Journal of Computer Science

Original Research Paper

Performance Analysis of Two Famous Cryptographic Algorithms on Mixed Data

[1,2,3]Emmanuel Abidemi Adeniyi, [4,5]Agbotiname Lucky Imoize, [6]Joseph Bamidele Awotunde, [7,8]Cheng-Chi Lee, [1,2,3]Peace Falola, [6]Rasheed Gbenga Jimoh and [9]Sunday Adeola Ajagbe

[1]*Department of Computer Sciences, Precious Cornerstone University, Ibadan, Oyo State, Nigeria*
[2]*PUCRID Center, SDG 9 (Industry, Innovation, and Infrastructure Research Group), Precious Cornerstone University, Ibadan, Oyo State, Nigeria*
[3]*PUCRID Center, SDG 4 (Quality Education), Precious Cornerstone University, Ibadan, Oyo State, Nigeria*
[4]*Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Lagos, Akoka, Lagos 100213, Nigeria*
[5]*Department of Electrical Engineering and Information Technology, Institute of Digital Communication, Ruhr University, 44801 Bochum, Germany*
[6]*Department of Computer Science, Faculty of Information and Communication Sciences, University of Ilorin, Ilorin 240003, Nigeria*
[7]*Department of Library and Information Science, Fu Jen Catholic University, New Taipei City 24205, Taiwan*
[8]*Department of Computer Science and Information Engineering, Asia University, Taichung City 41354, Taiwan*
[9]*Department of Computer and Industrial Production Engineering, First Technical University, Ibadan, 200255, Nigeria*

Article history
Received: 01-02-2023
Revised: 11-03-2023
Accepted: 06-04-2023

Corresponding Author:
Cheng-Chi Lee
Department of Library and Information Science, Fu Jen Catholic University, New Taipei City 24205, Taiwan
Email: cclee@mail.fju.edu.tw

Abstract: The rapid development of digital data sharing has made information security a crucial concern in data communication. The information security system heavily relies on encryption methods. These algorithms employ strategies to increase data secrecy and privacy by obscuring the information, which only those parties who have the accompanying key can decode or decrypt. Nevertheless, these methods also use a lot of computational resources, including battery life, memory, and CPU time. So, to determine the optimal algorithm to utilize moving forward, it is necessary to assess the performance of various cryptographic algorithms. Therefore, this study evaluates two well-known cryptographies (RSA and ElGamal) using mixed data such as binary, text, and image files. CPU internal clock was used to obtain the time complexity used by both algorithms during encryption and decryption. The algorithms used CPU internal memory to obtain memory usage during the encryption and decryption of mixed data. Evaluation criteria such as encryption time, decryption time, and throughput were used to compare these encryption algorithms. The response time, confidentiality, bandwidth, and integrity are all factors in the cryptography approach. The results revealed that RSA is a time-efficient and resourceful model, while the ElGamal algorithm is a memory-efficient and resourceful model.

Keywords: Cryptographic Algorithms, Asymmetric Encryption, RSA, ElGamal, Complexity

Introduction

Data security is the science and study of strategies for securing data from unauthorized disclosure and alteration in computer and communication systems. With the exponential increase in data communication and transfer volume and the proliferation, diversification, and intensity of malicious activities, the need to ensure and sometimes enforce data security has become even more urgent and critical (Li *et al*., 2022). Consequently, research activities in data security have evolved rapidly and have produced exciting developments in related application fields of computer security, such as cryptography. Cryptography is a technique for preventing illegitimate access to information and data. Cryptography is the act of securing data and information through encryption and decryption. It is always synonymous with transforming plain text (ordinary text, also referred to as simple text) into cipher text (a method called encryption), then back again as plain text (known as decryption) (Adeniyi *et al*., 2022).

The quick and broad adoption of different connectivity and communication methods like social networks and wearable devices among others, have made it easier for people to exchange information over the internet. Digital images are currently among the most significant pieces of information shared online, particularly on social media.

This is a result of the widespread use and quick development of wearable cameras, which are present in phones, homes, hospitals, and satellites used by the military and other places. Furthermore, the information conveyed by the photos is crucial and extremely helpful and can fall under the heading of a private concern (Panda and Nag, 2015). The development of new networking solutions is being driven by the demand for omnipresent personal communications. People spend a lot of time online, so information security has grown to be a crucial component of data exchange. The fact that most of the data intruders obtain from a system is in a form that can be read and understood is one of the main factors contributing to their effectiveness. Several methods are used to increase the security of the data being transmitted.

The use of cryptography, which is the art and science of protecting information from undesired individuals by changing it into a form indiscernible to its attackers while it is kept and delivered, is an essential technique for maintaining secrecy (Panda and Nag, 2015). It serves as a fundamental building piece for information system construction. It has to do with the study of mathematical methods connected to information security elements including confidentiality, data integrity, and data authentication (Yu *et al*., 2016). The word "plaintext" or "clear text" refers to data that can be read and comprehended without the use of any additional security measures. It serves as a fundamental building piece for information system construction. It has to do with the study of mathematical methods connected to information security elements including confidentiality, data integrity, and data authentication (Singh *et al*., 2022). The word "plaintext" or "clear text" refers to data that can be read and comprehended without the use of any additional security measures.

Additionally, there are numerous crucial uses for digital images, including in the fields of medicine, online banking, online shopping, telecommunications, and many others (Rajabi *et al*., 2021; Adeniyi *et al*., 2023). Because they are being distributed over an open network, it is crucial and imperative to safeguard these images. Also, any carelessness or omission in this regard jeopardizes the confidentiality of sensitive data. The most crucial method of data protection is encryption (Meng *et al*., 2018). As a result, researchers have addressed this issue and put forth numerous approaches for image encryption (Banu and Amirtharajan, 2020; Brahim *et al*., 2020; Hamza and Titouna, 2016). Nonetheless, there are a few characteristics that set digital image information apart from text-based information. The strongest association between image pixels, the volume of information, the frequency and level of redundancy of pixels, and others (Pourjabbar Kari *et al*., 2021) are the most significant of these.

