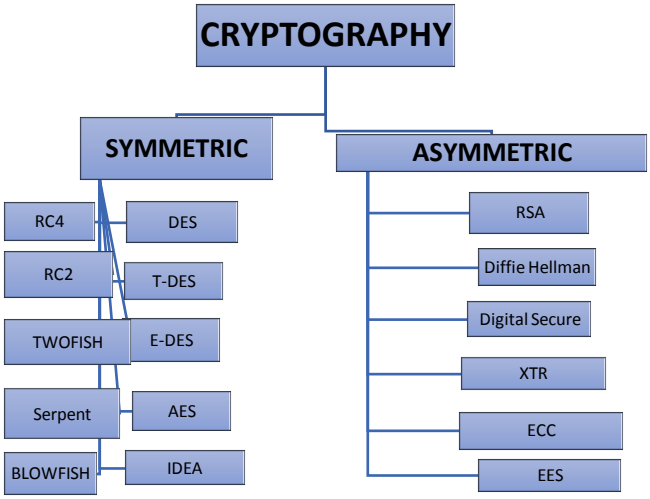

Figure 1: Standard Cryptography Algorithms

In the literature, some authors, such as in [5], [19], [22],[25], [40], [42], [44], [59] and [77], adopted the traditional naïve/full encryption algorithm to encrypt entire video in blocks and streams. Similarly, in [13], [59] and [60], the authors divided the video encryption process into layers or stages and encrypt different frames of the video at each layer. Matta et al. [91], as a specific instance, proposed a naïve security model that aims to secure data, both at storage and in-transit, within an IOT system. The work attempts to address data privacy and ownership in an IOT, such that data cannot be accessed by any eavesdropper/hacker without the consent of the owner. Generally, naive technique has been considered to have highest cryptography security, but associated with highest encryption/decryption ratio (computational complexity) which makes it not suitable for real-time applications.

Selective encryption technique involves the encryption of some parts or segments of the video, such as intra prediction mode, motion vector difference, sign bit of discrete cosine coefficients, residue data, I-frames, P-frames B-frames, quantization coefficients. Archival records show that the technique was adopted in several works, including [10], [14], [17-18], [20-21], [27-29], [33-34], [41], [43], [45], [48-49], [52-53], [56], [58], [62], [64], [66],[68-70], [74] and [80-82]. In Altaf et al. [92], a selective encryption technique (a modified advanced encryption standard (AES) technique) was proposed to address computational burden associated with insecurity, format non-compliance and compression inefficiency that are usually experienced when securing large videos. The work integrated chaotic-based substitution

boxes (S-boxes) of block cipher with AES and AVC (i.e. advanced video channel, also known as H.264). The latter authors claimed that the result of the proposed security algorithm shows a reduction in computation accompanied with increased security, compliance with video format, as well as recorded efficient video compression. However, selective encryption is considered to have lower cryptography security and computational complexity when compared to naïve technique. Notwithstanding, it is the most suitable for real-time applications and devices with low resources.

Furthermore, authors in [7], [9], [15-16], [23], [31], [35-36], [47], [50], [71-72], [73], and [89] adopted perceptual encryption techniques; it results in low-quality and visually degraded version of the video. The operations they performed on the video are: sign-flipping, rotation matrix and flipping; and controlling with a control factor. On the other hand, authors in [8], [12], [26], [55] and [58] adopted permutation-based techniques to encrypt video by using either a permutation list at random or shuffling of the video blocks. For instance, Sultana and Shubhangi [57] proposed an efficient computational and secure video algorithms that takes into consideration the large data size and time-constraints of video-based applications. The latter authors ensured the feasibility of encryption for real-time applications without incurring heavy computational overhead. They also utilized block shuffling technique to reduce key management.

However, some authors combine the techniques stated earlier to arrive at hybrid encryption. In [23], both full and perceptual encryptions were carried out on the video. Selective encryption and shuffle permutation were adopted in [47]. While in [31], the authors combined two different standard encryption algorithms which are AES (symmetric) and Elliptic Curve Cryptography (ECC) (asymmetric) to encrypt the video. Similarly, Mamvong et al. [93] deployed a fast and secure hybrid cryptosystem based on matrix encryption (symmetric) and Elgamal algorithm (asymmetric).

2.2 Video Encryption Performance Metrics

A number of metrics have been mentioned in the literature to evaluate cryptography algorithms. These metrics include the cryptography security, computational complexity, peak signal to noise ratio (PSNR), structural similarity index (SSIM), mean square error, to mention a few (see section 3.4.2 for more). However, cryptography security which indicates the level of difficulty an attacker will encounter to decrypt a video, is the most important and considered metric to measure the performance of an encryption algorithm, as measured in several works including: [7-10], [12-30], [32-34], [36-45], [47-52], [54], [56-57], [59-60], [62], [64-65], [68-72], [74], [77-78], and [80-85]. Another metric of importance, is the computational complexity (i.e. the encryption/decryption ratio).

III. METHODOLOGY

The research method used to review and select articles was systematic literature review (SLR). A systematic review method is important in the context of this study because it aims to find, as much as possible, research relevant to the particular research questions (RQs); then, use appropriate methods to deduce reliable conclusions based on the results of the studies. SLR is used to provide a complete and fair evaluation of the state of all relevant research works available on the specific topic of interest as propounded by [2].

In keeping with a methodological outline, this review followed the suggestions proposed in "Preferred Reporting Items for Systematic Reviews and Meta-Analyses" (PRISMA) [3] for creating a review protocol stage. Systematic Literature Review (SLR) is described as an activity to identify, specify, and analyze all researches or publications in a specific area to present the answer to each research question (RQ). The study proposed by [4] provides accounts on the original guideline to conduct the structure of this SLR.

3.1 Research Questions

With this review focus, as earlier identified, the research questions addressed herein are:

RQ1. What are the standard digital video formats?

RQ2. What are the techniques used for video encryption algorithm?

RQ3. What are the performance metrics for video encryption algorithms?

3.2. Identification of Relevant Literature

Previous studies on digital video encryption algorithms are retrieved and reviewed. Research papers are selected based on inclusion and exclusion criteria. Literature was searched through Google Scholar Database. Journal articles, books, reports and conference papers published between 2010 and 2020 related to the video encryption are included in this review. In order to reduce bias and to expand the quantity of articles sources, a pre-defined strategy such as PRISMA

flow chart [4] is employed to identify potential primary studies; it is described as shown in Figure 2 below.

The following search query was eventually used:

((“Cryptography” **OR** “Video Encryption” **OR** “Encryption technique”) **AND** (“MPEG” **OR** “H.26x” **OR** “AVC” **OR** “HEVC”) **AND** (“Format Compliant” OR “Fast encryption” OR “ Perceptual Encryption”)).

3.2.1 Inclusion and exclusion criteria

This study includes: papers that present empirical data related to the protection of video through cryptography; and papers containing information on video encryption. Such papers may be survey or peer reviewed works that are published in either journals or conference proceedings.

This study excludes papers that: are not written in English language; focus on economic, business or legal impacts of video encryption; and grey literature such as blogs and government documents.

Mendeley (http://mendeley.com), a web and desktop application, is used to manage and store the search results. The selected list of studies from the first stage has consisted of 400 full-text primary publications. There are 85 primary research after the exclusion of studies

3.3 Quality Assessment

Quality assessment rules was set to measure the degree of relevancy of the contents of a research article in relation to the review. The rules are:

Rule 1: Articles have video encryption techniques
Rule 2: Includes articles related to MPEG/H.26x , AVC or HEVC video
Rule 3: Articles discusses performance metrics of Video encyption algorithms
Rule 4: Articles with proposed video encryption algorithm.

