© DEC 2025 | IRE Journals | Volume 9 Issue 6 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I6-1712761

Development of A Bio-Cryptographic Security Based Digital Video using Reptile Search Rivest-Shamir-Adleman

AJIBADE BOLARINWA OLUSESAN[1], FALOHUN ADELEYE SAMUEL[2], OKEDIRAN OLADOTUN OLUSOLA[3] AWODOYE OLUFEMI O.[4] MAKINDE OLADAYO E.[5], OGUNTOYE JONATHAN P.[6]

[1, 2, 3, 4, 5, 6]*Computer Science and Engineering, Ladoke Akintola University of Technology. Ogbomoso, Oyo state, Nigeria.*

Abstract: The growing demand for video streaming services necessitates robust security measures to protect content from unauthorized access and piracy. Traditional cryptographic methods face vulnerabilities in securing digital video content from unauthorized access and dissemination. Existing Rivest-Shamir-Adleman (RSA) techniques that achieved high level of security are limited by high encryption and decryption time. Hence, this research developed a Bio-Cryptographic security of digital video using Reptile Search Rivest-Shamir-Adleman (RS-RSA) system for a secure video encryption. Nine hundred (900) sample images from 300 students of Ladoke Akintola University of Technology (LAUTECH), Ogbomoso, used in this study were acquired using Digital camera (Canon EOS R5) for faces; each with three samples. Six hundred and thirty (630) images of these faces were used for training while two hundred and seventy (270) images were used for testing. The acquired images were preprocessed using histogram equalization. RS-RSA was developed by using Reptile Search (RS) algorithm to optimize RSA. Matching score for identification was generated using Euclidean distance. The developed RS-RSA technique was implemented in MATLAB R2023a. The performace of the technique was evaluated using Encryption Time (ET), Decryption Time (DT), and Throughput (TH), by comparing with RSA technique. The verification of the faces were measured using Accuracy (ACC), False Acceptance Rate (FAR) and False Rejection Rate (FRR) for a range of threshold values. The ET, DT, TH for RS-RSA were 0.551 ms, 0.548 ms and 325.77 KB/s, respectively, while the corresponding value for RSA were 1.094 ms, 1.109 ms and 161.469 KB/s. The ACC, FAR and FRR for RS-RSA at optimum threshold of 0.98 were 94.44%, 5.128%, and 5.882%, respectively, while the corresponding value for RSA were 92.59%, 11.97% and 3.922%. The developed RS-RSA effectively improved the security of RSA through optimization using Reptile Search (RS) algorithm. The developed technique could be adopted for the development of a bio-cryptographic security based digital video.

Key words: Biometrics, Cryptographic, Digital video, Face, Reptile Search Algorithm, Rivest-Shamir Adleman, Encryption, Decryption Time, Throughput.

I. INTRODUCTION

Video streaming applications have undoubtedly become crucial for entertainment. It is to deliver video content exclusively to paid subscribers. However, there is a mismatch between the actual viewership size and the number of subscribed users. A minor portion of registered users voluntarily share their login credentials with people in their social circles, such as acquaintances and family members. There may be cases where subscribed individuals replicate content and disseminate it to others. Multiple research initiatives are focused on enhancing security protocols and maximizing revenue streams for these platforms (Fouzar *et al.,* 2023). The use of cryptographic techniques is vital in addressing the risks of unauthorized file sharing and piracy during video content distribution.

However, many studies have explored using cryptography to restrict the dissemination of video content. Most approaches in this area rely less on hardware components. Cryptography is a method of securing and transmitting data in a particular form so that only the intended recipients can read and process it. It is the science of scrambling data for secure communication, preventing eavesdropping regardless of awareness of the data transmission (Obakhedo, 2011; Olaniyi *et al.,* 2014). Symmetric and asymmetric key cryptography are two prominent methods employed to ensure robust security in the communication process. Symmetric key or secret key cryptography, is the predominant cryptographic technique employed in multimedia communication. Asymmetric or public-key cryptography, has emerged as a significant solution to the challenges posed by symmetric cryptography.

Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC) are some of the prominent methods in this field which have been extensively studied and are currently gaining recognition for their effectiveness in addressing the limitations of symmetric cryptography (Fouzar *et al.,* 2023). Reptile Search Algorithm (RSA) is an optimization strategy and a meta-learning algorithm proposed by researchers at Open AI in 2018. It is a model-agnostic meta-learning algorithm that can be applied to various machine learning models, including deep neural networks.

