End-To-End Cybersecurity Encryption- Video Algorithm

OBAIDA M. AL-HAZAIMEH[1,*], MA'MOUN A. AL-SMADI[2], TARIK ABUAIN[3], ASHRAF A. ABU-EIN[4]

[1]Department of Computer Science and Information Technology,
Al-Balqa Applied University,
Al-Huson University College, Irbid-21510,
JORDAN

[2]Department of Electrical Engineering,
Al-Balqa Applied University,
Al-Huson University College, Irbid-21510,
JORDAN

[3]College of Computing and Informatics,
Saudi Electronic University,
Riyadh 11673,
SAUDI ARABIA

[4]Department of Electrical Engineering,
Al-Balqa Applied University,
Al-Huson University College, Irbid-21510,
JORDAN

**Corresponding Author*

Abstract: - Recently, digital content transmission has advanced significantly. For data transfer security, video encryption is essential. As multimedia technology improves, its importance grows. This paper proposes a secure and effective video encryption method. The proposed technique uses symmetric key cryptography and audio samples to avoid a trusted third party in the key exchange. To establish sender-receiver communication, the method broadcasts the public table to all participants. The device's MAC address determines the rotation operations required to create the private table. Thus, only the sender and receiver share the private table. The new approach splits processed footage into audio samples and video frames. We encrypt the video frame and audio sample using the generated private key to create cipher data. Next, we randomly insert the audio sample into the encrypted data. The recipient will first extract the audio sample from the encrypted data and then decrypt it. The findings show that the technique can maximize the tolerance skew value to close to the optimal value, and the average time required to encrypt the video packet using the proposed technique is relatively small, specifically 0.685429814 milliseconds (i.e., "end-to-end delay time"). The findings showed that the proposed technique performs effectively in real-time and practical video transmission.

Key-Words: - Multimedia, cybersecurity, cryptography, audio samples, cryptanalysis, video encryption.

Received: April 11, 2024. Revised: October 9, 2024. Accepted: November 21, 2024. Available online: December 21, 2024.

1 Introduction

Cryptography protects information from unauthorized access by transforming it into an unrecognizable form during storage and transmission. Cryptography involves scrambling data information, such as audio, images, text, and video, to render it unreadable or incoherent during transmission or storage, known as encryption. The primary goal of cryptography is to secure data from unauthorized access. Data encryption is the opposite of data encryption, which restores the original data. Key events that affected information handling have evolved and influenced cryptography since its inception in ancient Egypt. By disabling the German Enigma cipher machine, which encrypts military communications, cryptography helped the Allies

win the war faster during World War II. To secure data while it travels over public networks (i.e., the Internet), cryptography is one of the methods utilized. It entails sending information in an unintelligible form. One problem with this method is that the majority of encryption algorithms used for both encryption and decryption were only ever designed to deal with text data. As a result, multimedia technologies (such as video conferencing, Pay-Tv, and video broadcast) are inappropriate for these algorithms, [1], [2], [3]. In most cases, digital multimedia material will consist of text, some visual elements (i.e., frames), and audio clips (i.e., samples), [4]. As a means of safeguarding these types of digital multimedia materials, software-based security solutions offer answers that can maintain read/write access to data, providing a robust defense against intrusion. It is possible to classify cryptographic algorithms as either asymmetric or symmetric keys, [5], [6]. For the purpose of this paper, we employ symmetric key cryptography since it is an appropriate encryption method for digital multimedia content in particular. Figure 1 illustrates the classification of multimedia encryption. There are three main categories of multimedia encryption algorithms, each tailored to a certain type of encrypted multimedia file: images, audio, and video, [7], [8], [9].

