Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 2, 379-393
2026
Publisher: Learning Gate
DOI: 10.55214/2576-8484.v10i2.12086

Multimedia content security in cloud environments using asymmetric cryptography

Najma Imtiaz Ali[1*], Imtiaz Ali Brohi[2], Mujeeb-Ur-Rehman Jamali[3], Nurul A. Emran[1], Syed Sohail Ahmed Shah[4], Mazhar Basheer Arain[5], Aadil Jamali[6], Noor Zaman Jhanjhi[7]

[1]Fakulti Teknologi Maklumat dan Komunikasi,Universiti Teknikal Malaysia, Melaka, Malaysia; najma@utem.edu.my (N.I.A.) nurulakmar@utem.edu.my (N.A.E).

[2,3,4,5]Department of Computer Science, Government College University, Hyderabad, Sindh, Pakistan; imtiaz.brohi@gcuh.edu.pk (I.A.B) mujeebjamali@usindh.edu.pk (M.R.J.) sohailahmed.shah@gcuh.edu.pk (S.S.A.S.) mazhar.arain@gcuh.edu.pk (M.B.A.).

[6]Institute of Mathematics and Computer Science, University of Sindh, Jamshoro, Sindh, Pakistan; aadilabdulkarim@gmail.com (A.J.).

[7]School of Computer Science, Faculty of Innovation & Technology, Taylor's University, Malaysia; noorzaman.jhanjhi@taylors.edu.my (N.Z.J.).

Abstract: Information security and cybersecurity involve protecting personal identifiable information and confidential data stored in the cloud. System vulnerabilities are heightened due to increased processing capabilities. The demand for multimedia content stored in cloud environments is growing, raising significant security concerns, particularly regarding unauthorized access to sensitive information. This study offers a posteriori analysis of various asymmetric algorithms tested with small, medium, and large datasets. The analysis reveals the efficiency and limitations of these algorithms, providing valuable insights for selecting appropriate security measures. Notably, Elliptic Curve Cryptography (ECC) with specific key curve parameters demonstrates superior efficiency, shorter key lengths, and adaptability to resource constraints, making it well-suited for cloud-based multimedia applications. Ensuring the protection of private and confidential data through cryptographic solutions that are resilient to evolving cyber threats is crucial in the dynamic cloud environment. The findings contribute to enhancing content security by applying modern cryptographic techniques within cloud infrastructure. These results will aid researchers and decision-makers in choosing effective algorithms to secure multimedia content stored in the cloud, ultimately strengthening data protection and privacy in cloud computing systems.

Keywords: *Asymmetric algorithms, Cloud computing, Elliptic curve cryptography, Multimedia, Security.*

1. Introduction

The usage of digital media has increased in the past several years as cloud environments become more vital for multimedia content storage and processing. The security of private and confidential data, including multimedia content such as text, images, audio, and video, used in applications over the cloud, is a significant issue. Transmitting sensitive information over public networks poses security risks.

Generally, authenticity and solutions rely on concealment techniques such as digital watermarking and encryption provided by designers and researchers. The techniques are not confirmed to be proposed by the researcher, but all are guaranteed to mitigate attacks. Cryptography is used to secure a variety of applications, such as e-commerce transactions and internet communication. Modern cryptography technologies are used to secure content from malicious and illegal activities, and the selection of the cryptographic algorithm is very critical [1]. The objective of this study is to provide insights for selecting the best asymmetric algorithm for the security of private and sensitive content used by applications over the cloud. Additionally, modern cryptographic application algorithm efficiency and limitations are also discussed in detail, with recommendations for cloud-service providers to improve the overall security posture of cloud-based multimedia applications.

History: Received: 27 November 2025; Revised: 16 January 2026; Accepted: 19 January 2026; Published: 10 February 2026
* Correspondence: najma@utem.edu.my

2. Cryptography

Cryptography is the science of transforming data into an unreadable format. The converted data using cryptographic methods is known as ciphertext. Various algorithms are used to protect data during communication and at rest from attackers. These methods aim to provide data confidentiality, integrity, and authentication. Cryptographic algorithms employ mathematically related keys. In the cryptographic process, keeping data confidential for only the intended user involves a private key to decrypt data into an understandable format, while a public key is used to encrypt the data. Keys are information that controls the algorithm's functionality. The strength of these algorithms, which provides a level of security, depends on the use of keys.

3. Asymmetric Cryptography

Public-key cryptography is widely utilized in a variety of security applications, including internet-based secure communication, digital signatures, and key exchange protocols. It is also known as asymmetric cryptography. There are pairs of keys that are used to protect private and confidential data, including multimedia content. The symmetric algorithm uses the secret key to prevent and mitigate attacks from attackers while data is in motion or at rest. A symmetric algorithm utilizes the same key for encryption and decryption purposes. It is different in the process compared to the asymmetric algorithm, which employs two independent but mathematically linked keys that are private and public. The public key is distributed to everyone for the purpose of encrypting data, while the private key is kept private, only accessible to its owner or intended user(s) to decrypt data. The sending of data over the cloud ensures that any malicious entity could not understand the data if, in any case, they intercepted or gained access. The process of transforming data into an understandable format using the private key in the case of the intended receiver, assures that only the intended receiver, who owns the key, has access to the data.

An asymmetric algorithm ensures the verification of the data using the process of digital signature if the data is altered or modified while in motion or at rest. The process in the asymmetric algorithm first takes the hash value in the fixed format and then encrypts it with the private key. In the verification phase, the public key is distributed to everyone for the purpose of verifying the data if there is any alteration or modification.

Asymmetric algorithms are also used to prove user authentication; using the digital certificate, only a valid user can gain access to data [1].

4. Literature Review

In this section, a summary of the various research works conducted and the tactics used to secure multimedia content are provided in different applications.

This research was conducted on multimedia content, i.e., pictures and audio. According to authors [2], there is a serious issue of privacy when transferring data over the network, and keeping it secure from unwanted readers is a significant concern. To mitigate this, modern cryptography can be used, with AES and RSA algorithms securing the multimedia materials. The authors compared the empirical performance of the given image. The outcome of the research was that AES provides higher picture quality. The authors proposed that the performance of symmetric and asymmetric techniques could be compared.

In Jamali et al. [3], the authors performed a comparative study of image, audio, and video encryption and decryption using well-known symmetric algorithms. The performance of the algorithms was recorded in milliseconds. The maximum key sizes used for security levels were Blowfish (448 bits), DES & 3DES (56 and 168 bits), and AES (128 bits).

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 2: 379-393, 2026
DOI: 10.55214/2576-8484.v10i2.12086

Table 1.
Comparative Analysis of the performance of symmetric algorithms for multimedia contents.