Hence, this study has developed a Rivest-Shamir-Adleman (RSA) algorithm with Reptile Search Algorithm (R-RSA) for securely transmitting and streaming the encrypted video content to authorized users while minimizing the risk of interception or suspicion. A biometric-based key generation and management system that seamlessly integrates with the R-RSA algorithm for encrypting and decrypting digital video content was developed.

Thus, this study evaluates the performance of the designed technique using the following metrics Encryption and Decryption Time, Throughput, False Acceptance Rate (FAR), False Rejection Rate (FRR), Accuracy and Recognition time.

II. LITERATURE REVIEW

Digital video is an electronic representation of moving visual images in the form of encoded digital data. Digital video can be easily viewed by anybody and be infinitely duplicated. The primary method used to protect data is limiting access to the data. This can be done through authentication, authorization, and access control. Numerous studies have explored various fields to improve security measures to protect content from unauthorized access and piracy. This review discusses key contributions in these fields, their innovations, and limitations, leading to the identification of the research gap that this study addresses.

Williams *et al,* (2020) explored the potential of integrating biometric traits with RSA encryption to safeguard digital video content. The researchers adopted an experimental design, applying RSA encryption to videos and using fingerprints as a biometric identifier for decryption. The results showed a significant increase in security compared to standard RSA encryption alone, reducing unauthorized access. Despite these positive results, the study did not investigate the speed and efficiency of this encryption system in real-time video streaming, presenting a research shortfall for future investigation.

Davis *et al,* (2021) focused on the effectiveness of RSA encryption when combined with biometric authentication for securing digital video. The researchers employed an empirical method, testing the encryption on video files while using facial recognition as the biometric component. The results indicated that the RSA and biometrics combination provided a robust layer of security, successfully preventing unauthorized access. However, the study did not address the potential vulnerability of biometric data being compromised, indicating a weakness in exploring the implications of biometric theft. It failed to explore multi-layer biometric encryption techniques to close this gap.

Patel *et al,* (2021) focused on securing video content through a combination of RSA encryption and biometric authentication. The researchers employed an experimental approach by encrypting videos using RSA and integrating iris scan biometrics for decryption. The results revealed strong encryption and access control, preventing unauthorized viewing of video content. However, the study left a shortfall in exploring how vulnerable the system might be to biometric spoofing attacks, suggesting further research into more resilient biometric systems. Addressing this issue could enhance the robustness of bio-cryptographic systems.

Kumar *et al,* (2021) analyzed the performance and security implications of using RSA encryption combined with biometric authentication for digital video files. The researchers used a simulation-based approach to measure both encryption strength and system performance. The findings indicated high security levels but revealed performance issues such as longer encryption times. The study did not delve into how this approach could be optimized for speed in real-time video encryption, uncovering a weakness in performance efficiency. Optimizing the encryption techniques in order to reduce encryption and decryption times were not considered.

Smith *et al,* (2022) investigated the use of bio-cryptography, integrating RSA encryption with biometric authentication to enhance the security of digital video. A hybrid method involving simulation and empirical testing was used to implement RSA encryption combined with biometric traits like fingerprints. The results revealed that the integration of biometric traits strengthened video security by ensuring only authenticated users could access the content. However, the study did not analyze how the system handles large-scale video datasets, creating a void in its application to high-demand environments like streaming services. There is a requirement to address scalability and performance in real-time usage scenarios.

Zhao *et al,* (2022) explored the use of RSA encryption combined with biometric data, such as fingerprints, to secure digital videos. A mixed-method approach was used, involving both simulation and testing of real-world video datasets with biometric authentication. The results demonstrated that RSA and biometrics worked synergistically to improve security by limiting access to authorized users. The research, however, did not address the scalability of this system for large-scale platforms, resulting in an insufficiency in its application in cloud-based or distributed environments. Optimizing the system for large datasets and high user traffic were not taken into consideration.

Lee *et al,* (2022) investigated how integrating RSA encryption with biometric authentication enhances the security of digital videos. The researchers conducted experimental tests using RSA encryption and facial recognition for secure access to video files. The results showed significant security improvements, although encryption time was found to be slower than anticipated. The study did not address the impact of network latency on encryption performance, leaving an unresolved issue in real-time encryption for online streaming platforms. Latency minimization to improve the usability of bio-cryptographic systems in dynamic environments were not considered.