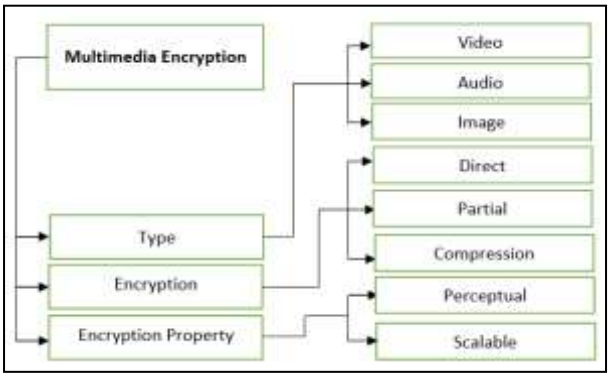

Fig. 1: Classification of Multimedia Encryption

There are four main categories of video encryption techniques, as shown in Table 1: fully encrypted, permutation encrypted, selective encrypted, and perceptual encrypted, [7], [8], [9], [10].

Video encryption is often seen as a more intricate procedure than text and voice encryption. Hence, recognizing its significance in real-world applications, researchers in the field of encryption have recently focused their endeavors on discovering and refining robust and meticulously designed techniques capable of effectively addressing the various challenges and complexities typically encountered during the process of video separation, [11], [12]. In this paper, we have introduced a novel video encryption algorithm that eliminates the necessity for a trusted third party to administer and distribute keys. The digital multimedia that is transmitted over an insecure channel (i.e., the Internet) is encrypted using the private key that is generated. On average, the proposed algorithm encrypts a video frame in a substantially shorter amount of time than the most advanced secure video encryption algorithms.

Table 1. Video Encryption Algorithms – Classification

Category	Description
Fully Encrypted	The algorithms function by initially compressing the entire video and subsequently encrypting the video data using a standard algorithm such as AES, DES, RC4, or 3-DES. However, as previously stated, these methods are time-consuming due to the intricate computational processes involved. Thus, these methods are unsuitable for such encryption requirements [10], [13].
Permutation Encrypted	The video material, including text-data, images, and audio, is encrypted using several permutation techniques (i.e., scrambling) [8], [14].
Selective Encrypted	This approach exclusively encrypts a specific video byte based on any of the conventional algorithms. This algorithm operates on the premise that certain components of video content are non-essential (i.e., I frames, video stream headers). Consequently, the encryption time will be reduced in comparison to fully encrypted techniques [1], [10].
Perceptual Encrypted	These algorithms enable the video to be accessible and permissible for others to listen to or watch, although with low-quality versions [14], [15].

2 Related Works

Numerous methodologies have suggested authentication, encryption, and digital signatures to ensure the security of data transmission over the internet. Proposed cryptographic techniques for video encryption include the AES (Advanced Encryption Standard), SDES (Simplified Data Encryption Standard), MAES (Modified Advance Encryption Standard), and RC4, [1], [16]. Table 2 displays video encryption approaches as well as a list of selected papers for each category.

Table 2. Representative Work in Vision- Video Encryption Algorithms

Reference	Year	Algorithm	Disadvantages
[15]	2018	AES, 3DES	High End-To-End delay time
[11]	2005	AES with OFB mode	High End-To-End delay time
[12]	2006	AES, DES	High End-To-End delay time.
[16]	2007	RCME and BCME	High End-To-End delay time
[13]	2012	Chaos cryptography	High End-To-End delay time in large scale.
[17]	2020	DCT coefficients - Flipping signs	-
[18]	2023	PRNG and XOR operation	Low Security level.
[19]	2020	Coding Characteristics	Low Security level.
[20]	2020	Chaos cryptography	High End-To-End delay time in large scale.
[21]	2021	Chaos cryptography	High End-To-End delay time.
[22]	2023	Chaos - based multiplexing	High End-To-End delay time.
[23]	2023	CHAOTIFICATION model	Low Security level.
[24]	2022	Chaos cryptography	High End-To-End delay time.

