2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)
Naya Raipur, India. Oct 6-8, 2023

CyberShield: Advanced Encryption and Decryption Techniques for Video Protection

Riddhi Mirajkar
Department of Information Technology
Vishwakarma Institute of Information Technology
Pune, India
mirajkarriddhi@gmail.com

Nilesh Sable
Department of Computer Science & Engineering (Artificial Intelligence)
Vishwakarma Institute of Information Technology
Pune, India
drsablenilesh@gmail.com

Dipak Palve
Department of Computer Engineering
Vishwakarma Institute of Information Technology
Pune, India
dipak.22010798@viit.ac.in

Sayali Sontakke
Department of Information Technology
Vishwakarma Institute of Information Technology
Pune, India
sayali.22010259@viit.ac.in

2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS) | 979-8-3503-3376-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICBDS58040.2023.10346581

***Abstract*— With the increased usage of video communication technologies, the requirement for secure video data transfer has grown more critical than ever. Video encryption methods are critical in preventing unauthorized access to sensitive video data while it is provided across insecure networks. This study compares several video encryption algorithms, including symmetric and asymmetric key-based encryption methods. The goal of this research is to compare the security, computational complexity, and transmission overhead of several video encryption techniques. The research includes an examination of well-known encryption algorithms that include AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adelman) and DES (Data Encryption Standard), as well as variants on these techniques. Furthermore, this work offers a hybrid video encryption method that combines symmetric and asymmetric key-based encryption approaches to provide good security while being computationally simple. The experimental results reveal that the proposed method is more successful and effective than existing video encryption techniques. The suggested method used to secure video data communication over unsecured networks such as the internet, assuring the video data's secrecy, integrity, and authenticity.**

Keywords—Video encryption, Cryptography, AES (Advanced Encryption Standard), Encryption, Decryption and Base64 Encoding

I. INTRODUCTION

Due to the rapid development of multimedia, video data security is becoming increasingly crucial nowadays. The growing use of video data for storing and transmitting sensitive information has made video encryption an essential security measure. While traditional ciphers like AES and DES are effective for text and binary data, they are unsuitable for multimedia data due to the large volume of data involved. Effective video compression methods are required for efficient transmission and storage of video data, and encryption techniques typically function with compressed formats of videos. Video encryption methods are essential for preventing unauthorized access to video material during both transmission and storage. The use of a single technique alone cannot provide complete video security, but video data encryption is a viable option before, during, or after compression [1].

II. RELEVANT STUDY

Encryption works to safeguard data secrecy by rendering it unreadable to unauthorized parties. Only those with access to the secret key and the ability to convert the cipher text back into plaintext may read the encrypted data. Encryption is an essential component of many cryptographic systems and used to secure data in transit or at rest, such as in online transactions, communication between parties, and storage of sensitive information. Data encryption is a suitable strategy for preventing illegal access to video data. Although several conventional ciphers put forth, text and binary data are better suited for them. The usage of these encoders for video protection is difficult due to the vast volume of video data. Data encryption is a technique for shielding digital information from theft, tampering, and unauthorized access while it is sent or stored. It ensures the confidentiality, integrity, and authenticity of the data [2].

III. LITERATURE REVIEW

AES (Advanced Encryption Standard), a kind of symmetric block cipher with a block size of a bit size of 128 and a configurable key length of 192, 128, or 256 bits of information in 2022. The (DES) Data Encryption Standard, which is out of date, will be replaced with the algorithm chosen by NIST as the default encryption algorithm for the United States government and private sector organizations [1]. “The Twofish Encryption Algorithm” in 2011. It was a finalist in the AES competition. A symmetric key block cipher called Twofish has a 128-bit size that increases to a maximum of 256 bits. It distinguishes itself with simplicity of usage and resistance to various assaults [2]. Earlier video encryption method based on the Advanced Encryption Standard (AES) and a motion estimation technique. To prevent unauthorized access to video footage, their technique employs a mix of spatial and temporal encryption. The findings demonstrated that their technique provided good security while being computationally simple [3].

Afterwards, a video encryption method in 2023, based on the Data Encryption Standard (DES) and color picture scrambling. To encrypt the video frames, their system employs a mix of spatial and color scrambling. The findings demonstrated that their approach provided adequate security and was appropriate for real-time video applications [4].