Images cannot be secured using traditional methods for text data encryption (Talhaoui and Wang, 2021). They may not always function well with images, be open to some attacks and be slow to execute, especially when shared in real-time (Khalil *et al*., 2021). The family of Elliptic Curve based Encryption (ECC) and the most popular encryption techniques Data Encryption Standard (DES), Advanced Encryption Standard (AES), Rivest Shamir Adleman (RSA) and have more criteria for the security of digital images (Oğraş and Türk, 2016; Nkandeu and Tiedeu, 2019). Images must be encrypted using traditional encryption techniques, which take more time, processing power, and high performance (Avasare and Kelkar, 2015). To create ways and methods of encrypting images that are strong and resistant to attacks of all kinds and can be executed quickly in real-time and other such things, it has become necessary to use other techniques and methods that are sensitive to and take into account the characteristics of images (Jan *et al*., 2022; Abutaha *et al*., 2022). As a result, many encryption algorithms have been developed based on various theories, including DNA computing (Liao *et al*., 2018; Zhang *et al*., 2013), neural networks (Maddodi *et al*., 2018), cellular automata (Khedmati *et al*., 2020), compressive sensing (Brahim *et al*., 2020), optical transformation (Kaur *et al*., 2020), quantum theory (Musanna and Kumar, 2020) and chaotic maps (Kaur *et al*., 2020; Niu *et al*., 2020; Pourjabbar Kari *et al*., 2021). More recently, there is also visually meaningful encryption (Huang *et al*., 2023; Ye *et al*., 2021), asymmetric image encryption (Ibrahim and Alharbi, 2020; Ye *et al*., 2022), and multi-image encryption (Ye *et al*., 2021).

Continually performed cryptanalysis of current chaotic image encryption techniques is done in addition to studying encryption algorithms to show the level of security and to expose weaknesses in the encryption algorithms. Particularly, several chaotic-based encryption algorithms have been defeated because they were unable to fend off a known or specific plaintext assault (Hu *et al*., 2017; Awotunde *et al*., 2022). Because of this, it is constantly necessary to develop new technologies and algorithms to defend digital images against these inventive attacks. The intricacy of an algorithm is the measure that evaluates the number of resources, such as time, space, energy, and so on, that the algorithm requires. It is a measure of how 'good' the algorithm is at solving the problem. It can also be described as the efficiency of the algorithm in terms of the amount of data the algorithm must process (Abdulraheem *et al*., 2021a). Typically, the complexity of an algorithm is a function that maps the input length/size to the number of main stages (time complexity) or specific storage positions (space complexity). Some algorithms are more efficient than others, so having metrics for comparing their efficiency will be necessary; therefore, this study aims to determine the time and space complexity of RSA and ElGamal cryptographic algorithms on mixed data (text, image, audio, and video) datasets.

Several studies have recently examined the performance evaluation of RSA and ElGamal cryptographic algorithms on text, audio, and image data. This section gives a detailed summary of studies conducted concerning the time and space complexity of RSA and ElGamal cryptographic algorithms. The methods applied are reviewed based on their relatedness to this study.

Kayalvizhi *et al*. (2010), the authors worked on the performance and comparison of RSA and ElGamal cryptography algorithms by assessing their power productivity and network lifespan. The researcher used a group-based wireless network topology situation with NS2 to investigate the performance of the collection. The information was scrambled at the foundation node and the ciphertext was sent to the target node through the cluster heads. The power consumption of RSA and ElGamal algorithms was analyzed and showed that RSA uses fewer resources and thus improves the life of the network relative to ElGamal. From the findings, the RSA algorithm has improved support for wireless communications and absorbs 14.5 percent less power than the ElGamal algorithm. The study was limited to 10 sensor nodes of the wireless network.

Arora *et al*. (2013) suggested introducing cryptographic algorithms in Java programming language to create safe cloud data by using diverse features to distinguish between symmetric and asymmetric techniques such as AES, DES, blowfish, and RSA. They reported that AES used the minimum time to execute cloud data. Blowfish used less memory consumption. DES has invested the least amount of time in cryptography. RSA has spent the most time in cryptography and the highest memory capacity. In another study (Boni *et al*., 2015), the authors suggested a novel methodology to enhance the Diffie-Hellman algorithm, thereby involving complicated calculations that increase the computational complexity when producing shared keys called the multipliers key exchange technique. They reported that the multiplicative key exchange is better than the Diffie-Hellman algorithm in terms of execution time, thus, needs few computations compared with the Diffie-Hellman algorithm. The new method is used when keys are generated frequently and faster instead of protection where systems are not complicated or have a reduced setup.

Okeyinka (2015), the authors worked on RSA and ElGamal Algorithms computing speeds performance for securing, confidentiality, and authentication of text data. The researcher used an internal computer clock for both RSA and ElGamal to compare and determine the execution times of each input text data and which one of the two methods is more computationally effective. The implementation of the work was checked with text details in different sizes. The result showed that RSA is more computationally efficient than ElGamal, which makes it perform better than ElGamal. However, the limitation of this research work is that text data was used with a limited character size.

Bhanot and Hans (2015), the authors evaluated the comparative analysis of encryption algorithms. AES, RSA, and DES encryption algorithms were implemented on audio and video files of different sizes to determine the encryption and decryption time. The result showed that AES is best in terms of encryption and decryption time compared with the performances of RSA and DES under the same condition. The study was limited to certain metrics for comparative analysis. Thu *et al*. (2019), the authors discussed the encryption and decryption time performance analysis of RSA and ElGamal public key cryptosystems. The researcher encrypted the plaintext (text, image, and audio) file with a public key for RSA and ElGamal and showed the encryption time comparison for the two algorithms. The result shows that RSA is about four times faster than ElGamal during the encryption process and RSA is faster than ElGamal during the decryption process. The result contradicted the previously reviewed works that ElGamal is faster than RSA during the decryption process. However, the comparison is only based on encryption and decryption time for text, image, and audio data.

Sari *et al*. (2020) examined the comparative study of LUC, ElGamal, and RSA algorithms in encoding texts. The study implements each algorithm using several texts to determine the encryption and decryption time. The result showed that the RSA algorithm performed better in text file encryption process time, while the LUC algorithm performed better in decryption. The work was limited to encrypting the secret message in text form. Desai *et al*. (2022), the authors examined several asymmetric public key cryptosystems. The research is comprehensive and subtle and it analyzes asymmetric public-key cryptosystems focused on performance-based criteria and metrics. The research entails a thorough, comparative, and in-depth examination of the RSA, ElGamal, and ECC-ElGamal public key cryptosystems. The study aims to produce clear conclusions on the performance requirements of the algorithms under consideration.

