Webology (ISSN: 1735-188X)
Volume 19, Number 1, 2022

A Review: Video Encryption Techniques, Advantages And Disadvantages

Tameem Hameed Obaida[1] , Abeer Salim Jamil[2] , Nidaa Flaih Hassan[3]

[1]Department of Computer Systems Techniques, Al-Furat Al-Awsat Technical University, Najaf Technical Institute, Najaf, Iraq.

[2] Computer Science & Information Systems Department, Al-Mansour University College, Baghdad, Iraq.

[3]Department of Computer Science, University of Technology, Baghdad, Iraq.

Abstract

Digital video contains potentially very important data that needs high protection, So researchers began competing in how to find ways to preserve data from illegal access, including the encryption that was used to protect the video content (fully or selectively). Where all methods aim to provide the highest levels of protection for the individuals. So the challenges began in designing strong encryption algorithms that are hard to break and also be fast.The goal of this study is to show some of the techniques used in video encryption, with mentioning the pros and cons of each technique to identify these cons and avoid them in future work. From our study and analysis, it was found that most technologies achieve one aspect, either increased accuracy rate or speedup implementation time, especially when implemented in real time , because both negatively affect the other. For example, methods that use lightweight algorithms such as RC4, chacha and others focus on speed, while other algorithms such as RSA,DES...etc focus on the level of security.Therefore we suggest combining the advantages for algorithms by hybridization to building a fast and robust algorithm that can be implemented in real-time.

Keywords: Video encryption, Object encryption , Selective encryption , Fully encryption.

1. Introduction

Protecting information and maintaining privacy from critical and important topics, whether this information is text, image, or sound. Therefore, as a result of the great development in multimedia, including video, which contains a large amount of information, it has been used in many fields including surveillance, legal affairs, medicine, and others[1].

One of the effective ways to protect sensitive data is encryption, numerous researchers are drawn to designing encryption methods that are both efficient and secure to video and image[2]. Where conventional encryption algorithms like advanced encryption standard AES, Rivets-Shamir-Adelman(RSA), IDEA, and Data Encryption Standard (DES) were designed, which were considered unsuitable for encrypting video, especially in the case of real-time encryption, because these methods are usually slow and require high computing power[3]. In general, video encryption is divided into two types, and each one has its pros and cons, they are as follows:-

1- Fully encryption is typically appropriate for small quantities of encrypted data and requires a high level of security. This method is not proper in applications that use real-time video because to slow speed and intensive computation.
2- selective encryption is appropriate for great quantities of encrypted data and powerful performance in real-time. This method does not encrypt every byte in the video, as it encrypts specific bytes, so this technique reduces computational complexity[4].

Because of the vast amount of video data, video encryption takes a long time. In this paper, various video encryption algorithms are described, whether for full or selective encryption. The remaining part of the paper is structured out as follows. The second and third sections are a simple explanation of symmetric and asymmetric key algorithms, respectively. As for the video encryption techniques, which included a detailed study of some techniques, they are mentioned in the fourth section, and the fifth section represents the analysis and recommendation, and finally the conclusion in the sixth section.

2. Symmetric key Algorithms

In symmetric key encryption technique, both sender and receiver use one key for encryption and decryption. Symmetric key encryption is also called a secret key, because both the sender and receiver must keep the key secret and completely protect it [5].

Symmetric keys cannot provide authentication because there is no method to prove who indeed sent the message if two people are using the same key, so although symmetric keys suffer from a lot of problems and flaws it still used in many applications, because they are fast and difficult to crack When large key sizes are used. The most popular symmetric key algorithms are Data Encryption Standard (DES), Triple DES, and Advance Encryption Standard [6]. As shown in figure 1.