3 Proposed Video Encryption Algorithm

The proposed technique aims to introduce a novel method for encrypting and decrypting complex data using parallel programming. This approach leverages the capabilities of multi-core processors to deliver enhanced speed and a greater level of security. Algorithm 1 outlines the many stages of the proposed video encryption method.

- Step 1: The process begins with the sender and receiver exchanging MAC addresses; depending on the MAC address's value, numerous rotations and shifts are executed at the sender and receiver ends, turning the public table accessible to all parties into a private table exclusive to the sender and receiver.
- Step 2: Audio samples and video frames from each other via video splitting.
- Step 3: Generating encrypted data (i.e., cipher data) by performing an XOR operation between the audio sample and the video frames
- Step 4: The private table integrates the audio sample into the encrypted data, resulting in encrypted data that includes the audio sample.
- Step 5: Repeat steps 3 and 4 to ensure the encryption of all video segments.

Figure 2 (Appendix) shows a detailed representation of the video crypto-system. Nevertheless, the parameters of the proposed crypto-system can decipher the ciphered video elements by reversing the sequence of Algorithm 1.

4 Experimental Results

We analyzed video data with a frame rate of 30 frames per second and a variety of resolutions, each with unique motion characteristics. Fast and Furious and Scream VI are among the example test video sequences. In Figure 3, you can see a few of the test videos alongside their respective frame numbers. After performing an XOR operation with audio samples, Figure 4 displays the associated video frames' visuals. After applying the proposed technique, Figure 5 displays the matching images and frame numbers of some of the test videos. The encryption process erases all the details in the video block. On average, each video spends 0.008031 milliseconds in the pre-processing stage of the suggested algorithm, which is connection establishment. This rare occurrence will not influence the encryption time of the video. We conducted experiments involving the suggested encryption algorithm on a 2.40 GHz core i5 (TM) with 8.00 GB of memory and 1-TB of hard drive capacity, using the DALI library and the MATLAB application tool. This library enables the digital video coding standards (i.e., “MPEG-1 and MPEG-2”).

(a) *(b)* *(c)*
(d) *(e)* *(f)*

Fig. 3: Test Video

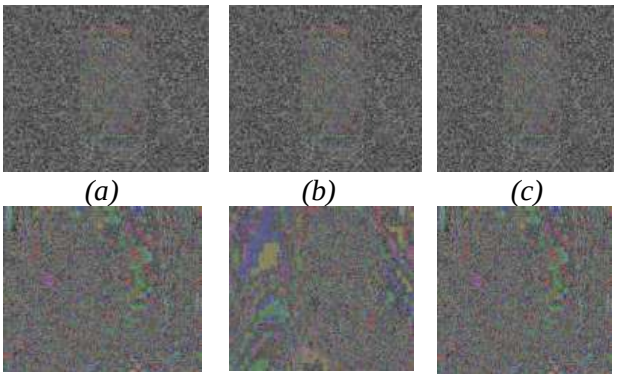

Fig. 4: Ciphered Data - Corresponding Data

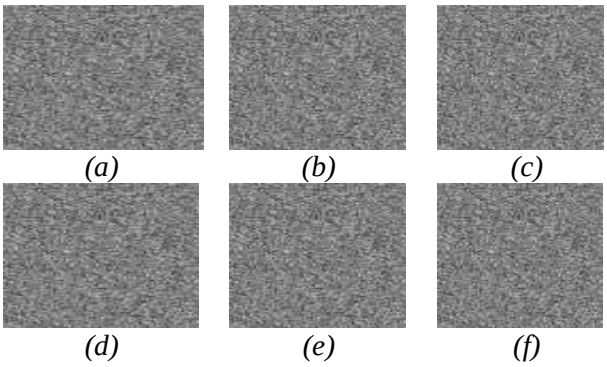

Fig. 5: Ciphered Data with Inserted Audio Samples - Corresponding Data

5 Security Analysis

This study intends to offer a novel and reliable video encryption technique that enhances video encryption performance while reducing the security level. This section provides a comprehensive examination of the security measures. We conducted a series of tests and analyses to evaluate the security of the proposed algorithm. The security analysis of the proposed algorithm was performed in two stages: the phase of distributing encrypted data and the phase of ciphered data with an inserted audio sample.