	Blowfish	DES	3DES	AES
Image (small, medium, & large datasets)				
Enc	2.2/10/24	3.5/22/54	9.4/64/154	2.1/8/8
Dec	3.1/13/30	3.9/24/55	12.7/69/162	2.3/8/8
Audio & Video (small, medium & large datasets)				
Enc	133.7/206.2/699.3	181/418.7/1470	418/1218/4399	74.9/84/181
Dec	108/209.5/702.1	174/438.9/1504	324/1200.5/4351	79.4/76/173

In Duan et al. [4], the authors proposed a steganography method to conceal private and confidential multimedia data, including images. They argued that in the host image, steganography techniques could be used to embed secret information; thus, the payload capacity is practically ignored. They also suggested enhancing the image quality for the human visual system. Additionally, they proposed that a deep learning-based technique could be used for increased novelty and higher steganography performance. Elliptic Curve Cryptography (ECC) encryption might be employed for anti-detection image features, while the Discrete Cosine Transform (DCT) is used to transform the secret image. The authors also proposed using the Deep Neural Network (SegNet) technique for concealment and extraction of the entire image. Their empirical results and recommendations indicate that pixels can be effectively assigned using this approach, with a Peak Signal-to-Noise Ratio of 40 dB and a Structural Similarity Index of 0.96. The deep neural network-based technique for steganography and extraction was suggested, with ECC and DCT solutions proposed. During the process, DCT image processing is performed, followed by ECC to produce a secret image via steganography. The resulting image appears noisy. The SegNet deep learning model embeds the image into the host image without modifying its integrity during embedding and extraction. The image quality remains unaffected, but its anti-detection properties are improved. The study's findings recommend that this approach is more suitable because it does not require creating a new algorithm.

In Yu et al. [5] authors argued that an image is reconstructed using probabilistic Visual Cryptography (VC), which included hidden information in the image that reduced visual quality. The technique was used in which a binary image replicates the continuous grayscale tone of the image. The VC technique is proposed with a grayscale image halftone.

In Blundo et al. [6], the authors argued that to enhance the quality of the reconstructed image, a probabilistic VC technique for grayscale images utilizing Efficient Direct Binary Search (EDBS) should be used. In this process, the EDBS halftone process reconstructed image is used as the optimization object. It was stated that the same security level is provided as classic VC, and the usefulness of the technique was confirmed. The posterior analysis reveals that in the reconstructed image, the minority pixels' hidden structure and tone are reconstructed. There is a great quality with high computational expense.

In Zhang et al. [7], asymmetric cryptography and the Hadamard basis pattern were combined to devise a way to perform multi-image encryption. Using the basic pattern, reconstruct the high quality of the image. The Hadamard pattern is used to achieve ghost image scrambling. The RSA algorithm was developed for low-quality random illumination patterns while improving the system security. The RSA algorithm is used for encryption and to detect values in the image. The outcome of the encryption process is a ciphertext collected with all observed intensity values of the image. In the process, randomness in the permutation process and asymmetric algorithm cryptography provide a security layer in the encryption method. The process of multi-image encryption prevents noise and crosstalk in the image. The suggested method and its security were validated using numerical simulation and practicality to encrypt numerous images using the RSA algorithm for the final ciphertext for adequate security.

In Yan et al. [8], the authors proposed an algorithm that is VC for the poor quality of a grayscale image to rebuild. To enhance the quality according to the criteria of the visual system, interpret the halftone binary image.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 2: 379-393, 2026
DOI: 10.55214/2576-8484.v10i2.12086

In Shyu [9], the authors proposed a process resulting in a visually appealing reconstructed secret image, which is an analysis-by-synthesis framework for use with halftoning. Pixels are reconstructed with VC encoding; in this process, the error diffusion process reconstructs the original image. It was argued that the experimental outcome showed that the framework is successful and can be used in various sizes of the VC method, such as block, vector, random grid, and probabilistic. The authors found that the AbS framework is a classic and secure VC method.

In Ke et al. [10], the authors stated that modern cryptography, including asymmetric and symmetric, is used for end-to-end communication. RDH-ED techniques were proposed by the authors, which are based on the Chinese remainder theorem. The technique is used to divide the secret image into various ciphertext shares. In this concept, image sharing is regenerated if at least shares are acquired. There are two hiding methods utilized, namely Homomorphic Difference Expansion in Encrypted Domain (HDE-ED) and Difference Expansion in Image Sharing (DE-IS). The first method reconstructs the image by using the homomorphism of secret sharing, and the second uses marked shares prior to the image that support data extraction. The empirical results show that the inception function of the secret sharing maintains security, efficiency, and higher reversibility.

In Sun et al. [11], the authors proposed a technique to reconstruct images using VC with various sizes of images and information hidden, as well as image quality. It simulates a grayscale image from a discrete binary image. The grayscale image was merged and shared using the halftone approach. The EDBS algorithm, which includes a multi-pixel encryption technique, is integrated into the halftone process. Optimization of both local and global aspects is achieved for image reconstruction. The authors claimed that, based on experimental findings, the technique is secure and efficient, which has been theoretically proven.

In Lin et al. [12], the authors stated that video steganography is in an experimental stage, and AI-based steganography using neural networks has made tremendous progress. Full video steganography (3DCNN) extracts spatiotemporal details from videos using long skip connections. It was a contribution of the authors that they developed a 3DCNN with a neural network-based video steganography model. The extraction network enables embedding and recovery of secret movies. There is a video classification using SRNet-based methods that accurately extracts secret messages. The model proposed by the authors claims to have anti-detection ability and usability across various video qualities.

In Singh et al. [13], it was argued by the authors that in the Industrial Internet of Things (IIoT), images are generated by sensors with cameras that are vulnerable when communicating over the public network. Hence, encryption is a technique that mitigates and protects the image over the public network.

There is concern that the protection from piracy and copyright of multimedia content, including video streaming in real-time, is increasing. The authors conducted a study mentioned as Fouzar et al. [14] and provided a solution that is hybrid cryptography with multi-key to be used for ensuring the security of the contents. ECC algorithms are implemented to secure the data from the sender's end, and the receiver uses the correct private key to decrypt and view the contents, which will be a reliable security measure against piracy and copyright infringement of video streaming. The implemented system is deployed on the Android platform, where both the sender and receiver enable streaming. It was claimed by the authors that the system is efficient in terms of resource utilization, that is, performance, and secure for streaming videos [14].

After the advent of quantum cryptography and the vulnerability of modern cryptography, there is a revolutionized post-quantum cryptography-based video cryptography for securing over the public network for the next generation. The approach used involves the bitstream of the video encoding, where small changes might conceal details. The approach used by the authors in applications such as UAV video identification as well as image communication. The work provides visual security of multimedia contents and visual adaptation. The approach has the capability to insert large messages [15]. This work proposes video steganography based on post-quantum cryptography to enhance the security of images and critical processing.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 2: 379-393, 2026
DOI: 10.55214/2576-8484.v10i2.12086

The multimedia content, i.e., images, audio, and video, has a wide range of applications. It is not common in the public to secure multimedia content, but this is a more active area of research because, without proper protection, it is vulnerable to unwanted or illegal access by malicious users while in communication, intercepted, or stored over the cloud. Well-known techniques are used to encrypt at the sender side and decrypt at the receiver side. The author proposed a cryptographic technique called Arnold's Cat Map, which uses iteration on the pixels of the image to protect digital multimedia content. It was claimed that this is a novel approach in digital media cryptography. The technique employs chaos functions and maps in the encryption and decryption process. In the first phase, to encrypt and decode the image, two chaotic maps are used to represent different types of images. The details of the image are encrypted and decrypted using Arnold's Cat Map. There is also a logistic map, which is used for black-and-white image encryption and decryption processes.