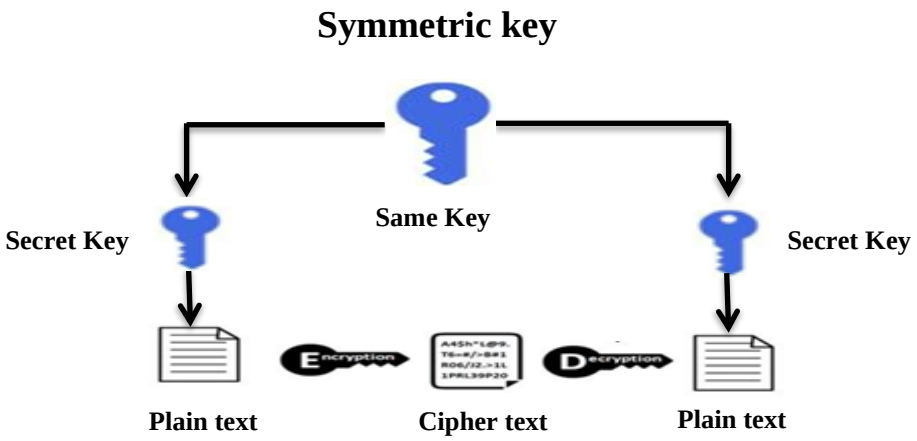

Figure 1. Use the same key in symmetric encryption.

A. Data Encryption Standard (DES)

This algorithm appeared in 1973 in a competition conducted by the US National Bureau of Standards called NIST, but was adopted in 1977 as a standard application, principle of its work depend on block cipher. [7]. IBM's winning standard was created as modulation of the previous LUCIFER system. DES is block cipher, encrypts 64 bits at a time, where the key length is 64 bits also, 8-bits are used to achieve parity after which the key size is reduced to 56 bit. This algorithm is commonly used in banking transactions, PIN number encryption, and other applications [5].

B. Advanced Encryption Standard (AES)

NIST in 1977 invite through a competition to submit applications for a new standard in place of the old DES, which resulted in the selection of the Rijndael Encryption System as the Advanced Encryption Standard (AES) in November 2001. The Rijndael cipher system can use variable key length and block length, allowing the use of key lengths of 128, 192, or 256 bits and block lengths of 128, 192 or 256 bits. Block length 128 is arranged as a 4×4 arrays with 8 bits as entries [8].

3. Asymmetric key Algorithms

In 1976 public key algorithms were publicly described by graduate student Whitfield Diffie and Martin Hellman professor in Stanford University. Public key algorithms have two keys, the first is called the public key, which is public to everyone, and the second is called the private key, usually a secret that only the owner knows. The message is encrypted with the secret key, and the public key is used for decryption. As shown in Figure 2.

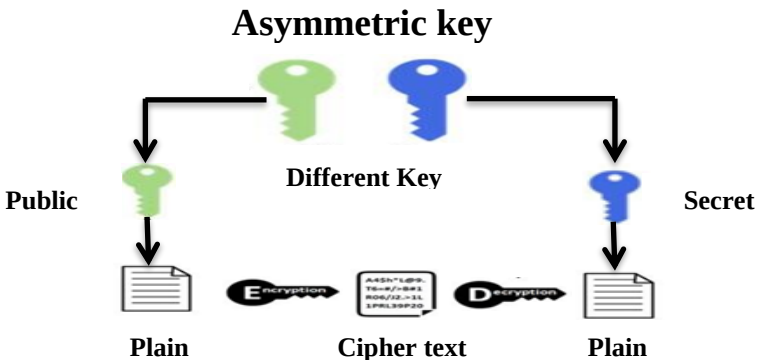

Figure 2. Use a different key in asymmetric encryption.

It is not a problem when the public key is known by anyone, because he is unable to access the private key, although the two keys are mathematically related, but the real problem is in obtaining the private key, because it is known only to the owner. The authentication is main condition, when the sender encrypts the message use the secret key, then the receiver decrypts the message with the public key. One of the most famous symmetric key algorithms is RSA and Diffie-Hellman Key Exchange. [9].