Brown *et al,* (2022) focused on applying RSA encryption and biometric authentication to secure streaming video content. The researchers employed a mixed-method approach, combining RSA encryption for video files with biometric traits, such as iris scans, for decryption. The results demonstrated a high level of security but indicated that the system was not well-optimized for live streaming scenarios due to latency. This highlights an opening in developing real-time encryption systems that can handle the demands of video streaming platforms. The work failed to explore lightweight encryption algorithms that enhance both security and performance in live video environments.

Ahmad *et al,* (2023) aimed to evaluate the effectiveness of RSA encryption combined with biometric authentication in securing video files. The researchers used simulation and quantitative analysis, applying RSA encryption and fingerprint biometrics to test security performance. The findings demonstrated that this approach significantly improved security but introduced latency issues during encryption and decryption processes. However, the research did not consider optimizing the system for high-performance environments, highlighting a deficiency in its application for real-time video encryption. Further studies are needed to explore lightweight encryption algorithms that can balance security with speed.

Grupta *et al,* (2023) addressed the challenge of securing digital video content using RSA encryption integrated with biometric data such as fingerprints. An experimental methodology was used to test the encryption of videos and the use of biometric traits for access control. Results indicated that the approach enhanced security, although there were challenges with processing speed during encryption. The study did not explore the integration of multi-factor authentication methods, leaving a breach in building even stronger security protocols. The research failed to investigate multi-modal biometric systems combined with cryptography for enhanced protection.

These persistent challenges underline the need for a more scalability, performance optimization, and computationally overhead introduced by biometric authentication and RSA's encryption processes. The integration of Reptile Search Algorithm into the Rivest-Shamir-Adleman framework offers a promising path forward. Reptile Search Algorithm contributes on optimizing encryption speed and reducing biometric vulnerabilities, to make bio-cryptographic security systems more adaptable for large-scale, real-time applications.

III. METHODOLOGY

The developed system operates in two phases: enrolment phase and authentication phase. During enrolment, pre-processed face images undergo feature extraction, which are fed into Rivest-Shamir-Adleman based key generation module, which leverages the Reptile Search Algorithm (RSA). The encrypted video, along with the user's facial features, was securely stored in the Secured Database for further authentication purposes. In authentication, each face is similarly processed and classified using Euclidean Distance, which measures the similarity between the two sets of features. Whenever a match is confirmed, the corresponding secret key is regenerated using the RSA algorithm. This key is used for the decryption of the encrypted video, granting the user access. Implementation was done in MATLAB R2023a on a Windows 11 system. The complete System Architecture is depicted in Figure 1.