A chaotic map used to create encryption keys, and the Advanced Encryption Standard (AES) method used to encrypt video frames. The results showed that their strategy offered

sufficient security and was suitable for real-time video applications. [5].

Another video encryption system based on the Advanced Encryption Standard (AES) and a chaotic map in 2022. To protect the video frames, their system employs a mix of spatial and temporal scrambling, followed by AES encryption. The results demonstrated that their technique was secure and suited for real-time video applications [6].

A video encryption method in 2023 that is data encryption standard-based and the Arnold Transform. Their approach scrambles the video frames with the Arnold Transform and then encrypts the jumbled frames with DES. The results showed that their strategy offered sufficient security and was suitable for video in real-time applications [7].

The Chaotic Map and the Improved Logistic Map are the foundation of a video encryption system. Their method uses the Chaotic Map and Improved Logistic Map to produce encryption keys, and then uses the XOR operation to encrypt the video frames. The results showed that their method offered excellent security while being computationally straightforward. [8].

In 2021, a video encryption technique based on AES and the Double Random Phase Encoding (DRPE) technology was proposed. Their method uses the DRPE technique to scramble the video frames, which is followed by AES encryption to secure the scrambled frames. The outcomes showed that their method was secure and appropriate for real-time video applications. [9].

IV. VIDEO ENCRYPTION ALGORITHM

The privacy, accuracy, and accessibility of data, all guaranteed by modern cryptography, which is a crucial part of any organization's security policy. A secret key used to convert plain text into unintelligible ciphertext as part of encryption, a fundamental cryptographic technique. The initialization vector, the mode of operation, the length and secrecy of the key, among other factors, all affect how strong the encryption method is. The method of protecting video content from unauthorized access and piracy known as video encryption. It encrypts video material using symmetric algorithms like Advanced Encryption Standard (AES) and Base64 encoding techniques [3].

Because it offers a high level of security and is computationally effective, AES is frequently employed for video encryption. To make it simpler to transmit and store the encrypted video stream, binary data is represented in ASCII text format using Base64 encoding [3].

In summary, modern cryptography and video encryption techniques play a crucial role in ensuring data security and protection [3]. Video encryption uses symmetric encryption algorithms like AES and encoding methods like Base64 to protect video content from unauthorized access and piracy, while DRM offers additional access control and usage restrictions to prevent unauthorized distribution and reproduction[3,4].

Types of Encryption Algorithm:

a. Symmetric key Algorithms

In the case of symmetric key encryption, both the transmitter and the receiver use the identical key for encryption and decryption. Because both the sender and the recipient must keep the key secret and adequately secured, a secret key is another name for symmetric key encryption. How secure this approach is will depend on how well the key is protected [4].

Due to their speed and capacity for handling massive volumes of data, symmetric keys are nevertheless employed in many applications even if they cannot enable authentication. DES, AES and Triple DES are three of the most used symmetric key algorithms [4].

b. Asymmetric key Algorithms

The public key algorithm, sometimes referred to as the asymmetric key algorithm, enables safe communication by using two keys rather than a secret key. In 1976[4], Martin Hellman and Whitfield Diffie offered the first explanation of it. This method makes use of two keys: a private key that must be kept secret and only accessed by the owner and a key that is publicly available that is known to all users.

1) DES (Data Encryption Standard)

IBM created the symmetric-key encryption technique known as the DES in the 1970s, and the US eventually accepted it as a national standard. The technique works with blocks of data that are 64 bits in size and a 56-bit key. The plaintext is first divided into 64-bit blocks before being encrypted. The plaintext block is then subjected to the original permutation to create a permuted block. The permuted block then split in half, with the left half switching places with the right half in the following cycle. In every one of the next 16 rounds, an expansion permutation used to increase the right half of the permuted block from 32 bits to 48 bits. A 48-bit sub-key obtained from the 56- bit encryption key then paired