A. Rivest- Shamir Adelman (RSA)

The RSA algorithm was invented by Ron Rivest, Adi Shamir, and Len Adelman in 1977, which is one of the most popular and widely used public-key algorithms to date. Its work is based on the idea of factorization of integers into their prime. [10]. The steps below illustrate how it works:

A.key generation

- ✓ .Choosing two large prime numbers randomly, such as x and y.
- ✓ compute $n=x*y$.
- ✓ calculate $\phi(n)=(x-1)(y-1)$.
- ✓ Choce integer e. where $1<e<\phi(n)$. The pair of numbers (n,e) represent the public key.
- ✓ Calculate d such that $e.d=1 \bmod \phi(n)$.

B. Encryption through $C=P^e \bmod n$.

C. Decryption through $P=C^d \bmod n$.

B. Diffie-Hellman Key Exchange

It is a cryptographic protocol that allows two persons without knowledge previously of each other to generate a shared secret key on an unsecured channel. This key can then be used to encrypt plaintext by the asymmetric key encryption algorithm. It appeared for the first time in 1976 and is considered the first way to do the task of exchanging keys using a mathematical process called the discrete logarithm [11]. This algorithm is considered insecure from the man-in-the-middle attack because keys are shared between two parties. Therefore, a digital signature can be used for authentication or establishing a secure communication channel .

4. Techniques of Video Encryption

Important videos, especially those used in legal affairs, for example, the protection of witnesses, which are transmitted through different media, require high security, as many methodologies have been used to protect video content, the most important of which is encryption, so many types of encryption algorithms appeared, some of which were used to encrypt the video fully and some of them are selective[12], in this section several algorithms that relied on these two types of encryption will be presented as follows:

4.1. Selective encryption techniques

This section presents the latest techniques used in selective video encryption, which have been used in order to reduce the encryption time because it focuses on encrypting only a specific part. As follows:

Hamidouche and et al[13], used selective video encryption (SHVC) with the scalable HEVC extension. The SHVC extension encodes video in multiple layers based on various spatial representations and use coding system based on chaos. By the empirical results, the performance of three encryption schemes was compared: lower layer, all layers, and upper layer only. The lower layer scheme and all layers achieved a high level of security, but there is a deterioration in the decoding of video while the upper layer scheme allows perceptual video in encryption by reducing quality of the upper layer without the quality of clear layers.

Li and et al[14], used AES encryption algorithm and (I) frame, where, merged the spark of distributed framework and selective encryption of video, on a single server, The results show that encryption efficiency is improved, and it can be used in real-time because its performance is good.

Malladar and Kunte [15], presented a way to encrypt the face through Local Binary Patterns (LBP) are used to detect the face area in a video frame, and this Region of Interest (ROI) is encrypted using Sattolo's encryption technique. The computational complexity is low, making it a lightweight method, according to results of the experiment.

In another methodology, Hore and et al [16], proposed a two-stage encryption technique based on the well-known sign speech dactylology or fingerspelling and Artificial Neural Networks to extract strong features Speeded-Up in real time and use ISL images as a secret symbol for encryption and decryption work.

In another way, Unterweger and et al[17], suggested a full-featured post-compression framework of encryption for video surveillance systems. It is used to detect and encrypt faces which combines and extends present face detection algorithms, Encryption, and signaling of RoI. According to their findings, the proposed framework's key drawback is the performance of state-of-the-art face detectors. Require about 99 % of the entire runtime. This makes face recognition harder than similar methods.

Researchers Saleh and others[18], discussed in this paper method for encrypting moving objects by High-Efficiency Video Coding (HEVC) media. Selective encryption is used

to encrypt moving objects in video due to high computational complexity. The AES algorithm was chosen to encrypt the vertical data of Motion Vector Difference (MVD).

Sallam and et al [19], present an effective RC6 based HEVC SE method for encrypting sensitive video bits with low complexity overhead, for encrypting the selective video.The empirical results obtained in this way saved average time of encoding for one frame by (0.7 and 4.4) sec compared with AES_CBC and AES_CFB, for low-resolution Forest (320 x 240) video. Whereas, the high resolution Bosphorus video (3840 × 2160), the average encoding time of one frame was 19 sec and 211sec. The results proved this method is fast and its complexity is low.