The relationship between various kinds of data is referred to as intrinsic characteristics [25], [26], [27]. As previously stated, the presence of this functionality enables attackers to track both the public and secret tables. Correlation analysis is commonly employed to assess the security and correlation of data [28], [29]. In order to examine the relationships between the public and private tables, Equation (1) is employed to compute the correlation coefficients in the horizontal, vertical, and diagonal orientations [7], [30], [31].

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)\big(y_i - E(y)\big)\ , r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \quad (1)$$

Table 3 displays the computed correlation coefficients for the public and private tables along the vertical, horizontal, and diagonal axes.

Table 3. Public and Private Tables – Correlation

Direction	Public	Private
Vertical	1.00	0.0315
Horizontal	1.00	- 0.0890
Diagonal	1.00	- 0.0725

The three-dimensional coefficients for the public table are 1.00, whereas those for the private table are nearly zero, as shown in Table 3. The results demonstrate that the public and private tables are unrelated. The complex 2-D array is constructed utilizing diffusion, confusion, and repeated iteration using the private key received from the MAC address, as previously mentioned in the suggested approach. Presented below are two arrays. Data is initially stored in the array, which subjected to a conventional XOR and iterative processing for both audio and video frames. We create the second array by inserting audio samples into a technique that creates encrypted data. As shown in Figure 7 and Figure 8, we analyzed the relationship between the two arrays using a correlation distribution.

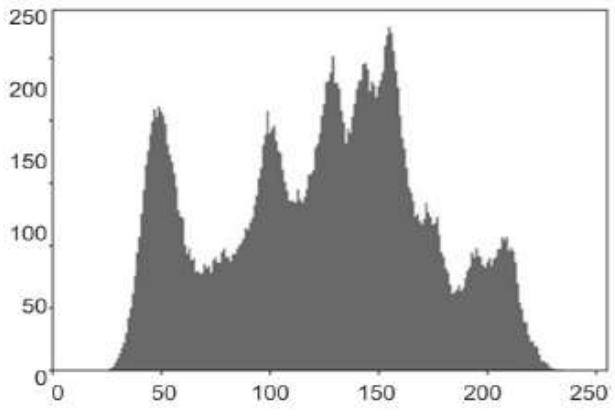

Fig. 6: Correlation Distribution – Plain-text Data

It is evident from Figure 7 and Figure 8 that the plain text data features seen in Figure 6 have vanished and been distributed. This suggests that the proposed algorithm is secure against cryptanalysis attacks and has high performance.