The criteria for rating the quality of an article based on the rules are presented in Table 1 while the articles and their quality based on the quality assessment criteria is presented in table 2 below.

Table 1: Quality Assessment Criteria

Criteria	**Quality**
If article obeys only 1	Low
If article obeys only (1 AND 2)	Medium
If article obeys only (1 AND 2 AND 3)	High
If article obeys only (1 AND 2 AND 3 AND 4)	Very High

3.4 Literature Classification

Various research articles and journals are classified in order to provide answers and analyze the research questions. A narrative synthesis method is used where the data is reconstructed in such a way that is relevant to answer the the research questions.

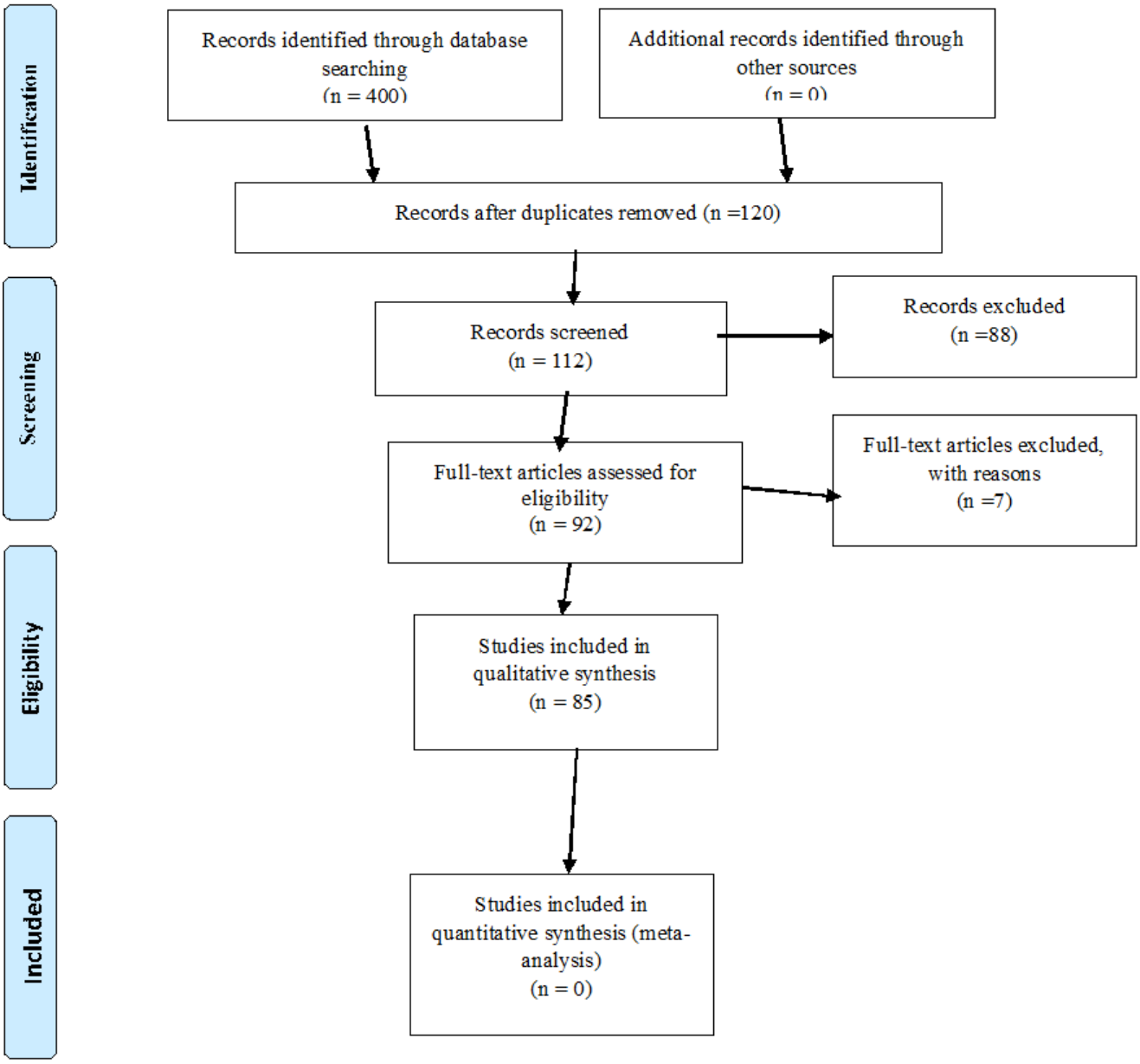

Figure 2: PRISMA Flowchart: Adapted for Video Encryption Algorithm [4]

Table 2: Articles for Review and their Quality Assessment

	Title of Articles	Quality Assessment
1	A Comprehensive Survey of Video Encryption Algorithm [88]	Very High
2	A fast selective video encryption algorithm by selecting data randomly [38]	Very High
3	A New Approach for Video Encryption Based on Modified AES Algorithm [8]	Very High
4	A new design of multiple transforms for perceptual video encryption [9]	High
5	A new perceptual assessment methodology for selective HEVC video encryption [85]	Very High
6	A new selective video encryption algorithm for the H.264 standard [67]	Very High
7	A novel idea of video encryption using hybrid cryptographic techniques [31]	Very High
8	A scalable frame scrambling algorithm for video encryption [51]	Very High
9	A Secure Video Encryption Technique Using Rijndael Algorithm [25]	Very High
10	A selective encryption scheme for protecting H.264/AVC video in multimedia social network [49]	Very High
11	A selective encryption scheme with multiple security levels for the H.264/AVC video coding standard [56]	Very High
12	A study on multimedia security systems in video encryption [30]	Medium
13	A survey of video encryption algorithms [6]	High
14	A Survey of Video Encryption Algorithms Implemented in Various Stages of Compression [79]	High
15	A Survey on Efficient and Secure Video Encryption Techniques [11]	High
16	A Survey on Video Encryption Techniques [46]	High
17	A Survey Report on Video Encryption and Decryption Techniques [86]	High
18	An analysis and comparison for popular video encryption algorithms [53]	Medium
19	An efficient format compliant video encryption scheme for HEVC bitstream [66]	Very High
20	An efficient scalable video encryption scheme for real time applications [64]	Very High
21	An efficient video encryption scheme for H.264 compressed bitstream [41]	Very High
22	An efficient video encryption scheme in compressed domain for H.264/AVC [81]	Very High
23	An experiment of scalable video security solution using H.264/AVC and advanced encryption standard (AES): Selective cryptography [74]	Very High
24	An improved selective encryption for h.264 video based on intra prediction mode scrambling [33]	Very High
25	An improved video encryption method design [42]	Very High
26	Commutative Encryption and Data Hiding in HEVC Video Compression [68]	Very High
27	Data (Video) Encryption in Mobile devices [44]	Medium
28	Design and implementation of network video encryption system based on STM32 and AES algorithm [59]	Medium
29	Design and Implementation of Video Encryption for Multimedia Applications [12]	High
30	Design of new unitary transforms for perceptual video encryption [71]	High
31	Dual-Layer Video Encryption using RSA Algorithm [13]	Very High
32	Efficient encryption of intra and inter frames in MPEG video [80]	Very High