In another paper by Gerhardt and Others,[20], It includes a face detection module as well as updated H.264 encoder/decoder that makes use of a new way for selective ROI encryption in data of video. Using an adapted prediction algorithm, the encoder separates the ROI from the rest of the video and AES-256 in ECB with specific block keys is used to encrypt quantized DCT coefficients for both luma and chroma values. This method works on individual faces decryption of in the video. In the future, advanced coding techniques may be introduced to predict bidirectional images.

Ahmad and others [3], proposed a real-time occupancy monitoring system with light-weight video encryption based on Region of Interest (ROI). A commonly used background model is used to detect people's movement, i.e., Kalman filter and Gaussian Mixture Model (GMM). The moving objects are encrypted using a TD-ERCS chaotic map. The results are good in terms of computational cost.

Zhang and et al[21], devised an approach to lightweight encryption based on a Layered Cellular Automaton (LCA). All RoIs are encrypted asynchronously and independently. According to what was mentioned in the paper, the theoretical analyzes and experimental results were effective and efficient.

Nguyen Tan and et al [22], presented a new method for face encryption in video and decryption on a graphics processing unit (GPU) using ring learning with errors (ring LWE) cryptography. Where ring arithmetic operations can be performed in parallel on GPU, In order to reduce the processing time. By simulating, the researchers found that processing time for one frame encryption and decryption was only 0.02 seconds on the GPU.

In another work by Shifa and et al[23], two methods of skin detection are presented and privacy protection, that depends on the ability to detect human skin in video bitstreams in the existence of various skin colors/complexion by converting them into RGB, perceptual (HSV), and orthogonal (YCbCr) color spaces. then, the pixels are encrypted using the encryption algorithm (AES-CFB).

Researchers Cheng and et al [24], combined a video encoding algorithm and an encryption algorithm. The H.264 / AVC video encoding algorithm and advanced encryption standard (AES). The key is generated and modified in real-time by a pseudo-random number generator (PRNG).

In another technique, Duong, TAN and LEE [25], provided a method to fully protect the facial image in a video using a post-quantum cryptosystem called NewHope cryptography.

In order to arrange the input data to greatly reduce the encryption and decryption times. The parallel data computing model was used in the Nvidia GTX 2080Ti GPU.

Alhasany and Jawad [26], suggested a method based on the video's motion information is selected intelligently using canny edge detection scaling, which decreases quantity of encrypted data, and strong and fast stream encryption is achieved using the chaos key generation model and the RC4 method. The experimental results showed that the security is high, resistant to attacks, and meets all compression efficiency requirements.

Table 1. shows the previously presented selective encryption methods, explaining the techniques used and the pros and cons of each method, as follows:

Table 1. Brief description of previous selective encryption techniques.

Technologies	Focused on	Advantages	Disadvantages
Chaotic encryption	SHVC extension, Encryption in several layers	High-security level	Reduce the quality of the upper layer.
AES	Choose I frame high depth	High speed, used in real-time	Low security, AES is a symmetric key
Sattolo's encryption, LBP	ROI	High speed	Low accuracy
Full-featured post-compression framework	Encryption and signaling of RoI	Can be used in real time+ minimal effort	Face detectors require about 99 % of the entire runtime
RC6, DCT	RC6 based HEVC SE for encrypting sensitive video bits	Fast and low complexity	Low security
AES-256 in ECB + unique block keys	Selective ROI encryption	High speed	Decrypt individual faces only. In the future, it is possible to use a technique to predict bidirectional images.