It is distinguished from existing up-to-date work discussed in the literature review. The implemented system used asymmetric algorithms, i.e., ECC with various curve specifications and the RSA algorithm with various key sizes, which provide a level of security. The limitation of asymmetric algorithms to encrypt and decrypt multimedia content is also addressed, which is not discussed by any researcher. A thorough posterior analysis was conducted compared to other research [16].

5. Research Design

The research work is designed to enhance multimedia content security using modern asymmetric cryptography and a rigorous statistical analysis of the implemented system. The best solution is recommended after a comparative analysis. The scoping and formulation of research, the systematic literature review conducted to analyze the current state-of-the-art techniques, the thematic analysis done to synthesize the key concepts from the literature, and the synthesized findings and discussion insights from the review.

The cryptographic concept for a specific problem in cloud-based applications is used to secure multimedia content. The concepts of privacy and confidentiality in cryptographic systems form the theoretical framework for evaluating the performance of asymmetric algorithms.

The conceptual framework included metrics for evaluating the algorithm's effectiveness in content processing. The complexity of generating key pairs for transforming data into ciphertext is discussed. The adaptability of the dynamic cloud environment, including change and scalability, is analyzed. The algorithm's ability to maintain the privacy and confidentiality of multimedia content during transmission and after storage is evaluated. The size of multimedia contents and their impact when using the asymmetric algorithm are also assessed. Figure 1 illustrates the research design flow: identifying research issues, literature review, formulating research objectives, conducting research, empirical posterior analysis, and discussing results.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 2: 379-393, 2026
DOI: 10.55214/2576-8484.v10i2.12086

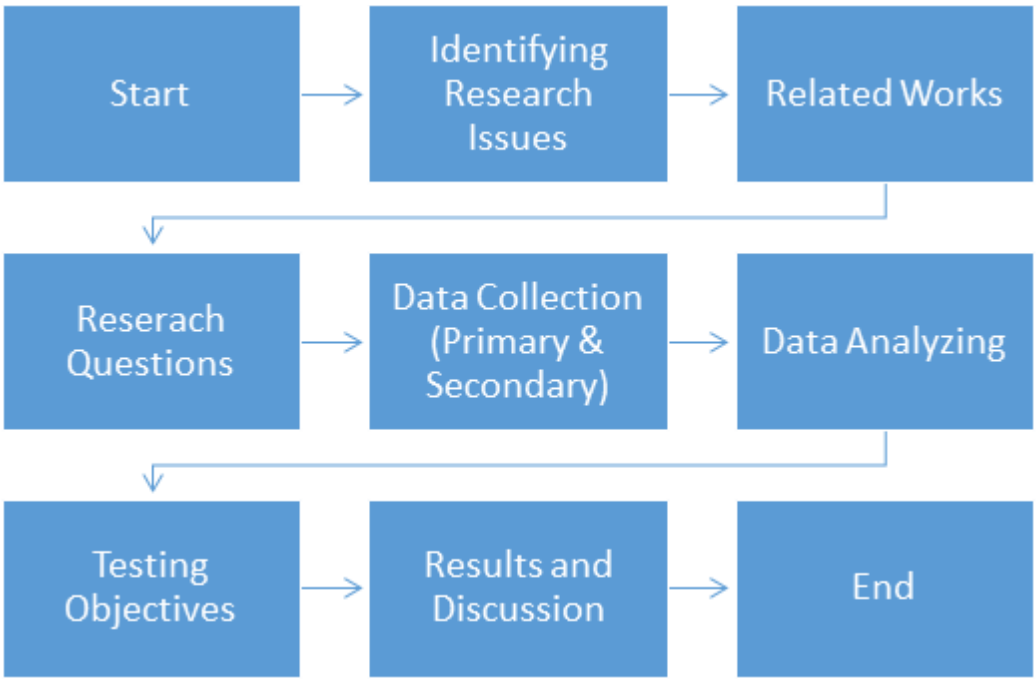

Figure 1.
Research Design Flow.

6. Methodology

The quantitative research approach used in this study and the subsequent analysis of the resources are examined. The controlled cloud environment facilitates the simulation tests. The performance of algorithms for encryption and decryption is systematically measured. Multimedia datasets of small, medium, and large sizes are utilized. Statistical analysis is conducted on the quantitative results obtained from the primary source implemented system. The findings thoroughly discuss the strengths and weaknesses of the algorithm across various datasets. The organized results provided will benefit academics and others interested in using multimedia content within a cloud environment.

7. Experiential Environment

The experimental data were prepared; that is, image, audio, and video. These datasets are classified as small, medium, and large, respectively. The content sizes of the images were 32.2 KB, 202 KB, and 500 KB. The sizes of the audio and video were 1 MB, 10.1 MB, and 14.1 MB. The performance was recorded in milliseconds and microseconds. To collect accurate data, each experiment was conducted ten times. RSA and ECC algorithms with various curve specifications were used for encryption and decryption of the datasets of the image, audio, and video.

The statistical descriptive method is used to analyze data quantitatively. The statistical dispersion of various scatter results and their variability are presented using advanced graphs. The dispersion of values from the means shows the consistent/inconsistent behavior of the algorithm.

The length of the keys of the algorithms varies, which affects the synthesis of findings. The small to large size of the keys of the various asymmetric algorithms, i.e., ECC, RSA, and ElGamal, selected for the experiment to analyze their performance, influences the results.

8. Results and Discussions

Figure 2 depicts the well-known asymmetric algorithms used for key pair generation in bits of ECC (secp5221k1), ElGamal (256), and RSA (4096). The performance of the algorithms for key pair generation was 49, 754.2, and 4,419.9, respectively. The figure illustrates the time taken for each algorithm.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 2: 379-393, 2026
DOI: 10.55214/2576-8484.v10i2.12086

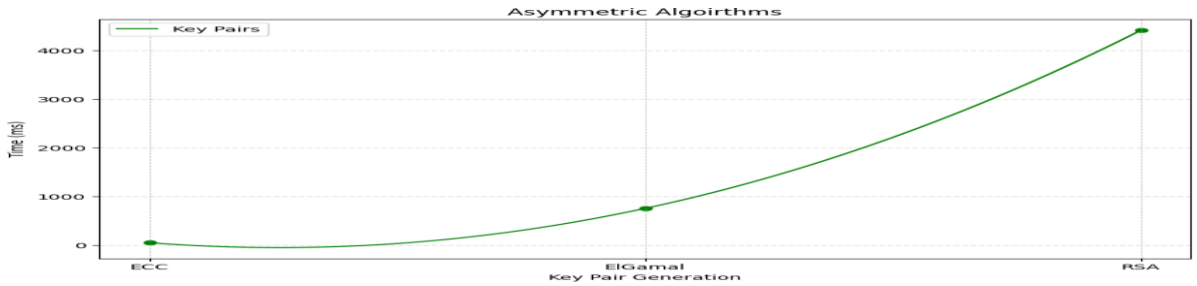

Figure 2.
Empirical Analysis of Asymmetric Algorithm Keys Generation

The posterior analysis of the ECC algorithm encryption and decryption of the small, medium, and large datasets of the image, audio, and video are presented as follows:

ECC asymmetric image encryption and decryption are performed using a hybrid symmetric key, AES, with various ECC key pairs (curve specifications) in bit prime fields, such as secp128r1, secp128r2, secp192r1, and secp256r1.