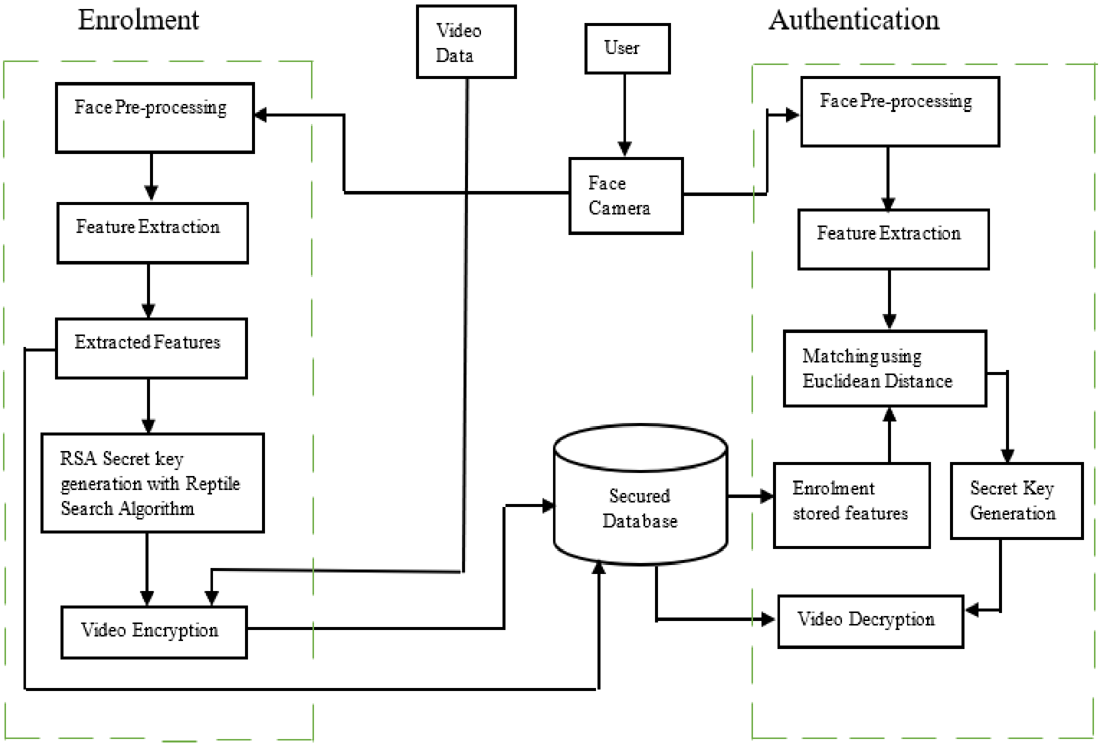

Figure 1: System Architecture of the Designed Bio-Cryptographic Security of Digital Video

3.1 Data Acquisition and Preprocessing

This study utilized video dataset obtained from online youtube in AVI and Mp4 format. Nine hundred (900) sample images from 300 students of Ladoke Akintola University of Technology (LAUTECH), Ogbomoso, were acquired using Digital camera for faces; each with three samples, to generate robust authentication parameters. Six hundred and thirty (630) images of these faces were used for training while two hundred and seventy (270) images were used for testing.

Preprocessing involved two key steps. First, Image acquisition, it involves capturing facial data using a digital camera or similar imaging device. The camera records the face in real-time, ensuring high-quality video or still images with sufficient resolution for accurate analysis. Proper lighting and positioning are essential during acquisition to minimize shadows, glare, and distortions that could affect subsequent processing. The captured images are then prepared for the next stages of processing, such as feature extraction, by ensuring they are clear and aligned to standard formats. Second, Image pre-processing, it enhances the quality of facial images for accurate analysis and recognition. It begins with noise reduction techniques to eliminate unwanted artifacts, ensuring a clean image for further processing. The images are then normalized to standard dimensions and intensity levels, enabling consistent feature extraction regardless of variations in lighting or scale.

Face alignment is also performed to position the facial features, such as eyes and nose, in a uniform orientation, improving the system's robustness. These pre-processing techniques ensure that the facial data is optimized for subsequent feature extraction and key generation steps, enhancing the overall reliability of the biometric system.

3.2 Feature Extraction

The acquired images were pre-processed using histogram equalization. R-RSA was developed by using Reptile Search Algorithm to optimize RSA. Matching score for identification was generated using Euclidean distance.

The system combined RSA encryption with the Reptile Search Algorithm (R-RSA) to optimize cryptographic efficiency and biometric facial recognition for secure access. The Reptile Search Algorithm enhanced RSA's key generation by searching for optimal encryption keys, thus improving encryption strength and reducing computational overhead. The framework involves three primary stages: RSA enhanced with Reptile Search Algorithm (R-RSA) for secure video encryption. Facial recognition for user authentication. R-RSA algorithm for video decryption, allowing authorized users to access the content.

3.3 Implementation of the Developed R-RSA

An interactive Graphic User Interface (GUI) application was designed. The GUI was designed in MATLAB R(2023a). The MATLAB software package was used for the implementation on a computer system with specific configuration.

3.4 Performance Metrics

The performance of the developed R-RSA model was evaluated using Encryption Time (ET), Decryption Time (DT), and Throughput (TH), and compared with RSA technique. The verification of the faces was measured using Accuracy (ACC), Recognition Time, False Acceptance Rate (FAR) and False Rejection Rate (FRR) for a range of threshold values. Encryption Time measures how long the system takes to encode the face biometric data using the RSA algorithm, while the Decryption Time evaluates how quickly the encoded data is decoded as shown in equation (1) and (2). Throughput evaluates the system's processing speed and is defined as the amount of data successfully encrypted or decrypted per unit time as shown in equation (3). Accuracy measures the overall effectiveness of the biometric system in correctly authenticating users as shown in equation (6). False Acceptance Rate measures the percentage of unauthorized users incorrectly accepted by the system while False Rejection Rate measures the percentage of legitimate users incorrectly denied access as shown in equation (4) and (5). Recognition Time the duration required to authenticate a user by comparing the extracted features against the stored features in the database as shown in equation

$$ET = T_{\text{end\_enc}} - T_{\text{start\_enc}} \qquad (1)$$

$$DT = T_{\text{end\_dec}} - T_{\text{start\_dec}} \qquad (2)$$

$$TP = \frac{\text{Total Data Size}}{\text{ET or DT}} \qquad (3)$$

$$FAR = \frac{\text{Number of False Acceptances}}{\text{Total Number of Impostor Attempts}} \times 100\% \quad (4)$$