33	Encryption for high efficiency video coding with video adaptation capabilities [62]	Very High
34	Enhanced Encryption schemes of video for real time applications [61]	Very High
35	Enhancing selective ISMACryp video encryption for real time applications in handheld devices [34]	High
36	Extended Selective Encryption of H.264/AVC (CABAC)-and HEVC-Encoded Video Streams [14]	Very High
37	Fast compression domain video encryption scheme for H.264/AVC streaming [45]	Very High
38	Fast video encryption using the H.264 error propagation property for smart mobile devices [18]	Very High
39	Format-compliant perceptual video encryption based on multiple description coding [35]	Very High
40	Hash key-based video encryption scheme for H.264/AVC [69]	High
41	Highly Secure and Fast Video Encryption Using Minimum Overhead in H.264/AVC Bitstream [37]	Very High
42	ICSECV: An efficient approach of video encryption [10]	Very High
43	Improved perceptual video encryption and decryption using S-transform [36]	High
44	Improved perceptual video encryption using alternative unitary transforms [83]	Very High
45	Improved perceptual video encryption using multiple 8×8 transforms in MPEG-4 [75]	High
46	Joint selective encryption and data embedding technique in HEVC video [58]	Very High
47	Layered video encryption utilizing error propagation in H.264/AVC [60]	Very High
48	Modified AES based algorithm for MPEG video encryption [19]	Very High
49	Motion compensation techniques in permutation-based video encryption [55]	Very High
50	Novel Selective Video Encryption for H.264 Video [82]	Very High
51	Partial Video Encryption Using Random Permutation Based on Modification on Dct Based Transformation [50]	High
52	Perceptual video encryption for multimedia applications [78]	High
53	Perceptual video encryption in multimedia secure communication [16]	High
54	Perceptual video encryption via unit anti-diagonal matrix [7]	Very High
55	Privacy-preserving H.264 video encryption scheme [17]	Very High
56	Proposed Video Encryption Algorithm v/s Other Existing Algorithms: A Comparative Study [5]	High
57	Puzzle - An efficient, compression independent video encryption algorithm [40]	Very High
58	Quality assessment for a perceptual video encryption system [73]	High
59	Real Time Video Encryption for Secure Multimedia Transfer: A Novel Approach [20]	High
60	Real-Time Partial Encryption of Digital Video Using Symmetric Dynamic Dual Keys Algorithm (SDD) [48]	Very High
61	Region of interest based selective encryption scheme for privacy protection in H.264 video [27]	High
62	Research of H.264 video transmission encryption technology based on blowfish algorithm [29]	Very High
63	Robust video encryption and decryption using selective encryption [28]	Low

64	Secure Implementation for Video Streams Based on Fully and Permutation Encryption Techniques [23]	High
65	Secured selective encryption algorithm for MPEG-2 video [52]	Very High
66	Securing compressed video streams using RC4 encryption scheme [26]	Very High
67	Selective encryption algorithm implementation for video call on Skype client [54]	High
68	Separable reversible data hiding and encryption for HEVC video [77]	High
69	Sketch attacks: A note on designing video encryption method in H.264/AVC [43]	High
70	A selective video encryption scheme based on coding characteristics [32]	Very High
71	Smart selective encryption of CAVLC for H.264/AVC video [21]	Very High
72	Study of selective video encryption for the H.264 standard [65]	Low
73	Survey of Video Encryption Algorithms [76]	High
74	The design of video-conference encryption system based on H.264 [70]	Very High
75	The video encryption scheme based on perceptual encryption algorithm in H.264 standards [72]	Very High
76	JLVEA: Light weight real-time video stream encryption algorithm for IOT [39]	Very High
77	Transparent encryption with scalable video communication: Lower-latency, CABAC-based schemes [89]	Very High
78	Video Encryption Algorithm and Key Management using Perfect Shuffle [57]	High
79	Video encryption based on special Huffman coding and rabbit stream cipher [24]	Very High
80	Video Encryption for Secure Multimedia Transmission - A Layered Approach [47]	Very High
81	Video encryption using AES algorithm [22]	Medium
82	Video Encryption: A Survey [87]	High
83	Visual protection of HEVC video by selective encryption of CABAC binstrings [84]	High
84	Visual quality control for perceptual video encryption with multiple transforms [15]	High
85	Visual security evaluation for video encryption [63]	Low

3.4.1 Techniques Used by Video Encryption Algorithms

I. Naïve/Full Encryption: In this method, the entire video is first compressed and is then encrypted using traditional algorithms like RSA, DES, and AES. The major drawbacks of full layered encryption technique are heavy computational cost and very low speed and low video quality; which make it not suitable to be applicable in real time video applications [8].

II. Permutation-based Encryption: This encryption can be carried out only on specific video frames or the complete video. A permutation list may be used as a secret key for encryption using a permutation algorithm. There are pure permutation and Zig-Zag permutation. The pure permutation algorithm is vulnerable to known-plaintext attack while the Zig-Zag permutation is vulnerable to a cipher-text only attack, and a known-plaintext attack [1].

III. Selective Encryption: This technique involves encrypting a selected part/portion of the entire video content, rather than encrypting the complete video. This lowers the encrypting time and improves as much security as possible [87]. It overcomes the drawback of the total or full layered approach by reducing computational complexity of encryption process.

IV. Perceptual Encryption: This technique involves the reduction in the quality of video that can be viewed by encryption i.e., the encrypted video can be partially viewed after encryption due to perceptual degradation. The level of quality/perceptual degradation can be continuously controlled by a factor p, which specifies a percentage corresponding to the encryption [90].

V. Hybrid Encryption: This technique can either combine two standard cryptography algorithms [31] or techniques [23] by exploring their strength.

Techniques of video encryption algorithm used by the researchers under this review is presented in Table 3.

Table 3: Techniques of Video Encryption Algorithms

Techniques of video encryption algorithm (VEA)	Previously proposed video encryption scheme
Naïve/Full Encryption Algorithm	1. A secure Video Encryption Algorithm using AES Rijndael [25]
	2. An improved Video Encryption method design [42]
	3. Data (Video) Encryption in Mobile Devices [44]
	4. Design and implementation of Network Video Encryption System based on STM32 [59]
	5. Dual layer video encryption using RSA [13]
	6. Layered video encryption utilizing error propagation in H.264/AVC [60]
	7. Modified AES based algorithm for MPEG video encryption [19]
	8. Proposed Video Encryption Algorithm v/s Other Existing Algorithms: A Comparative Study [5]
	9. Puzzle - An efficient, compression independent video encryption algorithm [40]
	10. Video encryption based on special Huffman coding and rabbit stream cipher [24]
	11. Separable reversible data hiding and encryption for HEVC video [77]
	12. Video encryption using AES algorithm [22]
Permutation Based Algorithm	1. JLVEA: Light weight real-time video stream encryption algorithm for IOT [39]
	2. A new approach for video encryption based on Modified AES [8]
	3. Design and implementation of Video encryption for multimedia application [12]
	4. Motion compensation techniques in permutation-based video encryption [55]
	5. Securing compressed video streams using RC4 encryption scheme [26]
	6. Video Encryption Algorithm and Key Management using Perfect Shuffle [57]
Selective Encryption Algorithm	1. A fast Selective VEA by selecting data randomly [38]
	2. A new Perceptual Assessment methodology for Selective HEVC video encryption [85]
	3. Scalable Frame scrambling algorithm for video encryption [51]
	4. A selective encryption scheme for protecting H.264/AVC video in multimedia network [49]
	5. Selective encryption with multiple security level for the H.264/AVC video coding standard [56]
	6. An efficient Format compliant video encryption scheme for HEVC bitstream [66]
	7. An efficient scalable video encryption scheme for real time applications [64]
	8. An efficient video encryption scheme for H.264 compressed bitstream [41]
	9. An efficient video encryption scheme in compressed domain for H.264/AVC [81]
	10. An Experiment of Scalable Video security solution using H.264/AVC and AES [74]
	11. An improved selective encryption for h.264 video based on intra prediction mode scrambling [33]
	12. Commutative encryption and data hiding in HEVC video compression [68]
	13. Efficient encryption of intra and inter frames in MPEG video [80]
	14. Research of H.264 video transmission encryption technology based on blowfish algorithm [29]
	15. Encryption for high efficiency video coding with video adaptation [62]
	16. Enhancing selective ISMACryp video encryption for real time applications in hand held devices [34]
	17. Sketch attacks: A note on designing video encryption method in H.264/AVC [43]
	18. Extended selective encryption of H/ H.264/AVC (CABAC) - and HEVC- encoded video