The following heat graph shows performance, measured in milliseconds, and the scattered values of multimedia content, i.e., images, audio, and video. Each action is executed 10 times, with results recorded for ECC encryption and decryption algorithms, as depicted in Figure 3.

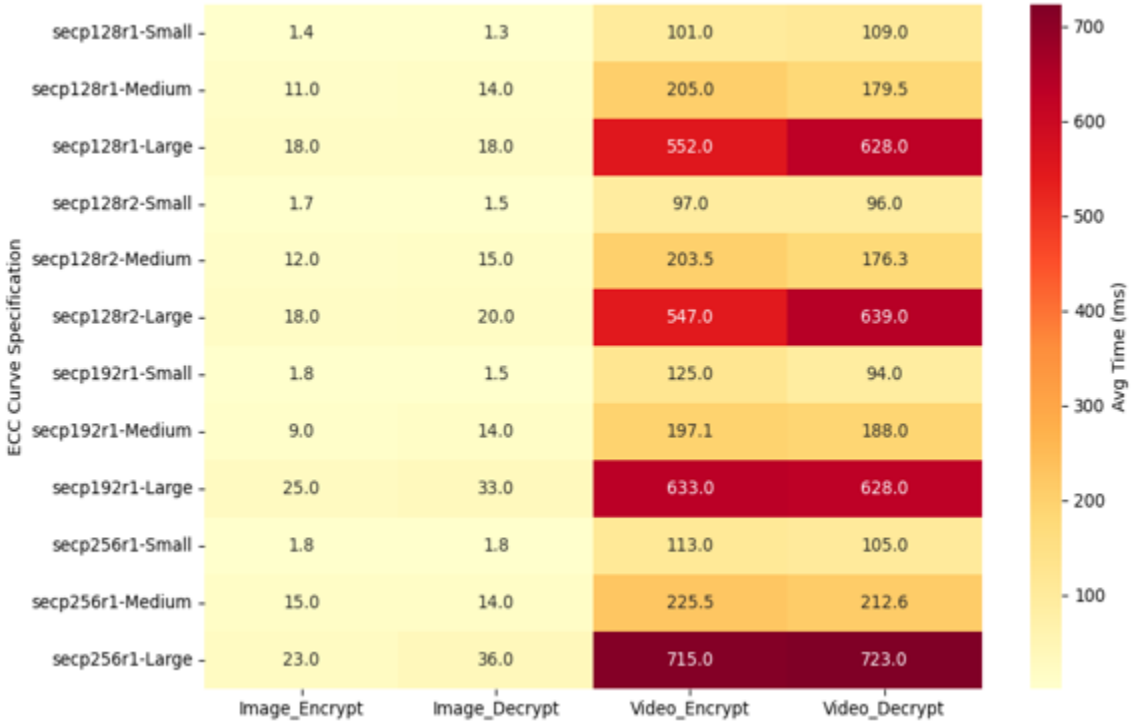

Figure 3.
ECC algorithm performance for multimedia contents.

In the above heat graph, images of various sizes have been encrypted, and decryption has been shown. The statistical analysis is done with the mean value and standard deviation. For small, medium, and large datasets of multimedia contents, i.e., images, using ECC algorithm with a hybrid symmetric key (i.e., AES) with prime field curve specification, i.e., secp128r1, secp128r2, secp192r1, and secp256r1, for encryption and decryption operation. The sizes of the datasets were 32,997 bytes (32.2 KB), 206,993 bytes (202 KB), and 512,017 bytes (500 KB). For small dataset encryption, the performance of the algorithm with

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 2: 379-393, 2026
DOI: 10.55214/2576-8484.v10i2.12086

dispersion from the mean value was 1.4±0.516, 1.72±0.757, 1.8±0.422, and 1.8±0.422, respectively. The decryption operation took 1.3±0.699, 1.47±0.566, 1.47±0.566, and 1.8±0.632, respectively. For the medium dataset, the outcome of the algorithm, i.e., mean value and scatter from mean, was 11±2, 12±2.9, 9±3, and 15±3, respectively. For the decryption operation, the results were 14±3, 15±1, 14±4, and 14±4. For a large dataset, the encryption operation took a mean time with dispersion of 18±2, 18±1, 25±10, and 23±0 (consistent behavior), respectively. For decryption, the algorithm took a mean time and standard deviation of 18±1, 20±1, 33±7, and 36±1, respectively.

The empirical results are depicted as raw data in Figure 4 of the multimedia contents, including image, audio, and video. The outcome revealed that it is directly proportional and correlated with key size, meaning encryption time of data increases simultaneously, and decryption operation takes more time when the size of the key increases.