$$FRR = \frac{\text{Number of False Rejections}}{\text{Total Number of Genuine Attempts}} \times 100\% \quad (5)$$

$$ACC = \frac{\text{Number of Correct Matches}}{\text{Total Number of Authentication Attempts}} \times 100\% \quad (6)$$

$$RT = T_{\text{end\_auth}} - T_{\text{start\_auth}} \qquad (7)$$

IV. RESULTS AND DISCUSSION

The performance of the developed R-RSA system was evaluated using three MP4-format digital videos: Video 1 (76.6 KB, 200 frames), Video 2 (67.3 KB, 180 frames), and Video 3 (81.3 KB, 230 frames). The encryption and decryption operations were carried out on these videos, embedding biometric information securely within the content. For each video, metrics such as encryption time, decryption time, and throughput were calculated to assess efficiency. The GUI supported the selection of RSA or R-RSA (Reptile-enhanced RSA) and displayed a side-by-side comparison of original and encrypted videos. The data show that the encryption-decryption cycle performed efficiently with minimal time delay and maintained high throughput even for increasing frame sizes.

The verification of faces with different threshold values are summarized in Table 1. Performance evaluation result with RSA are presented in Table 2 while Table 3 presented the evaluation result with R-

RSA. Table 4 summarized the comparison result of RSA and R-RSA. The comparative evaluation of RSA and R-RSA (RSA enhanced with Reptile Search Algorithm) for securing digital video demonstrates the superior performance of the R-RSA approach in terms of encryption and decryption efficiency.

As illustrated in Figure 1, which shows the plotted Average encryption time against Dataset, the average encryption time for the standard RSA method across all video datasets is significantly higher compared to R-RSA. This reduction can be attributed to the Reptile Search Algorithm's (RSA) optimization capability, which efficiently searches the key space to identify optimal encryption parameters.

Similarly, Figure 2 revealed that R-RSA outperforms traditional RSA in decryption tasks as well, maintaining average decryption times well below those of RSA across all video samples. The enhanced key selection process provided by the Reptile Search Algorithm ensures that decryption keys are both secure and computationally efficient, thereby reducing latency. Beyond time efficiency, throughput analysis further reinforces the advantage of R-RSA over the traditional RSA, as depicted in Figure 3. The error rate analysis presented in Figure 4 further validates the superiority of the R-RSA approach in maintaining encryption accuracy while achieving better performance metrics. The False Acceptance Rate (FAR) shows a declining trend from approximately 12% to 6% as threshold values increase from 0.2 to 1.0, while the False Rejection Rate (FRR) demonstrates remarkable stability, remaining consistently low between 4% and 6% across all threshold values. This balanced performance indicates that the Reptile Search Algorithm's optimization of RSA key generation not only improves computational efficiency but also maintains robust security characteristics by generating keys that provide consistent encryption quality.

Table 1: Result of Verification of Faces with Different Threshold Values

Threshold	TP	FN	FP	TN	FAR(%)	FRR(%)	ACC(%)	Time(sec)
0.01	147	6	14	103	11.97	3.922	92.59	45.02
0.1	147	6	14	103	11.97	3.922	92.59	45.02
0.15	147	6	14	103	11.97	3.922	92.59	45.02
0.2	147	6	14	103	11.97	3.922	92.59	45.02
0.21	146	7	11	106	9.402	4.575	93.33	44.93
0.25	146	7	11	106	9.402	4.575	93.33	44.93
0.3	146	7	11	106	9.402	4.575	93.33	44.93
0.35	146	7	11	106	9.402	4.575	93.33	44.93
0.36	145	8	8	109	6.838	5.229	94.07	44.56
0.4	145	8	8	109	6.838	5.229	94.07	44.56
0.45	145	8	8	109	6.838	5.229	94.07	44.56
0.5	145	8	8	109	6.838	5.229	94.07	44.56
0.6	144	9	6	111	5.128	5.882	94.44	45.12
0.75	144	9	6	111	5.128	5.882	94.44	45.12
0.85	144	9	6	111	5.128	5.882	94.44	45.12
0.98	144	9	6	111	5.128	5.882	94.44	45.12

Table 2: Performance Evaluation Result with RSA

Dataset	No of Frames	Memory Size (KB)	Encryption Time (ms)	Decryption Time (ms)	Throughput (KB/s)
Video 1	200	76.6	0.994	1.002	193.281
Video 2	180	67.3	1.089	1.104	134.208
Video 3	230	81.3	1.094	1.109	161.469