	streams [14]
	19. Fast compression domain video encryption scheme for H.264/AVC streaming [45]
	20. Fast video encryption using the H.264 error propagation property for smart mobile devices [18]
	21. Hash key-based video encryption scheme for H.264/AVC [69]
	22. Highly Secure and Fast Video Encryption Using Minimum Overhead in H.264/AVC Bitstream [37]
	23. ICSECV: An efficient approach of video encryption [10]
	24. Joint selective encryption and data embedding technique in HEVC video [58]
	25. Novel Selective Video Encryption for H.264 Video [82]
	26. Privacy-preserving H.264 video encryption scheme [17]
	27. Real Time Video Encryption for Secure Multimedia Transfer: A Novel Approach [20]
	28. Real-Time Partial Encryption of Digital Video Using Symmetric Dynamic Dual Keys Algorithm (SDD) [48]
	29. Region of interest based selective encryption scheme for privacy protection in H.264 video [27]
	30. Robust video encryption and decryption using selective encryption [28]
	31. Secured selective encryption algorithm for MPEG-2 video [52]
	32. Selective encryption algorithm implementation for video call on Skype client [54]
	33. A selective video encryption scheme based on coding characteristics [32]
	34. Smart selective encryption of CAVLC for H.264/AVC video [21]
	35. The design of video-conference encryption system based on H.264 [70]
	36. Visual protection of HEVC video by selective encryption of CABAC binstrings [84]
Perceptual Encryption Algorithm	1. A new design of multiple transforms for perceptual video encryption [9]
	2. Design of new unitary transforms for perceptual video encryption [71]
	3. Format-compliant perceptual video encryption based on multiple description coding [35]
	4. Improved perceptual video encryption and decryption using S-transform [36]
	5. Improved perceptual video encryption using alternative unitary transforms [83]
	6. Improved perceptual video encryption using multiple 8×8 transforms in MPEG-4 [75]
	7. Perceptual video encryption for multimedia applications [78]
	8. Perceptual video encryption in multimedia secure communication [16]
	9. Perceptual video encryption via unit anti-diagonal matrix [7]
	10. The video encryption scheme based on perceptual encryption algorithm in H.264 standards [72]
	11. Transparent encryption with scalable video communication: Lower-latency, CABAC-based schemes [89]
	12. Visual quality control for perceptual video encryption with multiple transforms [15]
Hybrid Encryption	1. Secure Implementation for Video Streams Based on Fully and Permutation Encryption Techniques [23]
	2. Video Encryption for Secure Multimedia Transmission - A Layered Approach [47]
	3. Partial Video Encryption Using Random Permutation Based on Modification on Dct Based Transformation [50]
	4. A novel idea of video encryption using hybrid cryptographic techniques [31]

3.4.2 Performance Metrics for Video Encryption Algorithm

Some set of parameters have been defined in various past literatures to evaluate and compare the performance of video encryption algorithms. The metrics include:

I. Cryptographic Security (CS): This refers to the level of resistance of encryption algorithm against various attacks: brute force, plaintext, and cipher text attack.

II. Encryption /Decryption Ratio (ER/DR): This is a measure of the ratio between the size of encrypted/decrypted part and the whole video size. It can also determine the computational complexity of the video encryption algorithm

III. Format Compliance (FC): It is desired that the encryption algorithm preserves the video compression format. In other words, after encrypting the video, common decoders can easily decode it without crashing.

IV. Perceptual Security/Visual Degradation (PS/VD): This criterion measures the perceptual distortion of the video with respect to the original unencrypted video. It could be important to achieve high level of visual distortion in order for an attacker to have some understanding of the video content such that access is granted to low quality version of the original video. This will definitely lead to interest in paying for the full access of the unencrypted version of the video content. On the other hand, a high security or sensitive content does not deserve any form of visual degradation.

IV. Encryption time and decryption time (ET/DT): These refer to the time it takes an algorithm to convert a plain video to a cipher video and convert a cipher video back to a plain video respectively. Both ET and DT, usually, are measured in seconds (s).

VI. Mean Square Error (MSE): It is the difference in the average between the number of original frames and the number of encrypted frames.

VII. Peak Signal to Noise Ratio (PSNR): This is a measure of the degree of noise (distortion) in decrypted video with reference to the original video. It is calculated in terms of MSE. It is measured in Decibels (dB).

VIII. Structural similarity (SSIM) index is a measure of the similarity between original video and the decrypted video considering their structural distortion instead of the error.

However, authors of previously proposed video encryption algorithms consider some or all the aforementioned metrics depending on the purpose of their algorithm. Table 4 shows a checklist of the performance metrics considered in the articles reviewed.

IV. RESULTS AND DISCUSSION

This study was carried out on 85 journals. Authors of 70 papers proposed video encryption algorithms while authors of 15 papers carried out survey and overview on video encryption related articles and journals. The summary of the video encryption techniques they adopted is shown in Table 5. The authors used some of the performance metrics mentioned earlier to measure the performance of their proposed video encryption algorithms. The frequency of usage of these metrics is summarized in Table 6.

4.1 Result of techniques of VEA

Among the authors of 70 papers that proposed video encryption algorithm, 36 of them employed selective encryption, 12 of them used naïve/full layered encryption, 12 used Perceptual encryption, 6 used permutation-based encryption while 4 of them combined two or more encryption techniques (hybrid). Their percentage distribution is: 51%, 17%, 17%, 9% and 6% respectively as shown in Figure 3. This result indicates that most of the authors adopted selective encryption techniques while hybrid technique which is a combination of two or more standard VEA is the least adopted.

4.2 Result of VEA Performance Metrics

The result from Table 6 shows that out of authors of 70 papers that proposed VEA, 65 measured cryptographic security (CS), 50 measured encryption/decryption ratio (ER/DR), 36 measured format-compliance (FC), 53 measured encryption/decryption time (ET/DT), 43 measured perceptual security/visual degradation (PS/VD), 37 measured peak- signal-to-noise ratio (PSNR), 37 measured mean square error (MSE) and 19 measured structural similarity (SSIM). Their percentage distribution is: 93%, 71%, 51%, 75%, 61%, 53%, 53% and 27% respectively as shown in Figure 4. The result shows that Cryptographic security is the most measured performance metrics while SSIM is the least measured performance metrics.