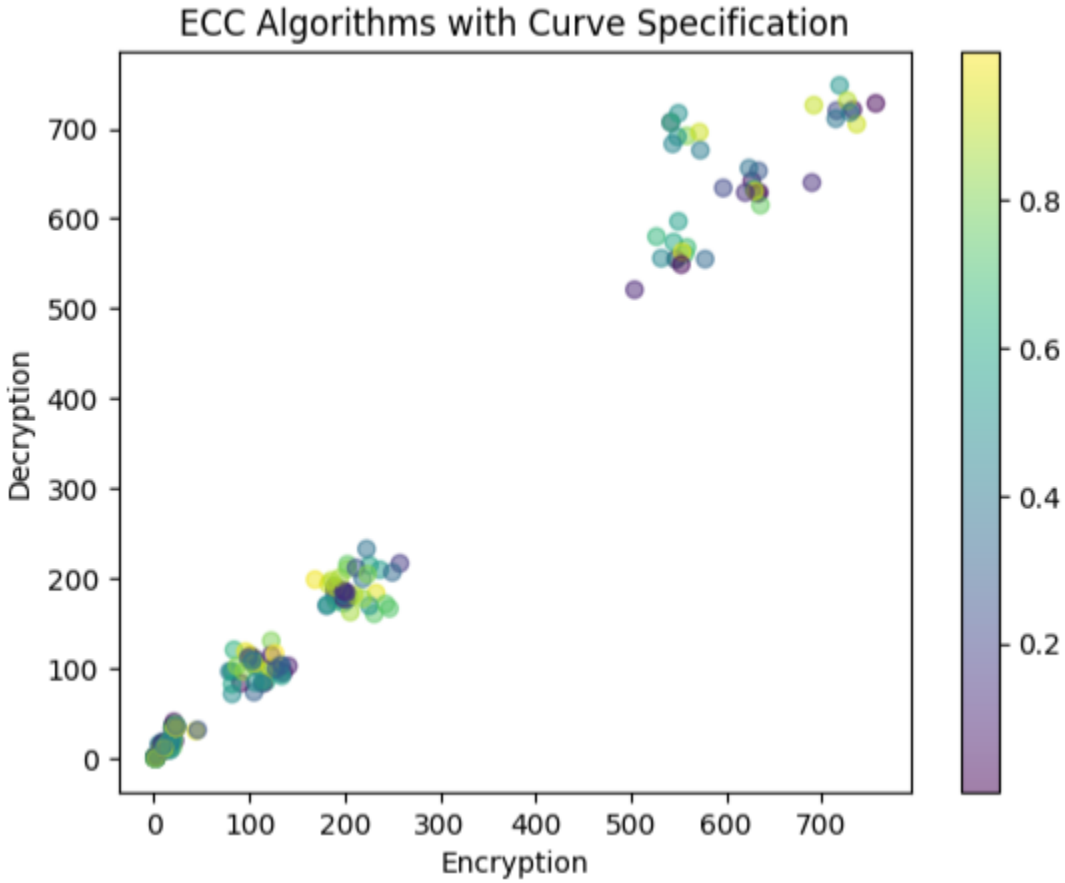

Figure 4.
ECC algorithm Performance for raw multimedia data

Figure 5 depicts a comparative analysis in a histogram and scatter plot of the encryption operation of the ECC algorithm with key curve specifications, i.e., secp128r1, secp128r2, secp192r1, and secp256r1. The synthesis shows the ECC algorithm with various curve specifications; when the size of the key increases, it directly affects the performance of the algorithm and takes more time for decryption operations.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 2: 379-393, 2026
DOI: 10.55214/2576-8484.v10i2.12086

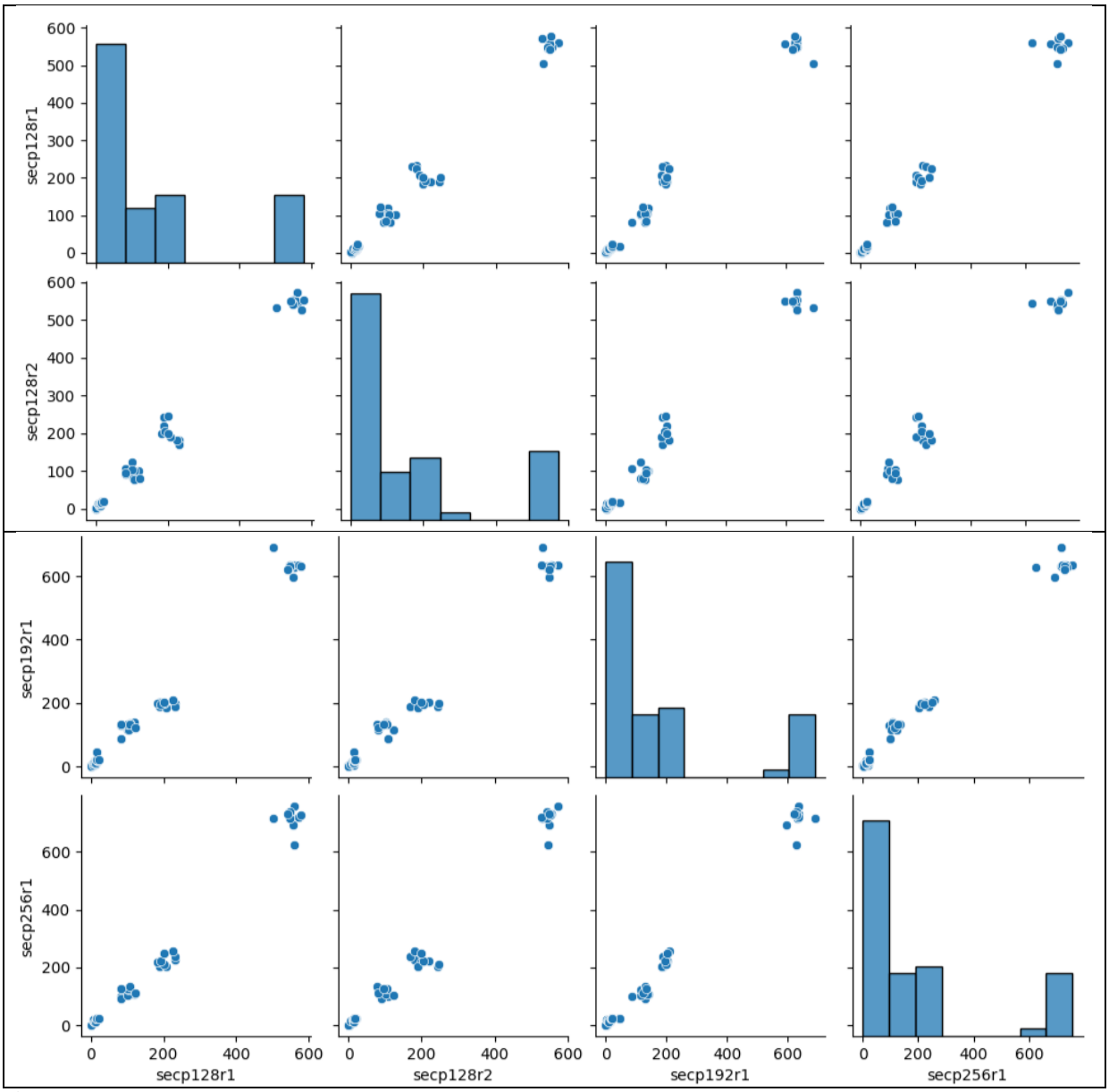

Figure 5.
ECC algorithm performance with curve specification encryption of the multimedia contents (image, audio, and video).

Figure 6 illustrates the comparative analysis in a histogram and scatter plot of the encryption operation of the ECC algorithm with curve specifications. The results indicate that the size of the key has a significant impact on the algorithm's performance.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 2: 379-393, 2026
DOI: 10.55214/2576-8484.v10i2.12086