Table 3: Result of R-RSA

Dataset	No of Frames	Memory Size (KB)	Average Encryption Time (ms)	Average Decryption Time (ms)	Average Throughput (KB/s)
Video 1	200	76.6	0.556	0.544	353.035
Video 2	180	67.3	0.553	0.550	268.560
Video 3	230	81.3	0.551	0.548	325.778

Table 4: Comparison Result of RSA and R-RSA

Dataset	No of Frames	Memory Size (KB)	Techniques	Encryption Time (ms)	Decryption Time (ms)	Throughput (KB/s)
Video 1	200	76.6	RSA	0.994	1.002	193.281
			R-RSA	0.556	0.544	353.035
Video 2	180	67.3	RSA	1.089	1.104	134.208
			R-RSA	0.553	0.550	268.560
Video 3	230	81.3	RSA	1.094	1.109	161.469
			R-RSA	0.551	0.548	325.778

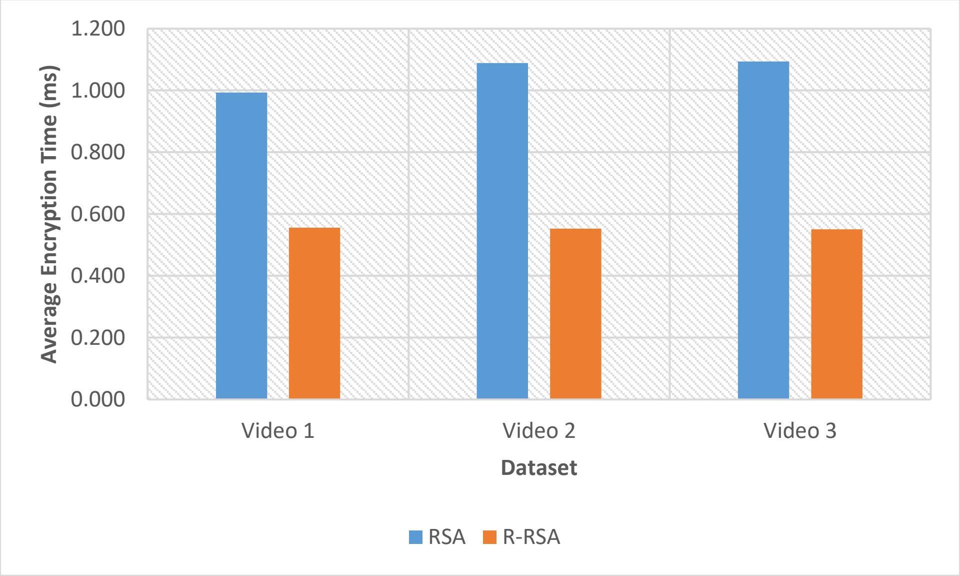

Figure 1: The Chart demonstrating Average Encryption Time

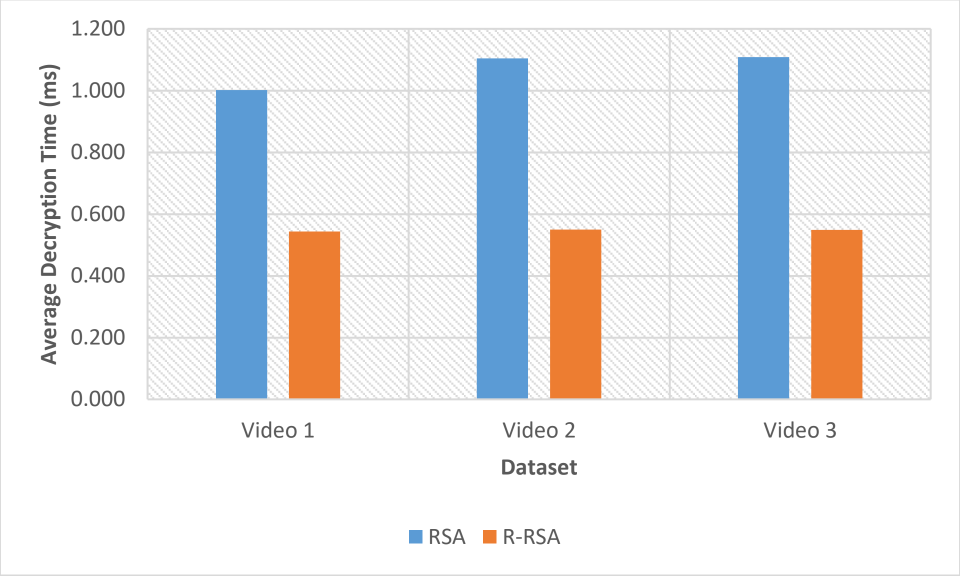

Figure 2: The Chart demonstrating Average Decryption Time

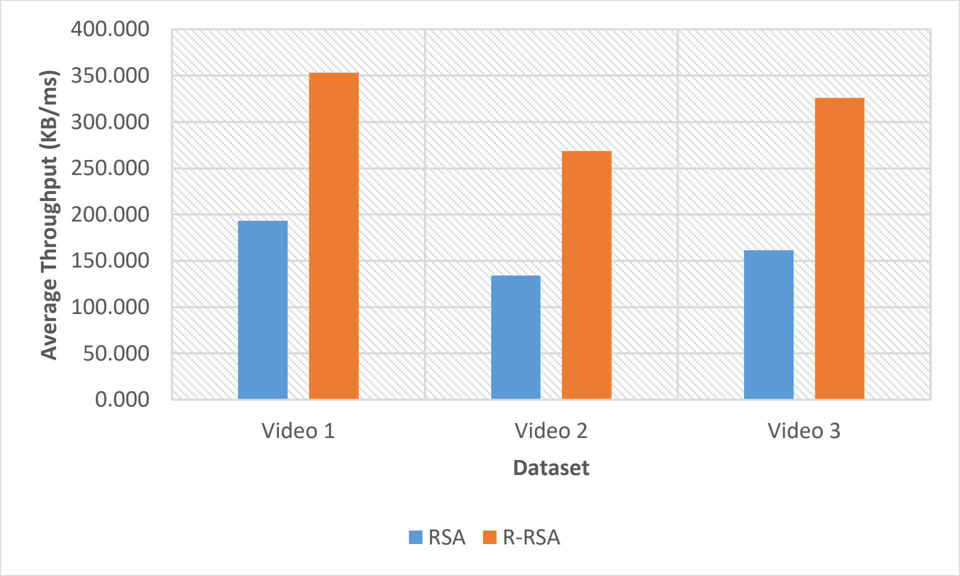

Figure 3: The Chart demonstrating Average Throughput