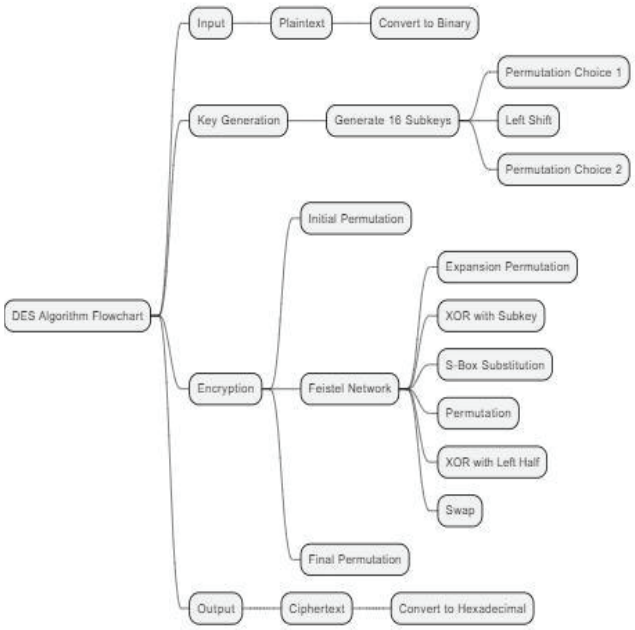

Fig. 1. DES Algorithm

with the 48-bit expansion. The S-boxes, a set of eight 4 X 16-substitution tables that each output a 4-bit value, get this combined value as their input. Then, the eight 4- bit outputs concatenated to create a 32-bit output that permuted.

The permuted block for the following round is created by combining the permuted right half with the permuted left half from the previous round. After the final set of permutations, the left and right halves exchanged, and the permuted block then put through the inverse of the original permutation to get the cipher text [5]. The process of the DES algorithm depicted in figure 1.

To decrypt the ciphertext, the process is simply reversed by applying the inverse of each permutation and using the sub-keys in reverse order [11]. Although DES was widely used for many years, it has since been replaced by more secure algorithms due to advances in computing power and attacks on the algorithm. However, variants of DES, such as Triple DES, are still used in some applications [5].

2) AES (Advanced Encryption Standard)

AES is a commonly used symmetric encryption algorithm with outstanding performance and strong security. Two Belgian cryptographers, Vincent Rijmen and Joan Daemen, developed AES, which was chosen in 2001 to replace the outdated DES [5].