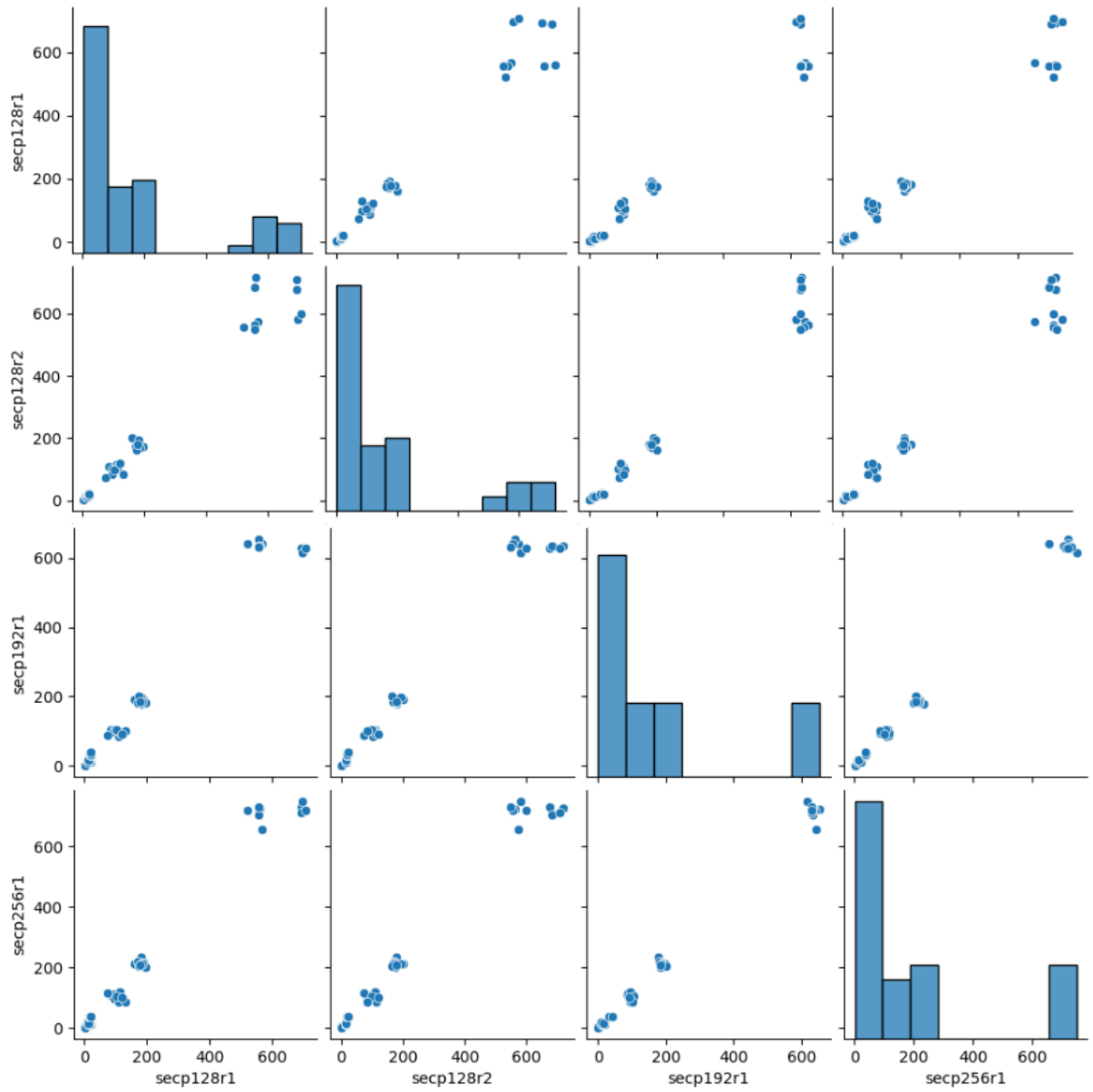

Figure 6.
ECC algorithm performance with curve specification decryption of the multimedia contents (image, audio, and video).

Figure 7 shows that the ECC algorithm took time for the decryption operation of small, medium, and large datasets, where the data size increases in conjunction with the increased size of the key.

For small, medium, and large datasets of multimedia content, i.e., audio and video, using the ECC algorithm with a hybrid symmetric key (AES) and prime field curve specifications such as secp128r1, secp128r2, secp192r1, and secp256r1 for encryption and decryption operations, the dataset sizes were 1,055,736 bytes (1.00 MB), 10,680,262 bytes (10.1 MB), and 14,813,476 bytes (14.1 MB). The algorithm's performance was recorded in milliseconds. For the small dataset, the mean values for each encryption operation were 101, 97, and 113, while decryption times were 109, 96, 94, and 105. For the medium dataset, the results for encryption were 205, 203.5, 197.1, and 225.5, with decryption times of 179.5, 176.3,

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 2: 379-393, 2026
DOI: 10.55214/2576-8484.v10i2.12086

188, and 212.6. For the large dataset, encryption results were 552, 547, 633, 715, and decryption results were 628, 639, 628, 723, respectively.

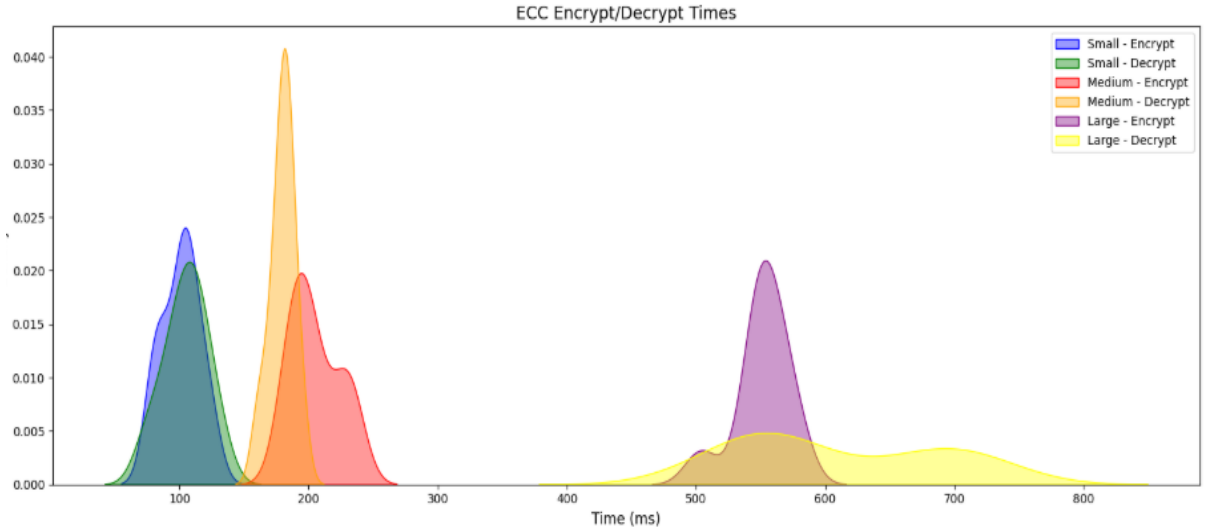

Figure 7.
ECC algorithm performance for multimedia contents (audio and video).

Figure 8 depicts the cumulative difference in performance between encryption and decryption operations on various datasets, small, medium, and large, for audio and video, using the ECC algorithm's encryption and decryption methods.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 2: 379-393, 2026
DOI: 10.55214/2576-8484.v10i2.12086