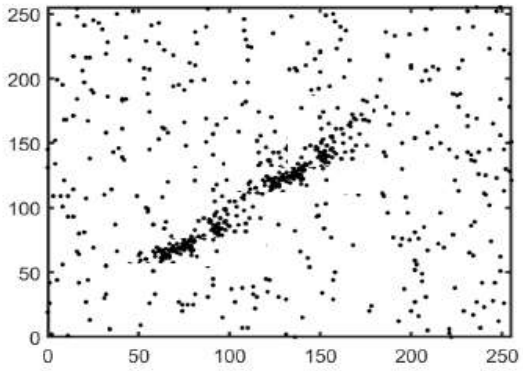

Fig. 7: Correlation Distribution – Ciphered Data

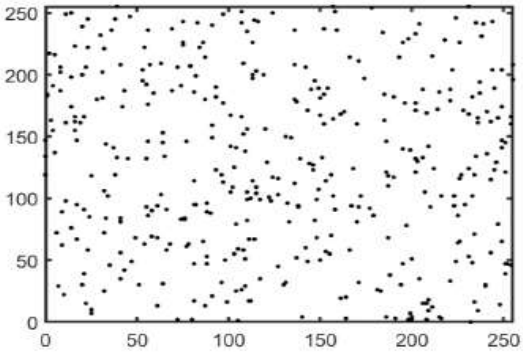

Fig. 8: Correlation Distribution – Ciphered Data with Inserted Audio Sample

6 Conclusion and Future Work

This research developed a video security cryptographic encryption algorithm using image frames and audio samples. Many text-based encryption techniques are too computationally intensive for real-time applications. Thus, video encrypts video data and randomly combines voice samples and image frames using a simple XOR algorithm to reduce computing cost and increase video security. The algorithm passed correlation analysis and other security tests, making it strong and safe. The average time required to encrypt the video packet using the suggested technique is relatively small, specifically 0.685429814 milliseconds. This suggests that real-time applications, such as video conferencing, can effectively utilize it. In future work, we aim to develop a new method to obfuscate and neutralize the public table without relying on MAC addresses in order to enhance the overall security level.

References:

[1] M. Kumar, J. Aggarwal, A. Rani, T. Stephan, A. Shankar, and S. Mirjalili, "Secure video communication using firefly optimization and visual cryptography," *Artificial Intelligence Review,* pp. 1-21, 2022, http://doi.org/10.1007/s10462-021-10070-8.

[2] A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq, and J.-J. Quisquater, "Overview on selective encryption of image and video: challenges and perspectives," *Eurasip Journal on information security*, vol. 2008, p. 179290, 2008, http://doi.org/10.1155/2008/179290.

[3] D. Zhu, J. Zheng, H. Zhou, J. Wu, N. Li, and L. Song, "A hybrid encryption scheme for quantum secure video conferencing combined with blockchain," *Mathematics*, vol. 10, p. 3037, 2022, http://doi.org/10.3390/math10173037.

[4] S. Suguna, V. Dhanakoti, and R. Manjupriya, "A study on symmetric and asymmetric key encryption algorithms," *Int Res J Eng Technol (IRJET),* vol. 3, pp. 27-31, 2016.

[5] I. Aribilola, M. N. Asghar, N. Kanwal, M. Fleury, and B. Lee, "Securecam: Selective detection and encryption enabled application for dynamic camera surveillance videos," I*EEE Transactions on Consumer Electronics*, vol. 69, pp. 156-169, 2022, http://doi.org/10.1109/TCE.2022.3228679.

[6] M. A.-H. Obaida, "Combining audio samples and image frames for enhancing video security," *Indian Journal of Science and Technology,* vol. 8, p. 940, 2015, http://doi.org/10.17485/IJST/2015/V8I10/53149.

[7] B. Furht, E. Muharemagic, and D. Socek, *Multimedia encryption and watermarking* vol. 28: Springer Science & Business Media, 2006.

[8] K. J. Singh and K. Gagneja, "Overview of securing multimedia content using efficient encryption methods and modes," *International Journal of Advanced and Applied Sciences,* vol. 4, pp. 84-96, 2017, http://doi.org/10.21833/IJAAS.2017.010.013.

[9] O. M. Al-Hazaimeh, "A new dynamic speech encryption algorithm based on Lorenz chaotic map over internet protocol," *International Journal of Electrical and Computer Engineering,* vol. 10, pp. 4824, 2020, http://doi.org/ 10.11591/ IJECE. V10I5. PP4824-4834.

[10] S. Li, "Perceptual encryption of digital images and videos," *Perceptual Digital Imaging: Methods and Applications,* vol. 14, pp. 431-468, 2012.

[11] J. M. Rodrigues, William Puech, Peter Meuel, Jean-Claude Bajard, and Marc Chaumont,

"Face protection by fast selective encryption in a video," pp. 420-425, 2006, *2006 IET Conference on Crime and Security, London, UK*, 13-14 June 2006, Print ISBN:0-86341-647-0.