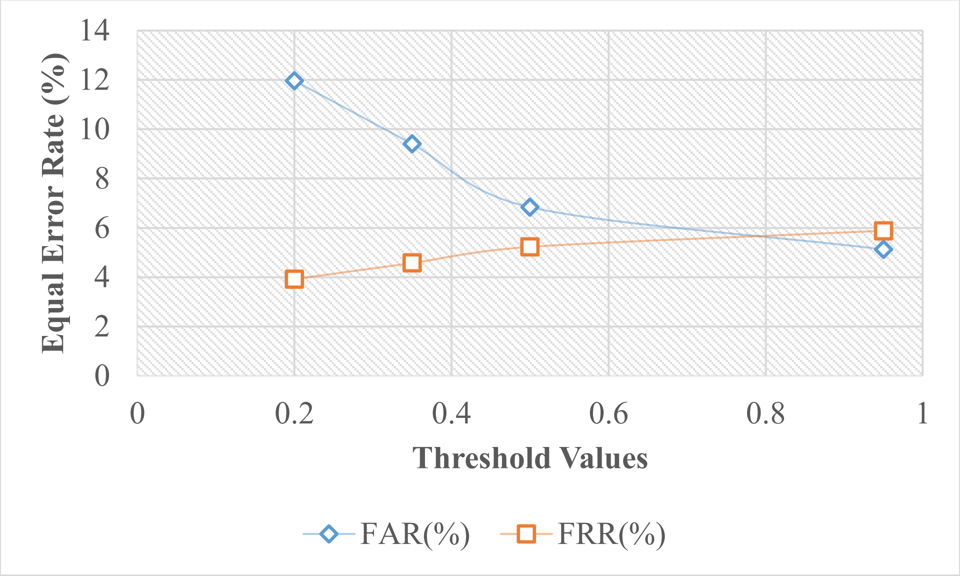

Figure 4: The Graph of Equal Error Rate

V. CONCLUSION

This research developed a bio-cryptographic security based digital video using Reptiles Search Rivest-Shamir-Adleman. Motivated by the limitations of traditional RSA, the developed R-RSA significantly reduced both encryption and decryption times by optimizing the key generation process, thereby minimizing computational overhead. Additionally, R-RSA achieves higher throughput, indicating a greater capacity for secure data processing in less time, which is crucial for real-time video applications. The results showed that R-RSA consistently outperformed traditional RSA across various video datasets, regardless of complexity or size. By reducing redundant operations and improving the cryptographic strength of the keys, R-RSA not only increased performance but also enhanced overall security of the system.