A real-time occupancy monitoring system + TD-ERCS chaotic map	ROI, GMM and Kalman filter for people movement detect	Fast, low-cost computation	Speed decreases when more than one person is in the frame+ low accuracy
Lightweight encryption based on LCA	All RoIs are encrypted in a synchronously and independently	Effective, efficient and resist brute-force attacks.	Unable to resist other attacks
Ring-LWE cryptography on GPU	Performing ring arithmetic operations in parallel	Very fast	Low security
AES-CFB algorithm	Various skin colors/complexion	Good speed, simplicity and efficiency	Used with resources constrained, Different skin color reduces security.
RC4 algorithm + key generation model of chaos	Canny edge detection, H.264	High speed, compression efficiency and resistance to attacks.	Not resistant to all types of attacks, low security

4.2. Fully Encryption Techniques

This section presents the techniques used to encrypt the fully video, which has been used to increase security, but the encryption time has become larger because it focuses on fully encrypting the video. As follows:

Sowjanya and Lorraine[27], used symmetric cryptographic algorithm is Secure force algorithm that low complexity With Affine transform, Which uses basic mathematical operations such as (SWAPPING, SHIFTING, AND, OR, XOR, XNOR), This algorithm is fast, but it is less secure due to the use of simple operations in encryption.

Chang and Lin[28], used a mechanism was improved to ensure safe transmission on OCDMA networks to improve H.264 / AVC stream security and logistic map is included in the codebook to implement the variable codeword strategy based on infinite period and pseudo-

random characteristics. The results showed this method is appropriate for secure H.264/AVC streaming in a cross-layer way.

Xu and et al[29], designed a chaos pseudo-random number generator(CPRNG) to generate keystream for encrypting video elements in H.264 / AVC. The intra-prediction mode (IPM), non-zero parameter markers (NZ) and signs of trailing ones (T1s), and signs of motion vector difference (MVD) are selected. Experimental results showed that the proposed method has the ability to resist malicious attacks.

In another study by Guo and et al [30], have proposed for encrypted H.264/AVC video bitstreams, use motion detection and tracking scheme, suggest a region update (RU) algorithm. This method is used in real-time video applications Like surveillance cameras. The score of the detection, according to data, maybe as high as 0.90, and the detection rate can be as high as 100 frames per second. Represent full encryption. The proposed algorithm achieved the following results: Precision is 0.8995 and F1-score is 0.8947.

Sultana and Shubhangi [31], introduced a methodology through use of block-shuffling technology. using a shuffle algorithm with random permutation where it rotates the image at an angle after which a key based on block size is created using Faro IN OUT shuffling.

Bouslehi and Seddik [32], built new fast hyperchaotic system(FHS) with a distinct equilibrium point and increased confusion. Dynamic tests such as Poincare map(PM), Lyapunov exponents(LE), Dissipation, Lyapunov Dimension(LD) computing, and existence of an attractor were represent the topics on which he relied in mathematical analysis. It is better suited for real-time processing or FPGA implementation than other algorithms.

Alhassan and et al[33], presented a methodology for encryption perceptual video using a rotation matrix and a unit anti-diagonal matrix to visually degrade video data. In order to counteract selected or known explicit text attacks.

Giradkar and Bhattacharya [34] , proposed a new technology that consists of three parts, the first part is H.264 / AVC video encryption, the second is data embedding and the third is data extraction. RC4 algorithm was used to generates a pseudorandom key(PK) stream that is ambiguous without knowing the input key. The results prove its more difficult for cryptanalysis attacks.

Wen and et al [1], suggest a method for encrypting important video frames depend on chaotic system and DNA sequences. Through analyzing the video into frames and selecting key frame. Then the key frame is encrypted by combining DNA and random vector(VR) generated by chaotic system. Where the results showed that method has good performance to block different security threats and represents the full encryption.

Wahab and Salih[35] , used unitary matrices as cipher keys and control stream to verify whose key would be used for every block. This research works on GF (p) and encryption key sizes ranging from 3×3 to 12×12, in order to obtain a high-security encryption algorithm.

The methodology suggested by Song et al [36], was effective to encryption of quantum video, depend on XOR operations controlled by qubit_planes(qp) and enhanced logistic map(LM) in encryption steps of multilayer. Where the video frames are fully encrypted.