In another development, (Parenreng and Wahid, 2022) proposed using the ElGamal encryption model to distribute the symmetric key. The AES encryption model is a fairly secure algorithm to protect message data or confidential information. The study implemented cryptography algorithms in the email system, which was used to encrypt messages and data to be sent via email effectively and efficiently. The study aimed to address email security problems, especially regarding data leakage when sending emails via email.

Advanced security techniques are strictly desired to ensure the security of user information through these safety-limited channels. However, the existing encryption systems cannot guarantee the user data's security and authentication on these online platforms. Hence, Certificate Group Signcryption Systems (CGSS) are necessary.

Meshram *et al*. (2021) uses conformable chaotic maps. This research provides an effective electronic currency (CCM) system based on CGSS. According to the study, any group signcrypter would work with the group manager to encrypt information or data (GM) and send it to the verifier, who uses the group's public criteria to verify the veracity of the sign-encrypted information/data. Furthermore, the CGSS-CCM ECS scheme's traceability, unforgeability, unlikability, and robust security have all been created using computationally challenging problems. The study's performance evaluation demonstrates that it is resistant to the indiscernible chosen cipher text attack. Meshram *et al*. (2022) proposed a novel lightweight speck cryptographic algorithm to enhance the security of cloud computing for healthcare data. Unlike the cryptographic techniques frequently used in cloud computing, the exploratory findings of the suggested methodology demonstrated a high degree of security, a clear enhancement in the speed at which data is encrypted, and the level of security that may be attained.

Similarly, Abdulraheem *et al*. (2021b) suggested a simple, provably secure certificateless method for group oriented signcryption (CGST) using Fractional Chaotic Maps (FCM). Any group signcrypter may encrypt data or information with the Group Manager (GM) and have it delivered to the verifier without interruption using the CGST-FCM protocol. When used in real-time security applications, the network security from the study demonstrates appreciable consistency and high efficiency. Finally, Kaur *et al*. (2020) proposed an enhanced lightweight cryptography algorithm to secure IoT-based environments from attackers. Results indicate that the algorithm is more effective and safer in an IoT-driven setup, making it better suited for data security.

Oladipupo *et al*. (2023) proposed a WSN paradigm that uses multicore WS clustering. The current Elliptic Curve Cryptographic (ECC) technique is enhanced for security against simple assaults and parallel execution of the encryption and decryption procedures. The key exchange mechanism was Elliptic Curve Diffie-Helman (ECDH) and the communication nodes were authenticated using Elliptic Curve Digital Signature Algorithm (ECDSA). Analyses of the model's security and performance compared to others were shown.

Materials and Methods

This study implements RSA and ElGamal cryptographic algorithms to obtain Encryption time, Decryption time, and the memory usage of both algorithms on mixed datasets. The data used were extracted from various data repositories such as (lipsum, datahub, Kaggle, and random text generators). Figure 1 displays the framework that was used in this study. The framework shows the phases involved in developing the models, including loading mixed data for processing encryption and decryption with RSA and ElGamal cryptographic algorithm for further analysis like time and space complexities.

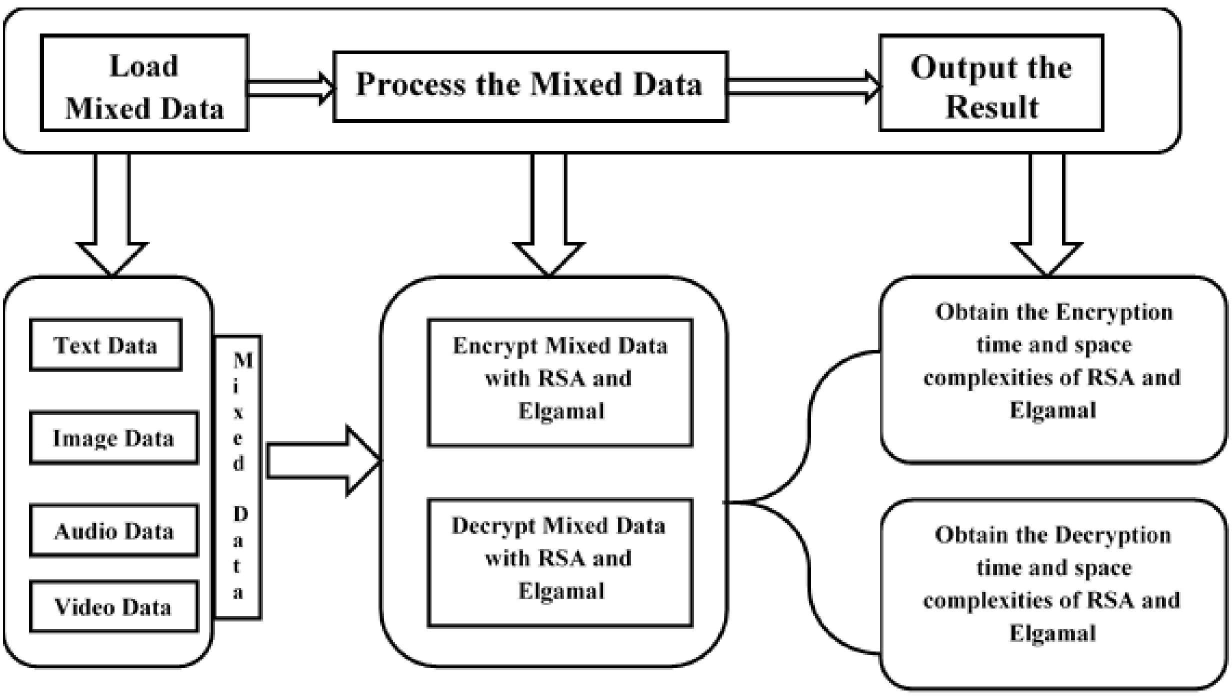

Fig. 1: Conceptual framework of the study

Figure 1 shows the Hierarchical Input Process Output (HIPO) of the study. This displays the stages involved in obtaining the desired result of this research. The mixed data which includes (text, image, audio, and video) are the input tools in the study. The second stage of the framework is the process tool which includes RSA and ElGamal cryptographic algorithms to scramble the input data into unreadable content. The third stage is the result stage, which displays the complexities of each of the algorithms used. Finally, the time and memory usage of RSA and ElGamal are obtained and their performance is compared to determine which algorithms perform better on mixed data:

RSA algorithm

Key generation

The key generation process is detailed below:

1. Get two integers, p and q from the user.
2. Check if p and q are prime.
   2.1 If prime, continue the process, else exit the code
3. Calculate $(p-1)*(q-1)$ and name it $\phi(n)$
4. Calculate $n = p * q$
5. Get an input e to act as private key, under the condition that $1 < e < \phi(n)$ and gcd $(e, \phi(n)) = 1$ (gcd-greatest common divisor)
6. Compute the value of d such that $1 < d < \phi(n)$ $and\, e.d \equiv 1(\bmod \phi(n))$.

Note: The public key is (n, e) and the private key is (n, d)
The values of (p, q), and $\phi(n)$ are private. 'e' is the public or encryption exponent. 'd' is the private or decryption exponent.

Encryption and decryption

Given the message to be M and Cipher C

$$C = M^e \bmod n$$

Decryption is done using the private key (d, n)

$$M = C^e \bmod n$$

ElGamal algorithm

Key generation

Generate a large random prime number (p)
Choose a generator number (a)
Choose an integer (x) less than (p-2), as the secret number
Compute (d) where (d) = $a^x \bmod p$
The private key is given as (x) and the public key as (p, a, d)

Encryption and decryption

Represent the plaintext as an integer m where: $0 < m < p-1$
Encryption is done using the public key (p, a, d)
Choose an integer k such that: $1 < k < p-2$
Compute y, $y = a^k \bmod p$
Compute z, $z = (d^k * m) \bmod p$
The ciphertext is given as $C = (y, z)$

Decryption is done using the private key (x)
The receiver obtains the ciphertext $C = (y, z)$
Compute (r) as follows: $r = y^{(p-1-x)} \bmod p$
Recover the plaintext as follows: $m = (r * z) \bmod p$

Performance Analysis Measurement Factors

In this study, the following factors are used as encryption efficiency criteria.

Encryption time: This is the running time the algorithm used throughout the encryption of mixed data, this is obtained through the computer internet clock.

Decryption time: This is the time taken during the decryption of mixed

Encryption memory: This factor is related to the amount of computer internet memory used during the mixed data encryption process.

Decryption memory: This factor is related to the amount of computer internet memory used during the decryption process of mixed data.

CPU internal clock: This is used to obtain the encryption and decryption time for all the categories of data.

CPU internal memory: This is used to obtain the memory space used by both algorithms during the encryption and decryption of all categories of data.

Results and Findings

RSA and ElGamal cryptographic algorithms were implemented in c-sharp programming language on mixed data (text, image, audio, and video). The experimental results of each dataset are indicated using tables and figures. For example, Table 1-8 gives the time taken to encrypt and decrypt each dataset are given in seconds (s), while the space (memory) used to encrypt and decrypt each dataset is given in kilobytes (KB). Figures 2-17 give the graphical representation of each table in terms of time and memory usage.

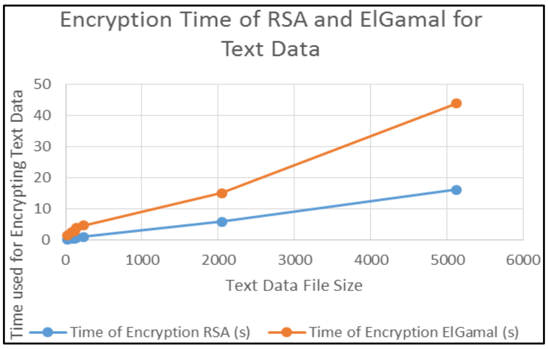

Fig. 2: Encryption time analysis for RSA and ElGamal cryptographic algorithms for text dataset

Table 1: Tabular representation of text data encryption for RSA and ElGamal algorithms

		Time of encryption		Space of encryption	
S/N	File size (KB)	RSA (s)	ElGamal (s)	RSA (kb)	ElGamal (kb)
1	22	0.1082	1.55	169.82	0.1650
2	80	0.3545	2.57	623.50	77.9300
3	120	0.4835	2.92	925.85	115.7100
4	140	0.5664	3.80	1054.83	131.8400
5	230	0.9315	4.67	1740.99	217.6200
6	2048	5.8852	15.12	11133.64	1391.7000
7	5120	16.1733	43.90	30116.30	3764.5200

Table 2: Tabular representation of text data decryption for RSA and ElGamal algorithms

		Time of decryption		Space of decryption	
S/N	File size (KB)	RSA (s)	ElGamal (s)	RSA (kb)	ElGamal (kb)
1	22	1.0756	0.0802	21.22	0.1650
2	80	3.9254	1.6674	77.93	77.93
3	120	5.7463	1.9284	115.71	115.71
4	140	6.8078	2.2112	131.84	131.84
5	230	11.1189	3.2596	217.62	217.62
6	2048	74.9069	19.3083	1391.69	1391.70
7	5120	194.2630	56.1963	3764.52	3764.52

Table 3: Image data encryption for RSA and ElGamal algorithms

		Time of encryption		Space of encryption	
S/N	File size (KB)	RSA (s)	ElGamal (s)	RSA (kb)	ElGamal (kb)
1	63	0.9896	2.9947	1890.32	236.29
2	85	1.0023	3.3907	2439.15	295.41
3	120	1.6205	8.7705	3088.11	385.73
4	130	1.7495	9.3232	3129.38	399.20
5	200	1.9853	10.5232	3764.52	470.56
6	300	2.9534	12.2056	5470.91	683.85
7	550	5.6149	16.2851	10597.82	1324.71