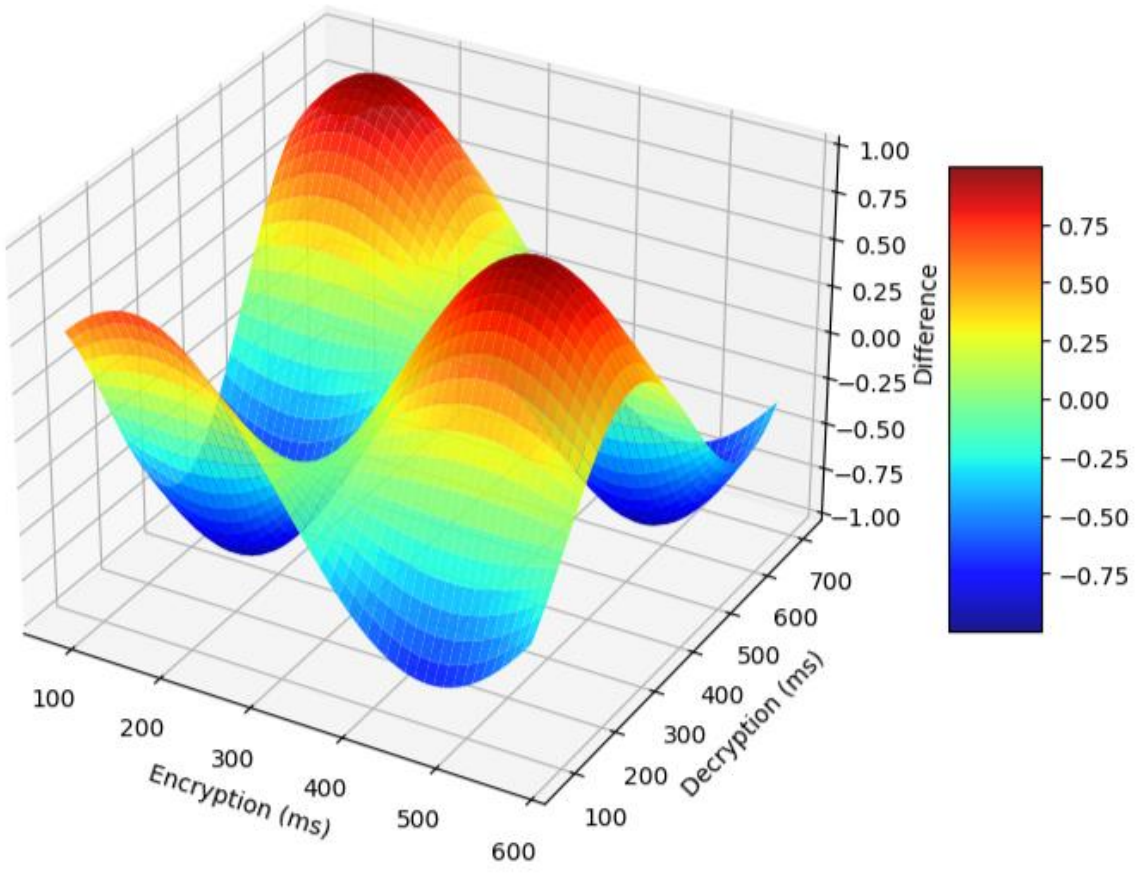

Figure 8.
ECC algorithm difference between encryption and decryption of the multimedia contents (audio and video).

In Figure 9, the histogram shows the result classification of the encryption and decryption operations performed in the small, medium, and large datasets of the multimedia contents, i.e., audio and video.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 2: 379-393, 2026
DOI: 10.55214/2576-8484.v10i2.12086

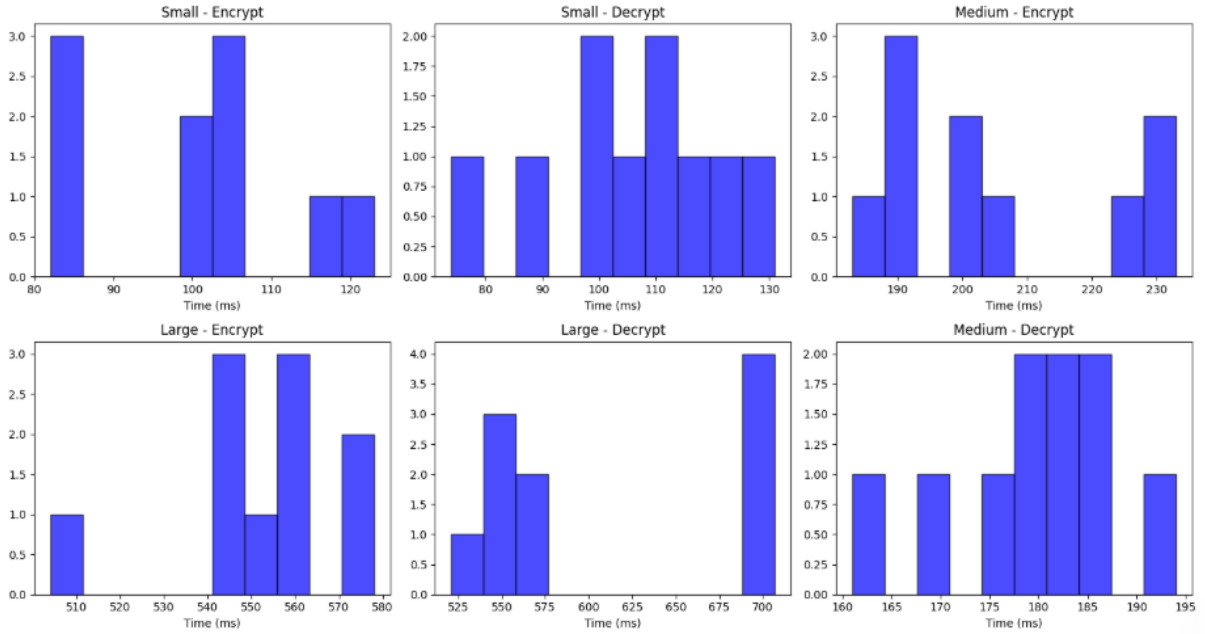

Figure 9.
ECC algorithm performance classification of multimedia contents (audio and video).

Figure 10 depicts multimedia contents, i.e., audio and video, where the dispersion value from the mean shows small, medium, and large datasets. For encryption, the small dataset's ECC algorithm took an average time with dispersion, i.e., 100.0 ± 14.3; the decryption process took an average time with dispersion, i.e., 104.6 ± 16.8. For the medium dataset, the mean and standard deviation were 205.0 ± 18.6; meanwhile, the decryption process took 179.5 ± 9.3. For the large dataset, encryption took a mean time with dispersion, i.e., 552.5 ± 20.1; decryption took 610.3 ± 75.5.

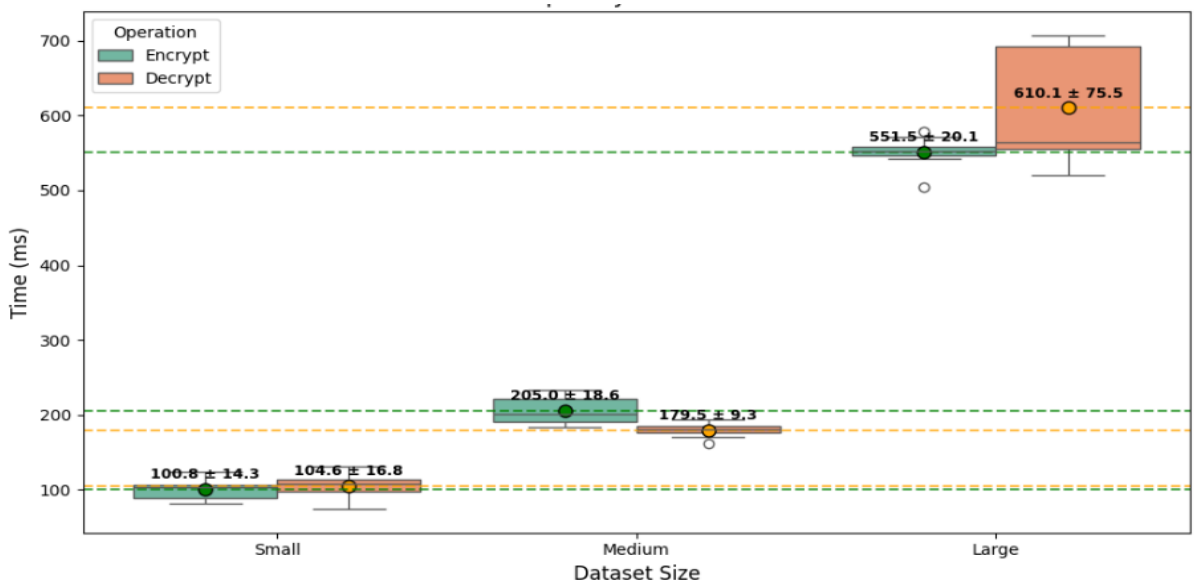

Figure 10.
ECC algorithm performance and dispersion of values from the means of multimedia contents (audio and video).