Table 4: Performance Metrics Measured by Authors of Previously Proposed Video Encryption Algorithms

Article Ref	Cs	Er/Dr	FC	ET/DT	PS/VD	MSE	PSNR	SSIM
FSVEA [38]	✓	✓	✓	✓	X	X	X	X
NAVEMAES [8]	✓	✓	X	✓	X	X	X	X
NDMTPVE [9]	X	✓	X	✓	✓	✓	✓	X
MPAMSVE [85]	✓	X	X	✓	✓	✓	✓	✓
NSVEAH [82]	✓	✓	✓	✓	X	✓	✓	X
NIVEHCI [31]	X	X	X	✓	X	✓	✓	X
SFSAVE [51]	✓	✓	X	✓	✓	✓	✓	X
SVETRAR [25]	✓	✓	X	X	X	X	X	X
SESPHMSN [49]	✓	✓	✓	X	✓	✓	✓	✓
SEMSLHCS [56]	✓	✓	✓	✓	X	✓	✓	X
EFCVESH [66]	✓	✓	✓	✓	✓	✓	✓	✓
ESVESR [64]	✓	✓	✓	✓	✓	✓	✓	X
EVESHCB [41]	✓	✓	✓	✓	✓	X	X	X
EVESCDH [81]	✓	✓	✓	✓	✓	X	X	X
ESVSAES [74]	✓	✓	✓	✓	X	✓	✓	X
ISEVIPMS [33]	✓	✓	✓	X	✓	✓	✓	X
IVEMD [42]	✓	✓	X	✓	X		X	X
CEPHHVC [68]	✓	✓	✓	X	✓	✓	✓	✓
DVEMD [44]	✓	X	X	✓	X	X	X	X
DINVESS [59]	✓	X	X	✓	X	X	X	X
DIVEMA [12]	✓	✓	X	✓	X	X	X	X
DNUTPVE [71]	✓	✓	✓	X	✓	X	X	✓
DLVRSA [13]	✓	✓	X	✓	✓	X	X	X
EEIIFMV [80]	✓	✓	✓	✓	X	X	X	X
EHEVCVA [62]	✓	✓	X	✓	X	X	X	X
EESVRTA [61]	✓	✓	X	✓	✓	X	X	X
ESISMACR [34]	✓	X	X	✓	✓	✓	✓	✓
ESEHIHEV [14]	✓	X	X	✓	✓	✓	✓	✓
FCDVEH [45]	✓	✓	✓	✓	✓	✓	✓	✓
FVEPSMD [18]	✓	✓	✓	✓	✓	X	X	X
FCPVEMD [35]	X	X	X	X	X	✓	✓	X
HRBVES [69]	✓	✓	✓	✓	✓	✓	✓	✓
HSFVEMO [37]	✓	X	✓	X	✓	✓	✓	X
ICSECV [10]	✓	✓	X	✓	✓	X	X	X
IPVEST [36]	X	✓	X	✓	✓	✓	✓	X
IPVENT [83]	✓	X	X	X	✓	✓	✓	X
IPVEM8T [75]	X	X	✓	X	✓	✓	✓	X
SSEDETHV [58]	X	X	X	✓	✓	✓	✓	X
LVEEP [60]	✓	✓	X	✓	✓	✓	✓	X
MABAVE [19]	✓	✓	X	✓	X	X	X	X
MCTPBV [55]	X	X	✓	✓	✓	✓	✓	X
NSEFOHV [82]	✓	✓	✓	✓	✓	✓	✓	X
PVERPB [50]	✓	✓	✓	✓	✓	X	X	X
PVEMA [78]	✓	✓	✓	X	✓	X	X	X
PVEMSC [16]	✓	X	✓	✓	✓	✓	✓	X
PVEUADM [7]	✓	✓	X	X	✓	X	X	X

PPHVES [17]	✓	X	✓	X	X	X	X	✓
PVEVSOEA [5]	✓	✓	✓	✓	X	X	X	X
PZ-CIVEA [40]	✓	✓	✓	✓	X	X	X	X
RTVESMT [20]	✓	✓	X	✓	X	X	X	X
RTPEDVSD [48]	✓	✓	X	✓	X	X	X	X
ROISESPP [27]	✓	✓	X	✓	X	✓	✓	X
RVTETBFA [29]	✓	✓	X	✓	X	X	X	X
RVE/DSE [28]	✓	✓	X	✓	X	X	X	X
SIVSBFPET [23]	✓	✓	X	✓	X	✓	✓	X
SSEAMV [52]	✓	X	✓	✓	✓	X	X	X
SCVSRC4 [26]	✓	X	✓	X	X	X	X	X
SEAIVCSC [54]	✓	✓	X	✓	X	X	X	X
SRDHEM [77]	✓	✓	✓	✓	✓	✓	✓	✓
SKATVEM [43]	✓	X	✓	X	X	X	X	X
SVESBCD [32]	✓	X	✓	X	✓	✓	✓	✓
SSECAVL [21]	✓	✓	X	X	✓	X	X	✓
DVCES [70]	✓	X	✓	✓	X	X	X	X
VEBPEA [72]	✓	✓	✓	X	✓	X	X	X
JLVEA [39]	✓	✓	X	✓	✓	X	X	✓
TESVCLL [89]	✓	✓	✓	✓	✓	✓	✓	✓
VEAKMSH [57]	✓	✓	X	✓	✓	✓	✓	✓
VESHUC/R [24]	✓	✓	✓	✓	X	X	X	X
VESMFLA [47]	✓	✓	X	✓	X	X	X	X
VEAES [22]	✓	✓	X	✓	X	X	X	X
VPHVSE [84]	✓	✓	✓	✓	✓	✓	✓	X
VQCPVMT [15]	✓	X	✓	X	✓	✓	✓	✓
TOTAL	**65**	**50**	**36**	**53**	**43**	**37**	**37**	19

Legend for Table 4: ✓ Metrics Measured X Metrics Not Measured

Table 5: Techniques of Video Encryption Algorithm

Techniques of VEA						
	Naïve / Full	Permut ation	Select -ive	Perce ptual	Hybrid	Total
No. of authors	12	6	36	12	4	70
%	17	9	51	17	6	100

Table 6: Frequency of Usage of Metrics for Video Encryption Algorithms

Frequency of usage of Performance Metrics								
	CS	ER / DR	FC	ET / DT	PS / VD	MSE	PSNR	SSIM
No. of authors	65	50	36	53	43	37	37	19
%	93	71	51	76	61	53	53	27

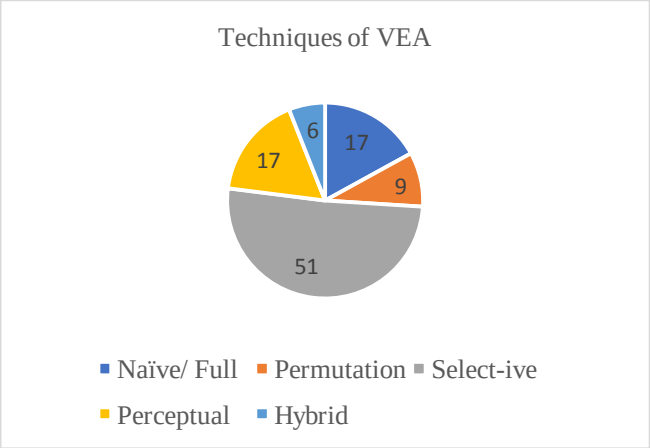

Figure 3: Percentage of Techniques of VEA

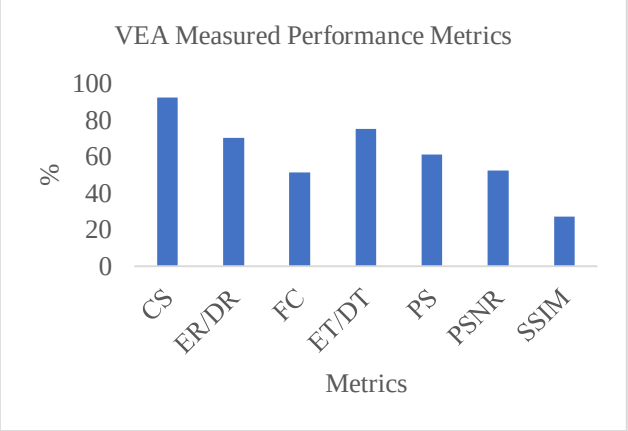

Figure 4: Percentage of Performance Metrics Measure

V. CONCLUSION

This study presents a systematic review of previously proposed video encryption algorithm in recent time. The review shows that most researchers employed selective encryption techniques to encrypt the video due to its lower computational cost and higher speed. Furthermore, Cryptographic security, Encryption/decryption ratio, Format compliance, perceptual security/visual degradation, PSNR and SSIM are some of the performance metrics used to measure the performance of the video encryption algorithm proposed by the researchers. Finally, this study reveals that Cryptographic security and Encryption/decryption time are the most measured performance metrics while SSIM is the least measured performance metrics considered by authors of previously proposed video encryption algorithms.