[12] K. Hong and K. Jung, "Partial encryption of digital contents using face detection algorithm," in *Pacific Rim International Conference on Artificial Intelligence*, 2006, pp. 632-640.

[13] S. M. M. Rahman, M. A. Hossain, H. Mouftah, A. El Saddik, and E. Okamoto, "Chaos-cryptography based privacy preservation technique for video surveillance," *Multimedia systems,* vol. 18, pp. 145-155, 2012, http://doi.org/ 10.1007/s00530-011-0246-9.

[14] O. Goldreich, "Foundations of Cryptography: Basic Tools, Cambridge U," ed: Press, 2001.

[15] T. E. Boult, "Pico: Privacy through invertible cryptographic obscuration. In: Computer Vision for Interactive and Intelligent Environment (CVIIE'05)," *IEEE,* pp. 27-38, 2005, Lexington, KY, USA.

[16] Q. Meibing, C. Xiaorui, J. Jianguo, and Z. Shu, "Face protection of h. 264 video based on detecting and tracking," in *2007 8th International Conference on Electronic Measurement and Instruments*, 2007, pp. 2-172-2-177, http://doi.org/ 10.1109/ICEMI.2007.4350647.

[17] P. Zhang, T. Thomas, and S. Emmanuel, "Privacy enabled video surveillance using a two state Markov tracking algorithm," *Multimedia systems,* vol. 18, pp. 175-199, 2012, http://doi.org/ 10.1007/s00530-011-0247-8.

[18] J. Guo, Jia-yun Xu, and Jia-li Bao, "Region of interest based selective encryption scheme for privacy protection in h. 264 video," *Journal of Shanghai Jiaotong University (Science)* vol. 19, pp. 385-391, 2023, http://doi.org/ 10.1007/s12204-014-1513-7.

[19] S. Cheng, L. Wang, N. Ao, and Q. Han, "A selective video encryption scheme based on coding characteristics," *Symmetry,* vol. 12, p. 332, 2020, https://doi.org/10.3390/sym12030332.

[20] H. Elkamchouchi, W. M. Salama, and Y. Abouelseoud, "New video encryption schemes based on chaotic maps," *IET Image Processing,* vol. 14, pp. 397-406, 2020, http://doi.org/ 10.1049/iet-ipr.2018.5250.

[21] X. Huang, D. Arnold, T. Fang, and J. Saniie, "A chaotic-based encryption/decryption system for secure video transmission," in *2021 IEEE International Conference on Electro Information Technology (EIT)*, 2021, pp. 369-373. United States.

[22] H. Wen, Y. Lin, Z. Xie, and T. Liu, "Chaos-based block permutation and dynamic sequence multiplexing for video encryption," *Scientific Reports,* vol. 13, p. 14721, 2023, http://doi.org/ 10.1038/s41598-023-41082-9.

[23] C. Chen, X. Wang, and J. Xu, "A robust VVC video encryption scheme based on the dynamical chaotification model," *Journal of King Saud University-Computer and Information Sciences,* vol. 35, p. 101752, 2023, http://doi.org/ 10.1016/j.jksuci.2023.101752.

[24] N. Tahat, O. M. Al-hazaimeh, and S. Shatnawi, "A New Authentication Scheme Based on Chaotic Maps and Factoring Problems," in *International Conference on Mathematics and Computations*, 2022, pp. 53-64, http://doi.org/ 10.1080/09720529.2022.2101601.

[25] M. Ephin, J. A. Joy, and N. Vasanthi, "Survey of Chaos based Image encryption and decryption techniques," in *Amrita International Conference of Women in Computing (AICWIC'13) Proceedings published by International Journal of Computer Applications (IJCA)*, 2013, India.

[26] F. Yan, A. M. Iliyasu, S. E. Venegas-Andraca, and H. Yang, "Video encryption and decryption on quantum computers," *International Journal of Theoretical Physics,* vol. 54, pp. 2893-2904, 2015, http://doi.org/10.1007/s10773-015-2524-3.