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 2: 379-393, 2026
DOI: 10.55214/2576-8484.v10i2.12086

This empirical research used well-known asymmetric algorithms with maximum key size to provide a higher level of security. It was found that the ElGamal and RSA algorithms have limitations in dataset size. Both algorithms cannot perform encryption or decryption on small, medium, and large datasets. Therefore, these algorithms are unsuitable for multimedia content security over the cloud.

There is only an ECC algorithm that can perform all datasets of multimedia contents, i.e., image, audio, and video encryption and decryption operations. The performance of the ECC algorithm with prime fields and various curve specifications was the fastest and most secure, with small key sizes in bits compared to other algorithms.

9. Conclusion

Cloud-based applications to store multimedia content are growing as there is a need for secure systems that use modern cryptographic algorithms for real applications. The outcomes of this research work contribute to enhancing the security of applications running over the cloud. It is suggested that continual research be done to ensure the protection of private and confidential data using cryptographic solutions that remain resilient to changing cyber threats in the dynamic context of the cloud environment. The limitation of asymmetric algorithms is that both ElGamal and RSA are unsuitable for multimedia content security over the cloud because they cannot perform encryption or decryption operations on small, medium, and large datasets. The results provide insight into the decision to choose an asymmetric algorithm for safeguarding multimedia content over the cloud. Findings identify the most secure, efficient, and flexible algorithm in the ever-changing world of cloud-based multimedia services. The comparative analysis seeks to help select the most secure and appropriate algorithm based on priorities. ECC emerged with higher performance with a small key length; it is ideal and computationally efficient for resource-constrained cloud environments. The findings will assist researchers and decision-makers when choosing modern algorithms for securing multimedia content running over the cloud.

Transparency:

The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

References

[1] N. I. Ali, I. A. Brohi, M. U. R. Jamali, M. B. Arain, and A. R. Nangraj, "A revolutionary approach using artificial intelligence and quantum cryptography – A review," *International Journal of Innovations in Science & Technology*, vol. 7, no. 3, pp. 1422–1436, 2025. https://doi.org/10.33411/ijist/202573142214 36

[2] D. M. Alsaffar *et al.*, "Image encryption based on AES and RSA algorithms," in *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-5). IEEE*, 2020.

[3] M.-u.-R. Jamali, N. I. Ali, A. G. Memon, M.-u.-R. Maree, and A. Jamali, "Architectural design for data security in cloud-based big data systems," *Baghdad Science Journal*, vol. 21, no. 9, p. 5, 2024. https://doi.org/10.21123/bsj.2024.8722

[4] X. Duan, D. Guo, N. Liu, B. Li, M. Gou, and C. Qin, "A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network," *IEEE Access*, vol. 8, pp. 25777-25788, 2020. https://doi.org/10.1109/ACCESS.2020.2971528

[5] B. Yu, R. Sun, and Z. Fu, "A novel probabilistic visual cryptography scheme using EDBS for grayscale image," in *2020 IEEE 6th International Conference on Computer and Communications (ICCC) (pp. 1427-1432). IEEE*, 2020.

[6] C. Blundo, S. Cimato, and A. De Santis, "Visual cryptography schemes with optimal pixel expansion," *Theoretical Computer Science*, vol. 369, no. 1-3, pp. 169-182, 2006. https://doi.org/10.1016/j.tcs.2006.08.008

[7] L. Zhang, X. Yuan, K. Wang, and D. Zhang, "Multiple-image encryption mechanism based on ghost imaging and public key cryptography," *IEEE Photonics Journal*, vol. 11, no. 4, pp. 1-14, 2019. https://doi.org/10.1109/JPHOT.2019.2923705

[8] B. Yan, Y. Xiang, and G. Hua, "Improving the visual quality of size-invariant visual cryptography for grayscale images: an analysis-by-synthesis (AbS) approach," *IEEE Transactions on Image Processing*, vol. 28, no. 2, pp. 896-911, 2018. https://doi.org/10.1109/TIP.2018.2874378

[9] S. J. Shyu, "Image encryption by random grids," *Pattern Recognition*, vol. 40, no. 3, pp. 1014-1031, 2007. https://doi.org/10.1016/j.patcog.2006.02.025

[10] Y. Ke, M. Zhang, X. Zhang, J. Liu, T. Su, and X. Yang, "A reversible data hiding scheme in encrypted domain for secret image sharing based on Chinese remainder theorem," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 32, no. 4, pp. 2469-2481, 2021. https://doi.org/10.1109/TCSVT.2021.3081575

[11] R. Sun, Z. Fu, and B. Yu, "Size-invariant visual cryptography with improved perceptual quality for grayscale image," *IEEE Access*, vol. 8, pp. 163394-163404, 2020. https://doi.org/10.1109/ACCESS.2020.3021522

[12] Y. Lin, Z. Ning, J. Liu, M. Zhang, P. Chen, and X. Yang, "Video steganography network based on 3DCNN," in *2021 International Conference on Digital Society and Intelligent Systems (DSInS) (pp. 178-181). IEEE*, 2021.

[13] A. K. Singh, K. Chatterjee, and A. Singh, "An image security model based on chaos and DNA cryptography for IIoT images," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1957-1964, 2022. https://doi.org/10.1109/TII.2022.3176054

[14] Y. Fouzar, A. Lakhssassi, and M. Ramakrishna, "A novel hybrid multikey cryptography technique for video communication," *IEEE Access*, vol. 11, pp. 15693-15700, 2023. https://doi.org/10.1109/ACCESS.2023.3242616

[15] Y. Huang, Z. Lei, Z. Song, Y. Guo, and Y. Li, "A video steganography scheme based on post-quantum cryptography," in *2021 IEEE International Conference on Information Communication and Software Engineering (ICICSE) (pp. 83-87). IEEE*, 2021.

[16] S. Guhe, P. Kodhe, S. Khiradkar, S. Dasgupta, S. Lokhande, and S. Kamble, "Video cryptography with chaos," in *2023 11th International Conference on Emerging Trends in Engineering & Technology-Signal and Information Processing (ICETET-SIP) (pp. 1-6). IEEE*, 2023.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 2: 379-393, 2026
***DOI:** 10.55214/2576-8484.v10i2.12086*