REFERENCES

[1] M. Abomhara, O. Zakaria and O. O. Khalifa, "An Overview of Video Encryption Techniques," *International Journal of Computer Theory and Engineering*, vol. 2, no. 1, pp. 103-110, 2010.

[2] M. K. Swartz, "The PRISMA statement: a guideline for systematic reviews and meta-analyses," *Journal of Peadiatric Health Care*, vol. 25, no. 1, pp. 1-2, 2011.

[3] D. Moher, A. Liberati, J. Tetzlaff and DG. Altman, "Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement," Ann. Intern. Med., vol.," *Annual International Med, PMID*, vol. 151, no. 4, p. 264, 2009.

[4] B. Kitchenham, R. Pretorius, D. Budgen, O. P. Brereton, M. Turner, M. Niazi and S. Linkman, "Systematic literature reviews in software engineering – A tertiary study," *Information and Software Technology*, vol. 52, p. 792–805, 2010.

[5] Ajay Kulkarni, Saurabh Kulkarni, Ketki Haridas, and Aniket More, Proposed Video Encryption Algorithm v/s Other Existing Algorithms: A Comparative Study, *International Journal of Computer Applications*, Volume 65, No.1, pp. 1-5, 2013.

[6] F. Liu and H. Koenig, "A survey of video encryption algorithms," *Computers and Security*, vol. 29, no. 1, pp. 3-15, 2010.

[7] S. Alhassan, M. M. Iddrisu and M. I. Daabo, "Perceptual video encryption via unit anti-diagonal matrix," *Applied Mathematics and Information Sciences*, vol. 12, no. 5, pp. 923-930, 2018.

[8] S. Ali Abaas and A. Kareem Shibeeb, "A New Approach for Video Encryption Based on Modified AES Algorithm," *IOSR Journal of Computer Engineering* (IOSR-JCE), vol. 17, no. 3, pp. 44-51, 2015.

[9] S. K. Au Yeung and B. Zeng, "A new design of multiple transforms for perceptual video encryption," *Proceedings - International Conference on Image Processing*, ICIP, pp. 2637-2640, 2012.

[10] S. Batham, V. K. Yadav and A. K. Mallik, "ICSECV: An efficient approach of video encryption," *2014 7th International Conference on Contemporary Computing*, IC3 2014, pp. 425-430, 2014.

[11] K. Ashrith, S. P. Prajwal, M. Raunak, R. Saurabh and A. Syed, "A Survey on Efficient and Secure Video Encryption Techniques," *International Journal of Innovations in Engineering and Technology (IJIET)*, vol. 6, no. 4, pp. 3-9, 2016.

[12] P. Aggarwal and S. Vishwanath, "Design and Implementation of Video Encryption for Multimedia Applications," *International Journal of Engineering Research and Applications*, vol. 4, no. 4, pp. 29-34, 2014.

[13] A. Chadha, S. Mallik, A. Chadha, R. Johar and M. Mani Roja, "Dual-Layer Video Encryption using RSA Algorithm," *International Journal of Computer Applications*, vol. 116, no. 1, pp. 33-40, 2015.

[14] B. Boyadjis, C. Bergeron, B. Pesquet-Popescu and F. Dufaux, "Extended Selective Encryption of H.264/AVC (CABAC)-and HEVC-Encoded Video Streams," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 27, no. 4, pp. 892-906, 2017.

[15] S. K. Au Yeung and B. Zeng, "Visual quality control for perceptual video encryption with multiple transforms," *2012 7th International ICST Conference on Communications and Networking in China, CHINACOM 2012 - Proceedings*, pp. 189-192, 2012.

[16] T. Bernatin, S. Kuzhaloli, M. S. Premi and L. B. Queen, "Perceptual video encryption in multimedia secure communication," *Proceedings of 2016 Online International Conference on Green Engineering and Technologies*, IC-GET 2016, 2017.

[17] S. Choi, J. W. Han and H. Cho, "Privacy-preserving H.264 video encryption scheme," *ETRI Journal*, vol. 33, no. 6, pp. 935-944, 1 12 2011.

[18] Y. Chung, S. Lee, T. Jeon and D. Park, "Fast video encryption using the H.264 error propagation property for smart mobile devices," *Sensors* (Switzerland), vol. 15, no. 4, pp. 7953-7968, 2015.

[19] P. Deshmukh and V. Kolhe, "Modified AES based algorithm for MPEG video encryption," *2014 International Conference on Information Communication and Embedded Systems*, ICICES 2014, 2015.

[20] N. Dilkash, A. Gupta and A. Jain, "Real Time Video Encryption for Secure Multimedia Transfer : A Novel Approach," pdfs.semanticscholar.org, vol. 8, no. 4, pp. 17077-17080, 2018.

[21] L. Dubois, W. Puech and J. Blanc-Talon, "Smart selective encryption of CAVLC for H.264/AVC video," *2011 IEEE International Workshop on Information Forensics and Security*, WIFS 2011, 2011.

[22] D. M. Dumbere and N. J. Janwe, "Video encryption using AES algorithm," *2nd International Conference on Current Trends in Engineering and Technology*, ICCTET 2014, pp. 332-337, 2014.

[23] A. M. Elshamy, M. A. Abdelghany, A. Q. Alhamad, H. F. Hamed, H. M. Kelash and A. I. Hussein, "Secure Implementation for Video Streams Based on Fully and Permutation Encryption Techniques," *2017 International Conference on Computer and Applications, ICCA 2017*, pp. 50-55, 2017.

[24] S. T. Faraj Al-Janabi, K. Shaaban Rijab and A. Makki Sagheer, "Video encryption based on special

huffman coding and rabbit stream cipher," *Proceedings - 4th International Conference on Developments in eSystems Engineering, DeSE 2011*, pp. 413-418, 2011.

[25] N. Geetha and K. Mahesh, "A Secure Video Encryption Technique Using Rijndael Algorithm," *International Journal of Science and Research* (IJSR),vol.3, no. 5, 2012.

[26] S. S. Giradkar and A. Bhattacharya, "Securing compressed video streams using RC4 encryption scheme," *Global Conference on Communication Technologies*, GCCT 2015, pp. 640-644, 2015.

[27] J. Guo, J. Y. Xu and J. L. Bao, "Region of interest based selective encryption scheme for privacy protection in H.264 video," *Journal of Shanghai Jiaotong University (Science)*, vol. 19, no. 4, pp. 385-391, 2014.

[28] R. N. Hole and M. Kolhekar, "Robust video encryption and decryption using selective encryption," *2017 International Conference on Nascent Technologies in Engineering, ICNTE 2017 - Proceedings*, 2017.

[29] R. Huang and C. Lu, "Research of H.264 video transmission encryption technology based on blowfish algorithm," *Proceedings of 2015 4th International Conference on Computer Science and Network Technology, ICCSNT 2015*, pp. 931-935, 2016.

[30] R. R. Igorevich, H. Yong, D. Min and E. Choi, "A study on multimedia security systems in video encryption," *NC2010: 6th International Conference on Networked Computing*, Gyeongju, Korea (South), 2010, pp. 1-5.

[31] S. C. Iyer, R. R. Sedamkar and S. Gupta, "A novel idea of video encryption using hybrid cryptographic techniques," *Proceedings of the International Conference on Inventive Computation Technologies, ICICT 2016*, vol. , 2016.

[32] S. Cheng, L. Wang, N. Ao, and Q. Han, "A selective video encryption scheme based on coding characteristics," *Symmetry*, vol. 12, no. 3, pp. 332-346, 2020.