Table 4: Image data decryption for RSA and ElGamal algorithms

		Decryption time		Space of decryption	
S/N	File size (KB)	RSA (s)	ElGamal (s)	RSA (kb)	ElGamal (kb)
1	63	11.8935	2.4517	236.29	236.29
2	85	12.6888	3.8033	295.41	295.41
3	120	19.6372	4.3965	386.00	386.00
4	130	19.9276	4.9207	399.20	399.20
5	200	23.6912	6.3696	470.56	470.56
6	300	34.7945	8.0873	683.85	683.85
7	550	67.0517	12.4493	1324.71	1324.71

Table 5: Encryption time and space usage of RSA and ElGamal for audio data

		Encryption time		Memory usage	
S/N	File size (Kb)	RSA	ElGamal	RSA	ElGamal
1	50	0.6186	5.7240	1167.72	145.96
2	55	0.6806	5.9135	1289.66	161.21
3	60	0.7383	6.4193	1384.90	173.10
4	70	0.8740	7.9503	1663.56	207.92
5	90	1.1263	8.1892	2131.86	266.48
6	120	1.3651	12.2567	2606.37	325.79
7	200	1.8295	16.7535	3483.51	435.55

Table 1 displays the time and space used to encrypt the text dataset using RSA and ElGamal cryptographic algorithms.

The execution time of both RSA and ElGamal was taken using the CPU time of the computer. It shows that the RSA algorithm consumes less time during text data encryption than the ElGamal algorithm.

According to Fig. 3, the bigger the text data supplied to the program, the higher the space consumed by the RSA algorithm. This shows that the RSA algorithm consumes more CPU internal memory while encrypting text data than the ElGamal algorithm.

Table 2 shows the decryption time and memory usage of RSA and ElGamal cryptographic algorithms on the test dataset.

According to Fig. 4, the RSA algorithm consumes the CPU time during the decryption of text data while ElGamal consumes less CPU time during the decryption of text data.

In terms of memory usage, both algorithms consume an equal volume of CPU internal memory to decrypt text data.

Table 3 displays the data obtained from encrypting image data using RSA and ElGamal cryptographic algorithms.

Image data was supplied as input and the RSA and ElGamal algorithms were executed on it. Figure 6 shows that the RSA algorithm uses a lesser CPU internal clock while encrypting image data than the ElGamal algorithm, which employs more CPU internal clocks.

Figure 7, the output shows that the ElGamal algorithm outperforms the RSA algorithm in terms of CPU internal memory consumption. ElGamal consumes less memory during image data encryption than the RSA algorithm.

Table 4 shows the data generated from image data decryption using RSA and ElGamal cryptographic algorithms.

The elGamal algorithm also outperforms the RSA algorithm during the decryption of image data. For example, Fig. 8 shows that ElGamal consumes less CPU memory space during the image data decryption compared to the RSA algorithm.

According to Fig. 9, both ElGamal and RSA algorithms consume the same amount of CPU internal memory space during the decryption of image data.

Table 5 shows the data generated from audio data encryption using RSA and ElGamal algorithms obtained from the CPU's internal clock and memory.

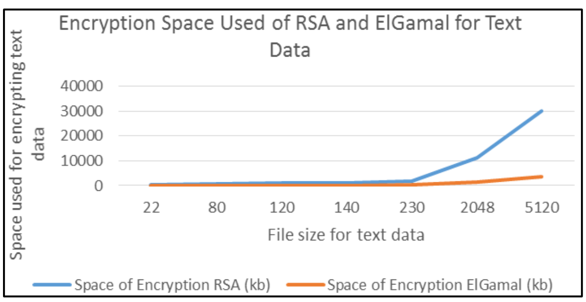

Fig. 3: Analysis of memory used for RSA and ElGamal for text dataset during the encryption process