In another proposal, X Li and et al [37], DNA encryption algorithm and Arnold transform(AT) of Y channel were used with more information. Lorenz hyperchaotic map((LHM)) encrypts Cb and Cr channels with less information. The test result shows it cannot meet the demand in real-time.

Srivastava and et al [38], use adaptable encryption and a chaotic neural network and they propose a secure key generation method. The proposed estimation encrypts polynomial key computed using SHA with the proposed adaptable encryption. In order to enhance the authentication system before establishing the connection.

Yun and Kim[39], used a new lightweight permutation-based algorithm to encrypt video real-time on low-performance devices, as it updates the permutation list for each frame by using a secure pseudo-random number generator. Real-time on low-performance devices.

Geetha and Mahesh[40], Rijndael's algorithm is used for RGB encrypting. According to the search results, the 128-bit Rijndael symmetric algorithm was compared with RSA asymmetric key, was Rijndael performance is better than RSA in terms of speed.

Table 2. shows the previously presented fully encryption methods, explaining the techniques used and the pros and cons of each method, as follows:

Table 2. Brief description of previous fully encryption techniques.

Technologies	Focused on	Advantages	Disadvantages
RSA+PN	Dual-layer video encrypt + merge of technologies	More efficient and safer	Low speed due to RSA
RC4 algorithm, PK	Compressed video stream encryption H.264 / AVC	More difficult for cryptanalysis attacks + high speed	Low accuracy because RC4 is based on XOR + Weak to other attacks
Secure force algorithm + Affine transform	SWAPPING, SHIFTING, AND, OR, XOR, XNOR	Fast	Less secure

AES+ CTR+ chaos encryption	Building a hybrid encryption system	Efficient and a robust	Low speed due to fully encryption. to execute in real time.
(RU) algorithm	Use a motion detection and tracking scheme + bitstream and code word length.	Better speed and accuracy of detection.	Need to increase speed and precision. Precision is 0.8995 F1-score is 0.8947
OPM and Henon chaotic map	Encryption fully and permutation encryptions	Security , efficiency and immunity to noise	Low speed
FHS, FPGA	Focused on dynamic tests PM,LE, LD.	High complexity and speed, resist the brute force attack.	Need to apply the method to a real-time video to know the speed.
Chaotic system + DNA sequences	Key frame is encrypted by combining the DNA and VR	Good performance to block different security threats.	Low speed

5. Analysis and Recommendation

Content protection for digital video is a very important topic, and the best way to protect is encryption. Therefore, there are two methods that are used to encrypt digital video content, which are either fully encryption or selective encryption, where after a presentation of a group of techniques used for encryption, the results were as follows: The most important criteria used in encryption are speed and security, especially when real-time implementation is required. When fully encrypting the video, it will take more time compared to selective encryption, which takes less time because a small part of the video data is encrypted. This means that selective encryption is faster than fully encryption on the one hand speed. while, In terms of security, fully encryption is more secure because all information is encrypted rather than a part of it, as in selective encryption.So, choice of any type of encryption depends on type and need of the application used. That is, if there is a need to use it in real time or offline.

As for the algorithms, some of them use high of security but slow algorithms such as RSA and DES and others, and some use lightweight algorithms such as RC4, ChaCha. etc, that are faster but less secure. Therefore, it is possible to use the method of hybridization between

algorithms to make them more robust, high security, and be fast at the same time. This applies to lightweight algorithms that can be made more robust by strengthening them with other algorithms.

6. CONCLUSION

This paper presents a review on the basic concept of video encryption techniques for contents protection. Although, an essential and various quality of video encryption techniques have been proposed in this study, most of the techniques are vulnerable to cryptanalysis attacks. Fully encryption techniques provide more security for video, but are computationally expensive and cannot be applied in real-time because they are slow. While selective encryption-based algorithms are fast, but not provide a significant degree of video security. Selective encryption techniques reduce computational complexity because they use simple arithmetic operations such as XOR and other arithmetic operations, within encryption a small amount of information in the video. We conclude that all the techniques used were able to achieve one requirement either to increase accuracy or speed, especially encryption in real-time, so we suggest hybridization between algorithms. for the purpose of avoiding disadvantages and benefits of the advantages of each algorithm, in order to build a fast and robust algorithm that can be implemented in real-time.