[27] O. M. Al-Hazaimeh, and A. Ma'moun, "Vehicle To Vehicle and Vehicle To Ground Communication-Speech Encryption Algorithm," *In 2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME),* pp. 1-4, 2023, Spain.

[28] S. Claude, "Communication theory of secrecy systems," *Bell system technical journal,* vol. 28, pp. 656-715, 1949, http://doi.org/10.1002/J.1538-7305.1949.TB00928.X.

[29] J. Zaman and R. Ghosh, "Review on fifteen statistical tests proposed by NIST," *Journal of Theoretical Physics and Cryptography,* vol. 1, pp. 18-31, 2012.

[30] N. A. Advani and A. M. Gonsai, "Performance analysis of symmetric encryption algorithms for their encryption and decryption time," in

2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), 2019, pp. 359-362, New Delhi.

[31] M. A.-H. Obaida, M. Al-Jamal, M. Bawaneh, N. Alhindawi, and B. Hamdoni, "A new image encryption scheme using dual chaotic map synchronization," *International Arab Journal of Information Technology*, vol. 18, pp. 95-102, 2021, http://doi.org/10.34028/iajit/18/1/11.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed to the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare.

APPENDIX

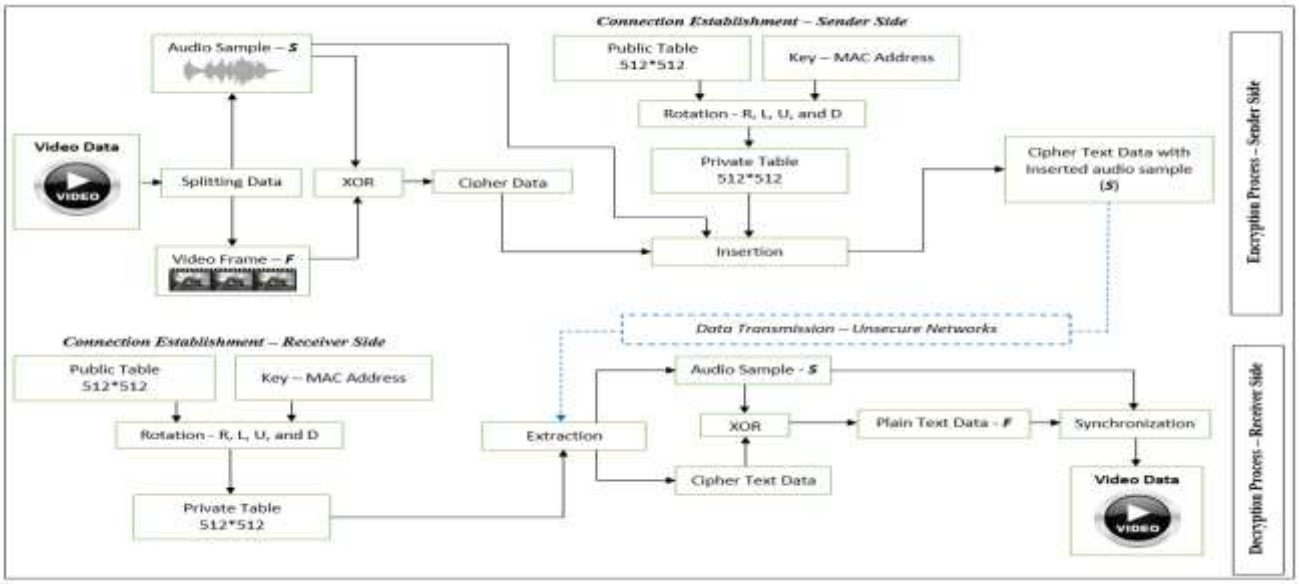

Fig. 2: Flow Chart Diagram