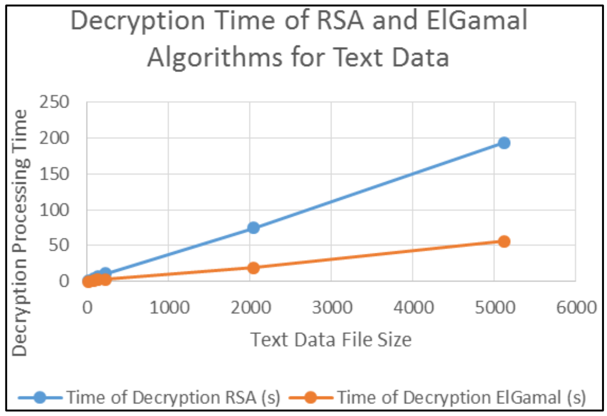

Fig. 4: Decryption time analysis of RSA and ElGamal algorithms for text dataset

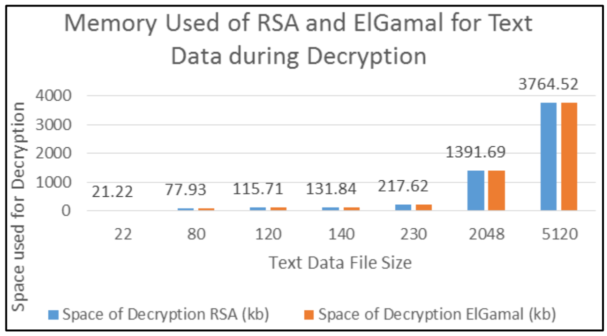

Fig. 5: Memory usage during decryption of text dataset

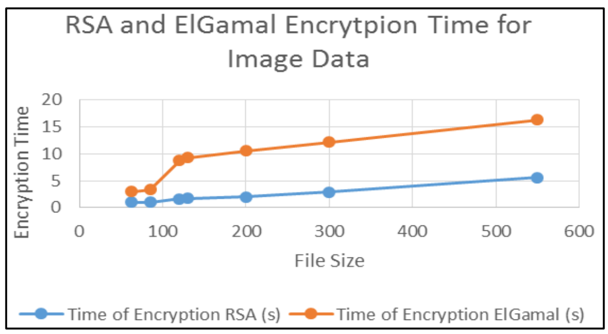

Fig. 6: RSA and ElGamal encryption time analysis for image data

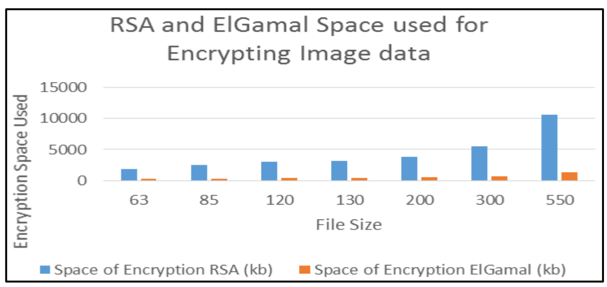

Fig. 7: RSA and ElGamal space are used for encrypting image data

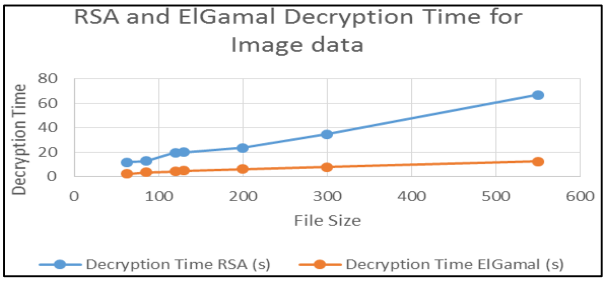

Fig. 8: RSA and ElGamal decryption time for image data

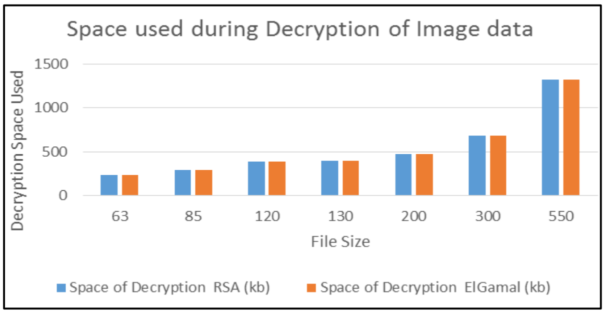

Fig. 9: Space used by RSA and ElGamal during decryption of image data

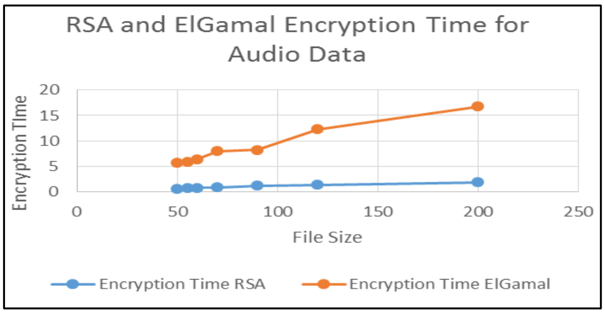

Fig. 10: Encryption time of RSA and ElGamal algorithms for audio data

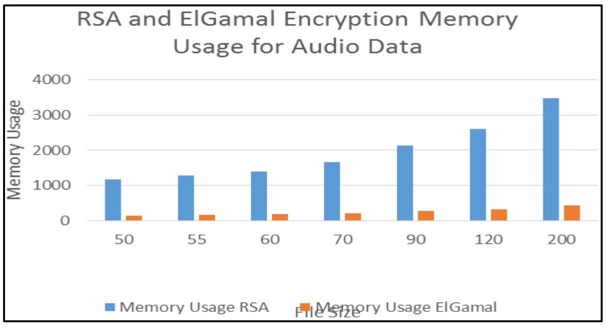

Fig. 11: Memory usage of RSA and ElGamal algorithms during encryption of audio data

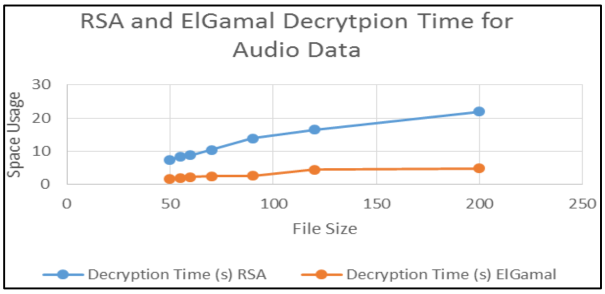

Fig. 12: Decryption time for RSA and ElGamal algorithms for audio data

The result of Fig. 10 shows that audio data was inputted into the program and RSA produced a better result in terms of CPU time. RSA uses a lesser CPU internal clock for audio data encryption than the ElGamal algorithm.

The analysis of Fig. 11 shows that the ElGamal algorithm outperforms the RSA algorithm in terms of CPU memory usage during audio data encryption. In addition, the ElGamal algorithm consumed lesser CPU memory for audio data encryption than the RSA algorithm.

Table 6 shows the decryption time and memory usage obtained during the decryption process of audio data with RSA and ElGamal cryptographic algorithms.

From the analysis of time using audio data, ElGamal uses less CPU time in decrypting audio data than the RSA algorithm, which consumes more CPU time during the decryption of audio data. Also, Fig. 12 shows that the larger the audio size, the higher the CPU time consumption interval between the two algorithms.

The analysis of Fig. 13 shows that there is no significant difference in the amount of CPU space consumed by both algorithms, irrespective of the file size.

Table 7 shows the time and space generated during the encryption of video data with RSA and ElGamal cryptographic algorithms.

The analysis from Fig. 14 shows that video data was inputted into the program. The result indicated that the RSA algorithm consumes less CPU internal time during the video data encryption and the interval between the two algorithms increases as the video data size increases.

The analysis from Fig. 16 shows that RSA consumes more CPU internal memory during video data encryption. At the same time, the ElGamal algorithm outperforms the RSA algorithm in terms of CPU memory consumption.

Table 8 gives the generated data from decrypting video data with RSA and ElGamal Cryptographic algorithms.

Analysis from Fig. 16 shows that ElGamal outperforms the RSA algorithm in terms of CPU memory usage. Also, the differences between the two algorithms increase as the video size increases.