REFERENCES

1. Wen, W., R. Tu, and K. Wei. Video frames encryption based on DNA sequences and chaos. in Eleventh International Conference on Digital Image Processing (ICDIP 2019). 2019. International Society for Optics and Photonics.
2. Mohsen, A.H. and S.H. Shaker, Authentication of Digital Video Encryption. Iraqi Journal of Science, 2016. **57**(4C): p. 2954-2967.
3. Ahmad, J., et al. An intelligent real-time occupancy monitoring system with enhanced encryption and privacy. in 2018 IEEE 17th International Conference on Cognitive Informatics & Cognitive Computing (ICCI* CC). 2018. IEEE.
4. Hassan, N.F. and A.R. Alawi, Review on Encryption of Video: Determination Optimal Measures for Robust Video Encryption. Journal of Al-Ma'moon College, 2020(35).
5. Obaida, T.H. and D.H. Abd, A Robust Approach for Mixed Technique of Data Encryption Between DES and RC4 Algorithm. Journal of Kufa for Mathematics and Computer Vol, 2016. **3**(2): p. 48-54.
6. Bisht, N. and S. Singh, A comparative study of some symmetric and asymmetric key cryptography algorithms. International Journal of Innovative Research in Science, Engineering and Technology, 2015. **4**(3): p. 1028-1031.
7. Oukili, S. and S. Bri, High throughput FPGA Implementation of Data Encryption Standard with time variable sub-keys. International Journal of Electrical and Computer Engineering, 2016. **6**(1): p. 298.
8. Dutta, M.P., et al., Two-way Mechanism to Enhance Confidentiality and Accuracy of Shared Information. International Journal of Electrical and Computer Engineering, 2016. **6**(4): p. 1785.
9. Karakra, A. and A. Alsadeh. A-RSA: Augmented RSA. in 2016 SAI Computing Conference (SAI). 2016. IEEE.
10. Adedeji, K.B. and A.A. Ponnle, Improved image encryption for real-time application over wireless communication networks using hybrid cryptography technique.

Indonesian Journal of Electrical Engineering and Informatics (IJEEI), 2016. **4**(4): p. 307-318.
11. Jirakitpuwapat, W. and P. Kumam. The generalized diffie-hellman key exchange protocol on groups. in International Econometric Conference of Vietnam. 2018. Springer.
12. Al-Mejibli, I. and S.F. Ismail, Innovative lightweight encryption algorithm for real-time video. Journal of Intelligent & Fuzzy Systems, 2019. **36**(3): p. 2817-2827.
13. Hamidouche, W., et al. Selective video encryption using chaotic system in the SHVC extension. in 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). 2015. IEEE.
14. Li, C., et al. A video selective encryption strategy based on spark. in 2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC). 2016. IEEE.
15. Malladar, R. and S. Kunte. Selective video encryption using Sattolo's encryption technique. in 2016 International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT). 2016. IEEE.
16. Hore, S., et al., A real time dactylology based feature extractrion for selective image encryption and artificial neural network, in Image feature detectors and descriptors. 2016, Springer. p. 203-226.
17. Unterweger, A., et al., Building a post-compression region-of-interest encryption framework for existing video surveillance systems. Multimedia Systems, 2016. **22**(5): p. 617-639.
18. Saleh, M.A., N.M. Tahir, and H. Hashim, Moving objects encryption of high efficiency video coding (HEVC) using AES algorithm. Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 2016. **8**(3): p. 31-36.
19. Sallam, A.I., O.S. Faragallah, and E.-S.M. El-Rabaie, HEVC selective encryption using RC6 block cipher technique. IEEE Transactions on Multimedia, 2017. **20**(7): p. 1636-1644.
20. Gerhardt, C., P. Aichroth, and S. Mann. Selective face encryption in H. 264 encoded videos. in 2017 IEEE Visual Communications and Image Processing (VCIP). 2017. IEEE.
21. Zhang, X., S.-H. Seo, and C. Wang, A lightweight encryption method for privacy protection in surveillance videos. IEEE Access, 2018. **6**: p. 18074-18087.
22. Tan, T.N., et al. Ring-LWE based face encryption and decryption system on a GPU. in 2019 International SoC Design Conference (ISOCC). 2019. IEEE.
23. Shifa, A., et al., Skin detection and lightweight encryption for privacy protection in real-time surveillance applications. Image and Vision Computing, 2020. **94**: p. 103859.
24. Cheng, S., et al., A selective video encryption scheme based on coding characteristics. Symmetry, 2020. **12**(3): p. 332.
25. Duong-Ngoc, P., T.N. Tan, and H. Lee, Efficient NewHope cryptography based facial security system on a GPU. IEEE Access, 2020. **8**: p. 108158-108168.
26. Alhasany, R.M. and L.M. Jawad, A NEW TECHNIQUE FOR DETERMINING REGION OF INTEREST IN SELECTIVE VIDEO PROTECTION APPROACH. Iraqi Journal of Information & Communications Technology, 2021. **4**(2): p. 33-49.
27. Sowjanya, P.L. and K.S. Lorraine, INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY IMAGE ENCRYPTION USING SECURE FORCE ALGORITHM WITH AFFINE TRANSFORM FOR WSN.