REFERENCES

[1] AbdulWahab, A. W., Jameel, M., Azam, M. A., and Khan, M. A. (2022). Application of metaheuristic optimization algorithms in cryptography: A review of recent advances and future trends. *IEEE Access, 10*, 18493-18514. https://doi.org/10.1109/ACCESS.2022.3149847

[2] Abualigah, L., Abd Elaziz, M., Sumari, P., Geem, Z. W., and Gandomi, A. H. (2022). Reptile Search Algorithm (RSA): A nature-inspired meta-heuristic optimizer. *Expert Systems with Applications*, *191*, 116-158.

[3] Abuguba, S., Milosavljević, M. M., and Maček, N., (2015). An Efficient Approach to Generating Cryptographic Keys from Face and Iris Biometrics Fused at the Feature Level, *IJCSNS International Journal for Computer Science and Network Security*, 15(6): 6–11.

[4] Ahmad, M., and Khan, N. (2023). Evaluating RSA and Biometric Security in Digital Videos. *International Journal of Cybersecurity*, 11(4), 66-81.

[5] Brown, C., and Lewis, D. (2022). RSA and Biometric Systems for Streaming Video Security. *Journal of Secure Multimedia*, 12(4): 123-138.

[6] Davis, P., and Johnson, R. (2021). RSA Encryption and Biometrics in Digital Video Security. *International Journal of Information Security*, 18(2): 108-122.

[7] Falohun, A. S., Fenwa, O. D., and Oke, A. O. (2016). An access control system using bimodal biometrics. *International Journal of Applied Information Systems, Foundation of Computer Science-FCS, New York, USA*, 10(5): 41-47.

[8] Gupta, V., and Sharma, P. (2023). RSA and Biometric Integration for Video Security. *Journal of Multimedia Encryption and Security*, 11(3): 92-107.

[9] Kumar, C., and Singh, S. (2024). Security standards for real time video surveillance and moving object tracking challenges, limitations, and future: a case study. *Multimedia Tools and Applications*, 83(10): 30113-30144.

[10] Kumar, S., and Das, P. (2021). RSA and Biometric Encryption in Digital Video

Protection. *Cybersecurity and Encryption Journal*, 13(1): 100-114.

[11] Lee, H., and Park, K. (2022). Enhancing Video Security with RSA and Biometrics. *International Journal of Cryptographic Systems*, 15(2): 45-60.

[12] Oluwadamilola, K. O., Ayodeji, A. O., Martins, O. O., Olufunmi, I. S., and Rapheal, O. A. (2017). An improved authentication system using hybrid of biometrics and cryptography. In *2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON)*, 457-463.

[13] Patel, R., and Singh, A. (2021). RSA-Based Bio-Cryptographic Security for Digital Videos. *Journal of Information Technology and Security,* 10(2): 52-64.

[14] Ross A., (2007). An introduction to Multibiometrics. Appeared in the *Proc. Of the 15th European Signal Processing Conference (EUSIPCO),* Poznan, Poland. arun.ross@mail.wvu.edu, http://www.csee.wvu.edu/˜ross

[15] Ross A. (2009). Multibiometrics. In: Li S.Z., Jain A. (eds) Encyclopedia of Biometrics. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-73003-5_147

[16] Selvarani, P., and Visu, P. (2015). Multi-model bio-cryptographic authentication in cloud

[17] storage sharing for higher security. *Research Journal of Applied Sciences, Engineering and Technology*, 11(1): 95-101.2

[18] Smith, J., and Lee, M. (2022). Bio-Cryptographic Video Security Using RSA. *Journal of Cryptography and Security*, 12(3): 44-57.

[19] Venna, S. R., and Inampudi, R. B., (2019). MMBAS-NS: Multimodal Biometric Authentication System and Key Generation Algorithm for Network Security on Mobile Phones. *International Journal of Recent Technology and Engineering (IJRTE)* ISSN: 2277-3878, Volume-7 Issue-5S2, 189-199.

[20] Williams, T., and Chen, L. (2020). Biometric-Enhanced RSA Encryption for Secure Video Content. *Journal of Digital Media Security*, 14(1): 32-46.

[21] Zhao, Y., and Miller, S. (2022). RSA and Biometric-Based Security in Digital Video Protection. *Journal of Multimedia Security*, 9(3): 85-99.