Table 6: Decryption time and memory usage of RSA and ElGamal for audio data

		Decryption time		Decryption memory usage	
S/N	File size (Kb)	RSA	ElGamal	RSA	ElGamal
1	50	7.3565	1.6570	145.96	145.96
2	55	8.2104	1.8803	161.21	161.21
3	60	8.6874	2.1033	173.10	173.10
4	70	10.4017	2.3383	207.92	207.92
5	90	13.7977	2.5158	266.48	266.48
6	120	16.4544	4.4145	325.79	325.79
7	200	21.9815	4.7963	435.55	435.55

Table 7: Encryption time and space usage of RSA and ElGamal for video data

		Video data encryption time (s)		Video data memory usage (Encryption) (kb)	
S/N	File size (Kb)	RSA	ElGamal	RSA	ElGamal
1	452	5.7833	54.8000	10853.30	1356.66
2	700	8.6895	81.5632	16585.40	2073.17
3	900	9.6173	88.5221	17841.30	2230.15
4	1372	17.3919	161.4096	32559.90	4069.97
5	3072	24.0244	222.1748	44514.91	5564.35
6	7608	52.1230	412.3847	56691.24	16691.01
7	10639	80.9202	749.1150	97942.83	18360.01

Table 8: Decryption time and space usage of RSA and ElGamal for video data

		Video data decryption time (s)		Video data memory usage (decryption) (kb)	
S/N	File size (Kb)	RSA	ElGamal	RSA	ElGamal
1	452	69.3627	14.7762	1356.66	1356.66
2	700	105.5035	22.4683	2073.17	2073.17
3	900	114.6094	23.9383	2230.15	2230.15
4	1372	207.9480	45.0798	4069.97	4069.97
5	3072	268.2103	61.0020	5564.35	5564.35
6	7608	394.8201	98.5002	16691.01	16691.01
7	10639	566.3400	133.4137	18360.01	18360.01

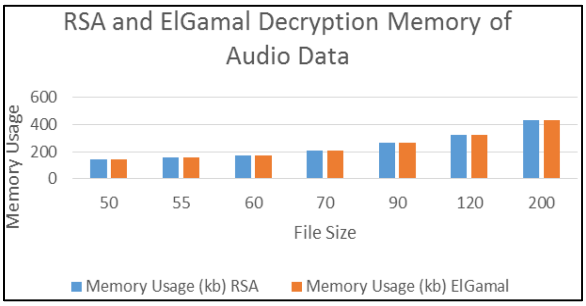

Fig. 13: Decryption memory usage of audio data using RSA and ElGamal algorithms

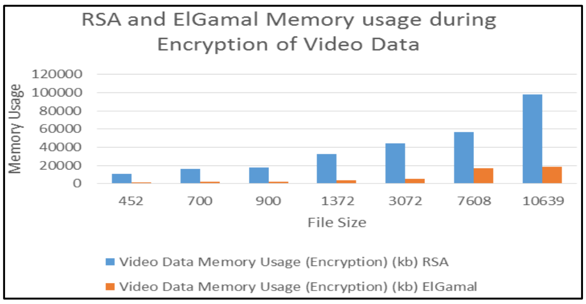

Fig. 15: Memory usage during encryption of video data with RSA and ElGamal cryptographic algorithms

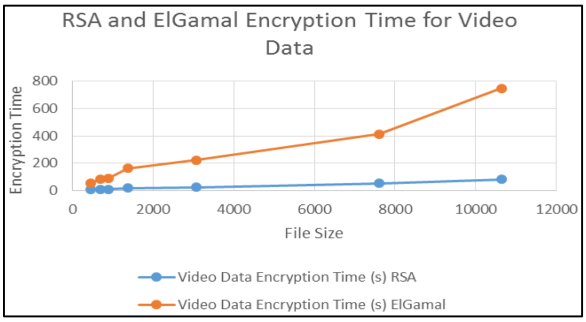

Fig. 14: Encryption time of RSA and ElGamal cryptographic algorithms for video data

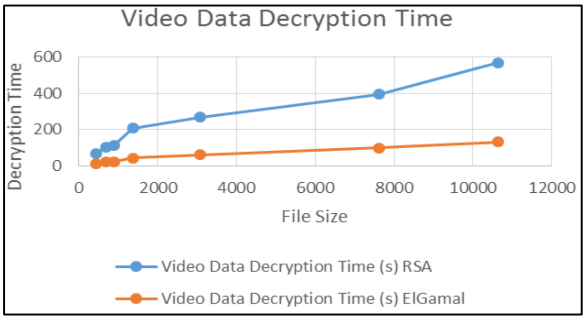

Fig. 16: RSA and ElGamal decryption time obtained from video data

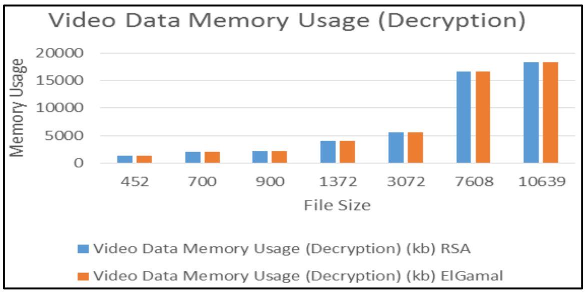

Fig. 17: RSA and ElGamal memory usage from video data decryption process

From Fig. 17, the analysis of the result shows no significant difference between the two algorithms in terms of CPU internal memory usage during the decryption of video data of various file sizes.

Discussion

Internet devices are sophisticated, intelligent infrastructures made up of numerous self-organizing gadgets. In this case, the gadgets are used to analyze the network and send crucial information via the internet. Because of the potential for numerous attacks in this vast network from unidentified devices, data security and privacy are of utmost importance. The main drawback of the IoT network is that because the devices run on batteries, they have a limited capacity for internal storage. To address the issues caused in the network, it is vital to find more resource-optimized and security-related solutions. Also, the complexity of the cryptographic methods requires the devices' resources to be consumed at a faster rate. Along with data integrity, it is also vital to determine the best cryptographic method for an automated IoT network.

Therefore, this study compared two prominent cryptographic methods with their operational behavior. On a laptop running Windows 10 64-bit, an i7 processor running at 2.23 GHz, and 8 GB of RAM, the simulation was run. As the test subjects, random sizes of files 22, 80, 5, 120, 140, 230, 2048, and 5120 were generated. The preferred language for implementation was the c-sharp programming language. The key sizes used were 128 bits, 64 bits, and 128 bits for the Cipher Block Chaining (CBC) mode of the two algorithms. Ten rounds of encryption and decryption were performed on each data block and the time requirements for each run were recorded.