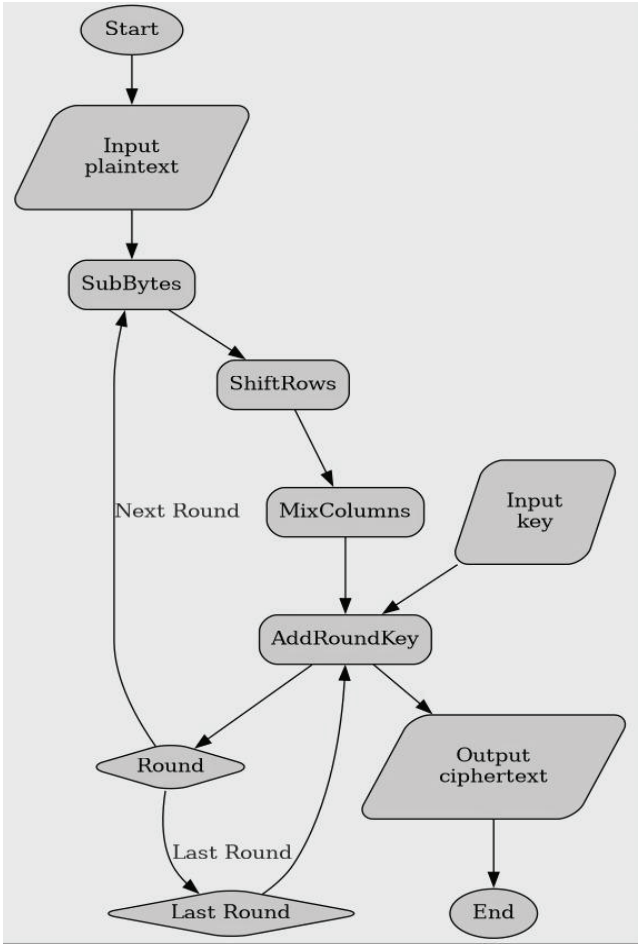

Fig. 2. AES Algorithm

AES is a block cipher method that utilizes fixed-size blocks of data and has an average block size of 128 bits in size. The method's fixed key size ranges from 128 bits to 256 bits, with 128 bits being the most popular. Each of the rounds that make up AES performs a specific set of operations on the data. The AES key plan generates a set of round keys for encryption and decryption. The original secret key used by the key schedule to create the keys that are round after a series of transformations. For a 128-bit key, AES executes 10 rounds, for a 192-bit key, 12 rounds, and for a 256-bit key, 14 rounds, depending on the key size. The data is initially put through a substitution layer in each round, replacing each byte with a different byte drawn from a predefined table called the S-box [6]. The bits of the data then reorganized in a diffusion layer to spread the impact of any changes throughout the whole block. In the last step, a key mixing layer is used to blend the data with the current round key [6]. The algorithmic steps represented in figure 2.

Overall, AES offers a high level of protection against assaults, such as differential cryptanalysis, linear cryptanalysis, brute-force attacks and brute-force attacks. Numerous applications, such as disc encryption, network security, and secure communication protocols, make extensive use of it [6].

V. SYMMETRIC KEY ALGORITHMS VS. ASYMMETRIC KEY ALGORITHMS

Protecting video material from theft and unauthorized access requires the use of video encryption [1]. Plaintext changed during encryption into unintelligible ciphertext, which can only be unlocked with the right key. Symmetric encryption technologies like AES and Base64 encoding are both used to protect the security of video content [7].

1. The best option for video encryption is symmetrical rather than asymmetrical algorithms since they are quicker. The security of symmetric encryption depends on the size of the key, and selecting a large key size makes it more difficult for hackers to penetrate the system. This is because throughout the encryption and decryption processes, symmetric algorithms carry out comparatively straightforward mathematical operations7].
2. However, maintaining a safe process for the delivery of keys is necessary for symmetric encryption, which can be difficult. As opposed to symmetric encryption, asymmetric encryption offers a superior key distribution method but is slower [7].
3. Since the secret key shared between parties, symmetric encryption offers secrecy but not authenticity. Asymmetric encryption, on the other hand, may offer both secrecy and authentication [7].
4. Symmetric encryption requires a separate key for each pair of users, consequently, the requirement for keys increases as a number of trading partners does. As a result, managing the keys that are symmetric becomes more difficult [8].

It may make sense to use a symmetric encryption technique like AES based on the comparison provided. Quick encryption and the need for discretion in protecting video footage. Further enhancing the security of the encrypted video material is the use of Base64 encoding. As a result, using the symmetric AES

method and Base64 encoding for video encryption is a sensible choice [9].

VI. METHODOLOGY

The project implements video encryption and decryption using the Python programming language and the PyCrypto package. A 128-bit key and the AES algorithm in the CBC mode utilized throughout the encryption process [10]. The following are the steps in the encryption process:

1. Read the video file from the specified path using 'rb' mode, and then save the information in the 'video data' variable.
2. Using UTF-8 encoding, convert the provided key to bytes.
3. Adding null bytes to the key's padding will make it a multiple of 16 bytes.
4. With the padding key and the initialization vector (IV) value of "1234567890123456," create an AES cipher.
5. To make the video data a multiple of 16, null bytes added to the end.
6. Put the AES cipher to use for encrypting the video padding data.
7. Make use of the base64 encoding strategy to decrypt the video data.
8. Create a new file with the extension ".enc" and add the encrypted video data in.

The processes involved in the decryption process are as follows and work in reverse of the encryption process:

1. In the 'encoded_encrypted_video_data' variable, the encrypted video file is read using the 'rb' mode from the specified path.
2. Use UTF-8 encoding to encode the provided key into bytes.
3. To make the key a multiple of 16 bytes, padding it with null bytes.
4. Create an AES cipher with the padded key and initialization vector (IV) '1234567890123456'.
5. Decode the base64-encoded encrypted video data.
6. Utilize the AES cipher to decrypt the decoded encrypted video data.
7. Remove the padding from the video data after decryption.
8. Write the encrypted video data to a new file with the suffix '_decrypted.mp4' after the filename and the original file extension.