[33] J. Jiang, Y. Liu, Z. Su, G. Zhang and S. Xing, "An improved selective encryption for h.264 video based on intra prediction mode scrambling," *Journal of Multimedia*, vol. 5, no. 5, pp. 464-472, 2010.

[34] J. M. Joshi and U. D. Dalal, "Enhancing selective ISMACryp video encryption for real time applications in handheld devices," *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, pp. 274-278, 2011.

[35] N. Kamnoonwatana, "Format-compliant perceptual video encryption based on multiple description coding," *2013 IEEE 11th Malaysia International Conference on Communications*, MICC 2013, pp. 75-80, 2013.

[36] A. Kirthanaa, N. Mathan and T. Vino, "Improved perceptual video encryption and decryption using S-transform," *2015 International Conference on Control Instrumentation Communication and Computational Technologies, ICCICCT 2015*, pp. 145-148, 2016.

[37] J. M. Joshi and U. D. Dalal, "Highly Secure and Fast Video Encryption Using Minimum Overhead in H.264/AVC Bitstream," *Journal of Testing and Evaluation*, vol. 44, no. 4, p. 140-332, 2016.

[38] Z. Li, X. Wang and W. Yang, "A fast selective video encryption algorithm by selecting data randomly," *Sixth International Conference on Electronics and Information Engineering*, vol. 9794, 2015.

[39] J. Yun and M. Kim, " JLVEA: Lightweight Real-Time Video Stream Encryption Algorithm for Internet of Things," *Sensors*, vol. 20, no. 13, pp. 3627-3641, 2020.

[40] F. Liu and H. Koenig, "Puzzle - An efficient, compression independent video encryption algorithm," *Multimedia Tools and Applications*, vol. 73, no. 2, pp. 715-735, 8 10 2014.

[41] N. Mao, L. Zhuo, X. Li and J. Zhang, "An efficient video encryption scheme for H.264 compressed bitstream," *Proceedings - 7th International Conference on Information Processing and Management, ICIPM 2011*, pp. 89-94, 2011.

[42] Y. Liang, K. Guo and J. P. Li, "An improved video encryption method design," *2013 10th International Computer Conference on Wavelet Active Media Technology and Information Processing, ICCWAMTIP 2013*, pp. 95-99, 2013.

[43] K. Minemura and K. Wong, "Sketch attacks: A note on designing video encryption method in H.264/AVC," *2014 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, APSIPA 2014*, 2014.

[44] A. K. Naji and S. N. Alsaad, "Data (Video)

Encryption in Mobile devices," *Kurdistan Journal of Applied Research*, vol. 2, no. 3, pp. 32-39, 2017.

[45] N. Mao, L. Zhuo, J. Zhang and X. Li, "Fast compression domain video encryption scheme for H.264/AVC streaming," *International Conference on Advanced Communication Technology, ICACT*, pp. 425-429, 2012.

[46] Y. Negi, "A Survey on Video Encryption Techniques," *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, no. 4, pp. 234-237, 2013.

[47] T. P. Pai, M. E. Raghu and K. C. Ravishankar, "Video Encryption for Secure Multimedia Transmission - A Layered Approach," *Proceedings - 2014 3rd International Conference on Eco-Friendly Computing and Communication Systems, ICECCS 2014*, pp. 127-132, 2015.

[48] A. S. Rahma and B. Z. Yacob, "Real-Time Partial Encryption of Digital Video Using Symmetric Dynamic Dual Keys Algorithm (SDD)," 2012.

[49] F. Peng, X. q. Gong, M. Long and X. m. Sun, "A selective encryption scheme for protecting H.264/AVC video in multimedia social network," *Multimedia Tools and Applications*, vol. 76, no. 3, pp. 3235-3253, 2017.

[50] S. Rajagopal and M. Shenbagavalli, "Partial Video Encryption Using Random Permutation Based on Modification on Dct Based Transformation," *irjes.com*, vol. 2, no. 6, pp. 54-58, 2013.

[51] J. Rajpurohit and A. Khunteta, "A scalable frame scrambling algorithm for video encryption," *2013 IEEE Conference on Information and Communication Technologies, ICT 2013*, pp. 981-985, 2013.

[52] M. Roy and C. Pradhan, "Secured selective encryption algorithm for MPEG-2 video," *ICECT 2011 - 2011 3rd International Conference on Electronics Computer Technology*, vol. 2, pp. 420-423, 2011.

[53] M. A. Saleh, N. M. Tahir, E. Hisham and H. Hashim, "An analysis and comparison for popular video encryption algorithms," *ISCAIE 2015 - 2015 IEEE Symposium on Computer Applications and Industrial Electronics*, pp. 90-94, 2015.

[54] A. A. Ramdan and R. Munir, "Selective encryption algorithm implementation for video call on Skype client," *2012 7th International Conference on Telecommunication Systems, Services, and Applications, TSSA 2012*, pp. 120-124, 2012.

[55] C. C. Sabino, L. S. Andrade, T. I. Ren, G. D. Cavalcanti, T. I. Jyh and J. Sijbers, "Motion compensation techniques in permutation-based video encryption," *Proceedings - 2013 IEEE International Conference on Systems, Man, and Cybernetics, SMC 2013*, pp. 1578-1581, 2013.

[56] F. Sbiaa, S. Kotel, M. Zeghid, R. Tourki, M. Machhout and A. Baganne, "A selective encryption scheme with multiple security levels for the H.264/AVC video coding standard," *Proceedings - 2016 16th IEEE International Conference on Computer and Information Technology, CIT 2016*, 2016 6th International Symposium on Cloud and Service Computing, IEEE SC2 2016 and 2016 International Symposium on Security and Privacy in Social Network, pp. 391-398, 2017.

[57] S. F. Sultana and D.C. Shubhangi, "Video Encryption Algorithm and Key Management using Perfect Shuffle," *International Journal of Engineering Research and Applications*, vol. 07, no. 02, pp. 1-5, 2017.

[58] Y. Tew, K. Wong and R. C. Phan, "Joint selective encryption and data embedding technique in HEVC video," *2016 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, APSIPA 2016*, 2017.

[59] X. Tian, C. Fan, J. Liu and Q. Ding, "Design and implementation of network video encryption system based on STM32 and AES algorithm," *Smart Innovation, Systems and Technologies*, vol. 82, pp. 51-58, 2018.

[60] L. Tong, G. Cao and J. Li, "Layered video encryption utilizing error propagation in H.264/AVC," *Proceedings - 2012 IEEE Symposium on Electrical and Electronics Engineering, EEESYM 2012*, pp. 182-187, 2012.

[61] L. M. Varalakshmi, G. Florence Sudha and V. Vijayalakshmi, "Enhanced Encryption schemes of video for real time applications," *2011 - International Conference on Signal Processing, Communication, Computing and Networking Technologies, ICSCCN-2011*, pp. 408-413, 2011.

[62] G. V. Wallendael, A. Boho, J. D. Cock, A. Munteanu and R. V. D. Walle, "Encryption for high efficiency video coding with video adaptation capabilities," *IEEE Transactions on Consumer Electronics*, vol. 59, no. 3,pp. 634-642, 2013.

[63] L. Tong, F. Dai, Y. Zhang and J. Li, *Visual security evaluation for video encryption*, 2010, pp. 835-838.

[64] L. M. Varlakshmi, G. F. Sudha and G. Jaikishan, "An efficient scalable video encryption scheme for real time applications," *Procedia Engineering*, vol. 30, pp. 852-860, 2012.

[65] Q. H. Wang and X. J. Wang, "Study of selective video encryption for the H.264 standard," *Applied Mechanics and Materials*, Vols. 397-400, pp. 2097-2103, 2013.