28. Chang, Y.-T. and Y.-C. Lin, Dynamic reconfigurable encryption and decryption with chaos/M-sequence mapping algorithm for secure H. 264/AVC video streaming over OCDMA passive optical network. Multimedia Tools and Applications, 2016. **75**(16): p. 9837-9859.
29. Xu, H., X. Tong, and X. Meng, An efficient chaos pseudo-random number generator applied to video encryption. Optik, 2016. **127**(20): p. 9305-9319.
30. Guo, J., P. Zheng, and J. Huang, An efficient motion detection and tracking scheme for encrypted surveillance videos. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 2017. **13**(4): p. 1-23.
31. Sultana, S.F. and D. Shubhangi, Video encryption algorithm and key management using perfect shuffle. International Journal of Engineering Research and Applications, 2017. **7**(2): p. 1-5.
32. Bouslehi, H. and H. Seddik, Innovative image encryption scheme based on a new rapid hyperchaotic system and random iterative permutation. Multimedia Tools and Applications, 2018. **77**(23): p. 30841-30863.
33. Alhassan, S., M.M. Iddrisu, and M.I. Daabo, Perceptual video encryption via unit anti-diagonal matrix. Appl. Math. Inf. Sci, 2018. **12**(5): p. 923-929.
34. Giradkar, S.S. and A. Bhattacharya. Securing compressed video streams using RC4 encryption scheme. in 2015 Global Conference on Communication Technologies (GCCT). 2015. IEEE.
35. Wahab, H.B.A. and M.A. Salih, Using Unitary Matrices in High-speed Video Encryption. IJCSNS, 2015. **15**(6): p. 92.
36. Song, X.-H., et al., Quantum video encryption based on qubit-planes controlled-XOR operations and improved logistic map. Physica A: Statistical Mechanics and its Applications, 2020. **537**: p. 122660.
37. Li, X., et al., Video encryption based on hyperchaotic system. Multimedia Tools and Applications, 2020. **79**(33): p. 23995-24011.
38. Srivastava, G., et al., Two-stage data encryption using chaotic neural networks. Journal of Intelligent & Fuzzy Systems, 2020. **38**(3): p. 2561-2568.
39. Yun, J. and M. Kim, JLVEA: Lightweight Real-Time Video Stream Encryption Algorithm for Internet of Things. Sensors, 2020. **20**(13): p. 3627.
40. Geetha, N. and K. Mahesh. Video Frame Encryption using Symmetric Algorithm. in 2020 International Conference on Communication and Signal Processing (ICCSP). 2020. IEEE.