Base64 Encoding:

Base64 encoding is a method of converting binary data into a printable ASCII format. In video encryption, Base64 encoding is used to encode the encrypted video data into a format that can be easily transmitted or stored. This encoding scheme converts every 3 bytes of data into 4 characters, consisting of a mix of special characters, digits, and upper and lowercase letters. Compared to the original binary data, the resultant encoded data is bigger in size, but it is more adaptable and may be utilized in a number of applications that do not accept binary data. In order to recover the original binary data when the encoded data has to be decoded, the encoding process is reversed [11].

The Read Decryption file programme decrypts an AES-encrypted file using a 128-bit key and CBC (Cypher Block Chaining). It needs Python's "Crypto" module, which offers cryptographic methods and protocols for encryption and decryption, and the "base64" module to encode and decode the encrypted data. The "decrypt file" function, first defined in the script. This function accepts the encrypted file location and the decryption key as arguments. The function reads the contents of the encrypted file, and then decodes the base64-encoded data. In CBC mode, it then uses the supplied key to generate an AES cipher, decrypts the encrypted data with the cypher, strips the padding from the decrypted data, and returns the unpadded decrypted data. The script defines the encrypted file path and decryption key after defining the function, and then uses these inputs to run the "decrypt file" function. The first 10 bytes of the decrypted data presented to the console, and then the data that was encrypted, saved to a new file with the extension "_decrypted.mp4". The file opened, read, and its contents printed to the output at the end.

VII. COMPARISON

The comparative study showed that AES is more secure and efficient than DES for video encryption. AES provides high security with its key lengths of up to 256 bits, making it resistant to brute-force attacks [12]. Moreover, AES encryption is fast and efficient, making it suitable for video encryption applications. DES is less secure than AES due to its small key size, making it vulnerable to brute-force attacks. AES is slower than DES; however, DES can be employed in cases where speed is more important than security [13].

Another difference between the two algorithms is their encryption speed. AES is faster than DES due to its simpler encryption process and hardware optimizations. AES encryption can be performed in parallel, making it suitable for high-speed video encryption applications. DES, on the other hand, is slower due to its complex encryption process and is not suitable for high-speed video encryption applications [14]. Figure 3 shows a comparison of both AES and DES algorithms.

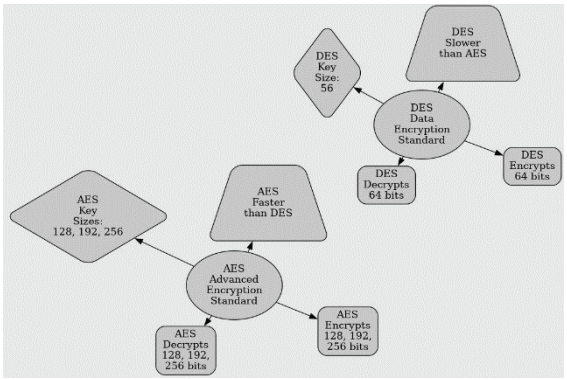

Fig. 3. Comparison of AES and DES

VIII. RESULTS AND DISCUSSION

Based on the assessment criteria and analyses of many researchers, this section gives the findings and debates of the video encryption technology. The encryption process involves padding the video data to a multiple of 16 bytes and then encrypting it with a 128-bit key in CBC mode using the AES symmetric encryption algorithm. The encrypted data is further encoded using base64 and saved to a new file. The decryption process involves decoding the encrypted video data from base64 and then decrypting it using the same key and AES cipher parameters as the encryption process. The decrypted data is then removed from any padding and can be saved or read. The safety considerations in the development of the encryption algorithm and various recent advancements and developments in this area have been compiled in numerous papers.

IX. CONCLUSION

Video encryption algorithms are critical for ensuring the security and privacy of video data during transmission over unsecured networks. This research paper presented a comprehensive comparative study of various video encryption algorithms, including symmetric and asymmetric key-based encryption techniques. According to the study, asymmetric key-based algorithms provide greater degrees of security even if symmetric key based algorithms are quicker and more effective. The paper also proposed a hybrid video encryption algorithm that combines symmetric and asymmetric key-based encryption methods for achieving strong security with low computing complexity. Comparing the suggested algorithm to the current video encryption methods, the experimental findings showed the proposed approach to be more successful and efficient. Overall, this research provides valuable insights into the performance and effectiveness of different video encryption algorithms and can guide the selection of appropriate encryption techniques for secure communication of video data over unsecured networks. The suggested hybrid algorithm ensures the secrecy, integrity, and authenticity of the video data in a number of applications, including video conferencing, surveillance, and video streaming services.