[66] M. Yang, L. Zhuo, J. Zhang and X. Li, "An efficient format compliant video encryption scheme for HEVC bitstream," *Proceedings of 2015 IEEE International Conference on Progress in Informatics and Computing, PIC 2015*, pp. 374-378, 2016.

[67] Q. Wang and X. Wang, "A new selective video encryption algorithm for the H.264 standard," *PIC 2014 - Proceedings of 2014 IEEE International Conference on Progress in Informatics and Computing*, pp. 275-279, 2014.

[68] D. Xu, "Commutative Encryption and Data Hiding in HEVC Video Compression," *IEEE Access*, vol. 7, pp. 66028-66041, 2019.

[69] X. Wang, N. Zheng and L. Tian, "Hash key-based video encryption scheme for H.264/AVC," *Signal Processing: Image Communication*, vol. 25, no. 6, pp. 427-437, 2010.

[70] H. Z. Yao and Y. T. Jing, "The design of video-conference encryption system based on H.264," 2010 *International Conference on Multimedia Technology, ICMT 2010*, 2010.

[71] S. K. A. Yeung, S. Zhu and B. Zeng, "Design of new unitary transforms for perceptual video encryption," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 21, no. 9, pp. 1341-1345, 2011.

[72] X. Y. Zhang, H. C. Deng and L. W. Chen, "The video encryption scheme based on perceptual encryption algorithm in H.264 standards," 2013.

[73] S. K. A. Yeung, S. Zhu and B. Zeng, "Quality assessment for a perceptual video encryption system," *Proceedings - 2010 IEEE International Conference on Wireless Communications, Networking and Information Security, WCNIS 2010*, pp. 102-106, 2010.

[74] M. Abomhara, O. O. Khalifa, A. A. Zaidan, B. B. Zaidan, O. Zakaria and A. Gani, "An experiment of scalable video security solution using H.264/AVC and advanced encryption standard (AES): Selective cryptography," *International Journal of Physical Sciences*, vol. 6, no. 16, pp. 4075-4085, 2011.

[75] S. K. Au Yeung and B. Zeng, "Improved perceptual video encryption using multiple 8×8 transforms in MPEG-4," *2012 7th International ICST Conference on Communications and Networking in China, CHINACOM 2012 - Proceedings*, pp. 185-188, 2012.

[76] A. N. Babatunde, R. G. Jimoh, O. C. Abikoye and B. Y. Isiaka, "Survey of Video Encryption Algorithms," *Covenant Journal of Informatics and Communication Technology*, vol. 5, no. 1, pp. 65-80, 2017.

[77] M. Long, F. Peng and H. y. Li, "Separable reversible data hiding and encryption for HEVC video," *Journal of Real-Time Image Processing*, vol. 14, no. 2, pp. 1-12, 2018.

[78] U. Potdar, K. T. Talele and S. T. Gandhe, "Perceptual video encryption for multimedia applications," *2010 2nd International Conference on Computer Engineering and Applications, ICCEA 2010*, vol. 1, pp. 587-589, 2010.

[79] S. Rajagopal and A. Shenbagavalli, "A Survey of Video Encryption Algorithms Implemented In Various Stages of Compression," *International Journal of Engineering Research & Technology*, vol. 2, no. 2, pp. 1-12, 2013.

[80] V. Vijayalakshmi, L. M. Varalakshmi and G. F. Sudha, "Efficient encryption of intra and inter frames in MPEG video," *The Third International Conference on Network Security and Applications (CNSA 2010),in Communications in Computer and Information Science*, pp. 93-105, 2010.

[81] L. Zhuo, N. Mao, J. Zhang and X. Li, "An efficient video encryption scheme in compressed domain for H.264/AVC," *International Conference on Advanced Communication Technology, ICACT*, pp. 11-16, 2013.

[82] D. Goyal and N. Hemrajani, "Novel Selective Video Encryption for H.264 Video," *International Journal Of Information Security Science*, vol. 3, no. 4, pp. 216-227, 2014.

[83] S. K. A. Yeung, S. Zhu and B. Zeng, "Improved perceptual video encryption using alternative unitary transforms," *2010 5th International ICST Conference on Communications and Networking in China, ChinaCom 2010*, 2010.

[84] Z. Shahid and W. Puech, "Visual protection of HEVC video by selective encryption of CABAC binstrings," *IEEE Transactions on Multimedia*, vol. 16, no. 1, pp. 24-36, 2014.

[85] N. Sidaty, W. Hamidouche and O. Deforges, "A new perceptual assessment methodology for selective HEVC video encryption," *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, pp. 1542-1546, 2017.

[86] S. Singh, N. Verma and V. Kumar, "A Survey Report on Video Encryption and Decryption Techniques," *International Journal of Computer Science and Mobile Computing*, vol. 3, no. 12, pp. 270-274, 2014.

[87] J. Shah and D. V. Saxena, "Video Encryption: A Survey," *IJCSI International Journal of Computer Science Issues*, vol. 8, no. 2, pp. 525-535, 2011.

[88] D. Hooda and P. Singh, "A Comprehensive Survey of Video Encryption Algorithms," *International Journal of Computer Applications* , vol. 59, no. 1, pp. 14-20, 2012.

[89] M. N. Asghar, R. Kousar, H. Majid and M. Fleury, "Transparent encryption with scalable video communication: Lower-latency, CABAC-based schemes," *Journal of Visual Communication and Image Representation*, vol. 45, pp. 122-136, 2017.

[90] C. Sridevi, "A survey on Network Security," *Global Journal of Computer Science and Technology*, vol. 17, no. 5, 2018.

[91] P. Matta, B. Pant and U. K. Tiwari. "DDITA: A naive security model for IoT resource security." In *Smart Innovations in Communication and Computational Sciences*, pp. 199-209. Springer, Singapore, 2019.

[92] M. Altaf, A. Ahmad, F. A. Khan, Z. Uddin and X. Yang, "Computationally efficient selective video encryption with chaos based block cipher," *Multimed Tools Appl* 77, 27981–27995 (2018).

[93] N.J. Mamvong, T. Aboiyar and T. Gbaden, "A Hybrid Cryptosystem Using Elgamal Algorithm and Matrix Encryption," *African Journal of Computing and ICT*, vol. 8, no. 3, pp. 43-50, 2015.

BIODATA OF AUTHORS

Adetokunbo Abayomi Adenowo, Ph.D, is a Senior Lecturer in the Department of Electronic and Computer Engineering, Lagos State University, Epe Campus, Lagos State. He obtained Bachelor of Science (BSc) and Master of Science (MSc.) in Computer Science from University of Lagos in 1990 and 1995 respectively, and Master of Business Administration (MBA) from Lagos State University in 2000. In 2012, he received Doctor of Philosophy (PhD) in Software Engineering and eLearning from De Montfort University, United Kingdom. He is currently the Postgraduate Coordinator in the Department of Electronic & Computer Engineering, Lagos State University. His research interest includes: Software Engineering, Intelligent Learning Systems, and Security Engineering.

Latifat Folake Oderinu received her B.Tech Degree in Computer Engineering from Ladoke Akintola University of Technology, Ogbomoso, Oyo State, Nigeria, in 2007 and a Post-Graduate Diploma in Education (PGDE) from National Teachers' Institute, Nigeria in 2016. Her undergraduate project focused on Dynamic Load Balancing in Network Applications while her PGDE project focused on Multimedia Use, Teaching and Learning of Computer Science in secondary schools (Ifako-Ijaiye Local Government Area of Lagos State). She is currently a Masters Student at the department of Electronic and Computer Engineering, Lagos State University, Epe Campus. Her current thesis is based on video encryption algorithms.