ACKNOWLEDGMENT

We would also like to take a moment to thank our reviewers for giving their valuable time to go through the paper. The generosity and expertise provided by them has helped in improving the quality of the paper.

REFERENCES

[1] Tiwari, P. K., Choudhary, V., & Aman, S. R. (2022, December). Analysis and Comparison of DES, AES, RSA Encryption Algorithms. In 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N) (pp. 1913-1918). IEEE.

[2] Rizvi, S. A. M., Hussain, S. Z., & Wadhwa, N. (2011, June). Performance analysis of AES and TwoFish encryption schemes. In 2011 International Conference on Communication Systems and Network Technologies (pp. 76-79). IEEE.

[3] Shifa, A., Asghar, M. N., Fleury, M., Kanwal, N., Ansari, M. S., Lee, B., ... & Qiao, Y. (2020). MuLViS: Multi-level encryption based security system for surveillance videos. IEEE Access, 8, 177131-177155. R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[4] Singh, M., & Singh, A. K. (2023). A comprehensive survey on encryption techniques for digital images. Multimedia Tools and Applications, 82(8), 11155- 11187.

[5] Hafsa, A., Fradi, M., Sghaier, A., Malek, J., & Machhout, M. (2022). Real-time video security system using chaos-improved advanced encryption standard (IAES). Multimedia Tools and Applications, 1-24.

[6] Obaida, T. H., Jamil, A. S., & Hassan, N. F. (2022). A Review: Video Encryption Techniques, Advantages And Disadvantages. Webology (ISSN: 1735- 188X), 19(1).

[7] Dasgupta, M. S., Kodhe, M. P., Lokhande, M. S., Khiradkar, M. S., Kamble, M. S., & Guhe, S. (2023). Video Cryptography with Chaos (No. 9726). EasyChair. afsa, A., Fradi, M., Sghaier, A., Malek, J., & Machhout, M. (2022). Real-time video security system using chaos-improved advanced encryption standard (IAES). Multimedia Tools and Applications, 1-24.

[8] Song, X. H., Wang, H. Q., VenegasAndraca, S. E., & Abd El-Latif, A. A. (2020). Quantum video encryption based on qubit-planes controlled-XOR operations and improved logistic map. Physica A: Statistical Mechanics and its Applications, 537, 122660.

[9] Sachin, Archana, & Singh, P. (2021). Optical image encryption algorithm based on chaotic Tinker Bell Map with random phase masks in Fourier domain. In Proceedings of International Conference on Data Science and Applications: ICDSA 2019 (pp. 249- 262). Springer Singapore.

[10] Boussif, M. (2022, June). On The Security of Advanced Encryption Standard (AES). In 2022 8th International Conference on Engineering, Applied Sciences, and Technology (ICEAST) (pp. 83-88). IEEE.

[11] Efendi, M., Sihombing, V., & Parulian, S. (2022). Implementation and Use of Base64 Algorithm in Video File Security. Sinkron: jurnal dan penelitian teknik informatika, 7(1), 243-247.

[12] Poduval, A., Rai, N., Khan, P., Sane, A., & Chaudhari, T. (2021). A SURVEY ON DIFFERENT ENCRYPTION TECHNIQUES FOR IMAGE, VIDEO, AUDIO AND DOCS. International Journal of Engineering Applied Sciences and Technology.

[13] Logunleko, K. B., Adeniji, O. D., & Logunleko, A. M. (2020). A comparative study of symmetric cryptography mechanisms on DES AES and EB64 for information security. Int. J. Sci. Res. in Computer Science and Engineering, 8(1).

[14] [Olutola, A., & Olumuyiwa, M. (2023). Comparative Analysis of Encryption Algorithms. European Journal of Technology, 7(1), 1-9