The experimental results obtained from all the datasets used (text, image, audio, and video), as displayed in the tables and figures showed that the RSA algorithm outperformed the ElGamal algorithm during the encryption time of all categories of the dataset as regards the usage of CPU internal clock for text, image, audio, and video file sizes. This is under the existing works of literature (Thu *et al*., 2019; Sari *et al*., 2020; Desai *et al*., 2022; Parenreng and Wahid, 2022). ElGamal algorithm outperformed the RSA algorithm during the decryption time of all categories of data. This is consistent with the existing pieces of literature (Boni *et al*., 2015; Thu *et al*., 2019; Parenreng and Wahid, 2022; Meshram *et al*., 2021; AbdulRaheem *et al*., 2021c). It was observed that the RSA algorithm generated large files and consumed more space (memory) during the encryption process of all categories of text, audio, image, and video data concerning the CPU's internal memory usage. This is consistent with the existing literature (Meshram *et al*., 2022; Abdulraheem *et al*., 2021a; Oladipupo *et al*., 2023). ElGamal algorithm outperformed the RSA algorithm in terms of memory usage. It was also observed that both RSA and ElGamal algorithms consumed similar computational space for decrypting mixed data (Gadde *et al*., 2023; Ullah *et al*., 2023).

Therefore, this study used CPU internal clock and CPU internal memory for time and space performance metrics to evaluate which of the RSA algorithm and the ElGamal algorithm performs better when it comes to mixed data. Based on the various experimental results generated, it was observed that the RSA algorithm is time efficient. In contrast, the ElGamal algorithm is a memory-efficient algorithm for all categories of data. The performance of RSA and ElGamal algorithms was evaluated in the current work. Future work can be performed using other performance evaluations like throughout, accuracy, precision, recall, etc., on encryption and decryption of both algorithms. The comparative analysis of other faster cryptographic can experiment on text, audio, and video as well. In future work, various compression algorithms can be used before encryption to increase the speed of both algorithms further

Conclusion

The RSA and ElGamal cryptographic algorithms were implemented to determine the time and space complexity of both algorithms on mixed (text, image, audio, video) data. The experimental results showed that the RSA algorithm performs better in time complexity for all categories of the dataset (text, image, audio, and video) during the encryption process. Furthermore, the RSA algorithm is better regarding time complexity during the decryption of mixed data. On the other hand, the ElGamal algorithm performs better in terms of memory consumption for encryption and decryption processes for all the dataset categories. Based on the comparative analysis of the time and space complexity of both RSA and ElGamal algorithms, it was discovered that RSA is a better algorithm for time complexity. That is, RSA can be said to be a time-efficient algorithm. On the other hand, the ElGamal algorithm performed better than RSA in the memory usage aspect. Therefore, the ElGamal algorithm is said to be a memory-efficient algorithm. This study provides an addition to the body of knowledge by investigating the performance of selected cryptographic algorithms (RSA and ElGamal) in terms of computer resource usage (time and memory) on mixed data. This seeks to enhance decision-making on which algorithms perform better concerning time and memory usage and the design of a high-impact computer system. Furthermore, the study encourages using additional performance metrics for both algorithms or adding more algorithms to the existing works.

Acknowledgment

The authors would like to express their appreciation to the anonymous referees for their valuable suggestions and comments. The work of Agbotiname Lucky Imoize is supported in part by the Nigerian Petroleum Technology Development Fund (PTDF) and in part by the German academic exchange service (DAAD) through the Nigerian-German postgraduate program under grant 57473408.

Funding Information

There is no funding to support this study.

Author's Contributions

All authors are equally contributed to this study.

Data Availability Statement

The data that support the findings of this study are available upon reasonable request from the corresponding author.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and that no ethical issues are involved.

References

Abdulraheem, M., Awotunde, J. B., Jimoh, R. G., & Oladipo, I. D. (2021a). An efficient lightweight cryptographic algorithm for IoT security. In *Information and Communication Technology and Applications: 3rd International Conference, ICTA 2020, Minna, Nigeria, November 24-27, 2020, Revised Selected Papers 3* (pp. 444-456). Springer International Publishing. https://doi.org/10.1007/978-3-030-69143-1_34

Abdulraheem, M., Awotunde, J. B., Jimoh, R. G., & Oladipo, I. D. (2021b). An efficient lightweight cryptographic algorithm for IoT security. In *Information and Communication Technology and Applications: Third International Conference, ICTA 2020, Minna, Nigeria, November 24-27, 2020, Revised Selected Papers 3* (pp. 444-456). Springer International Publishing. https://doi.org/10.1007/978-3-030-69143-1_34

Abdulraheem, M., Balogun, G. B., Abiodun, M. K., Taofeek-Ibrahim, F. A., Tomori, A. R., Oladipo, I. D., & Awotunde, J. B. (2021c). An enhanced lightweight speck system for cloud-based smart healthcare. In *Applied Informatics: Fourth International Conference, ICAI 2021, Buenos Aires, Argentina, October 28-30, 2021, Proceedings 4* (pp. 363-376). Springer International Publishing. https://doi.org/10.1007/978-3-030-89654-6_26

Abutaha, M., Amar, I., & AlQahtani, S. (2022). The parallel and practical approach of efficient image chaotic encryption based on Message Passing Interface (MPI). *Entropy*, *24*(4), 566. https://doi.org/10.3390/e24040566

Adeniyi, A. E., Misra, S., Daniel, E., & Bokolo Jr, A. (2022). Computational complexity of modified blowfish cryptographic algorithm on video data. *Algorithms*, *15*(10), 373. https://doi.org/10.3390/a15100373

Adeniyi, A. E., Abiodun, K. M., Awotunde, J. B., Olagunju, M., Ojo, O. S., & Edet, N. P. (2023). Implementation of a block cipher algorithm for medical information security on cloud environment: Using modified advanced encryption standard approach. *Multimedia Tools and Applications*, 1-15. https://doi.org/10.1007/s11042-023-14338-9

Arora, R., Parashar, A., & Transforming, C. C. I. (2013). Secure user data in cloud computing using encryption algorithms. *International Journal of Engineering Research and Applications*, *3*(4), 1922-1926.

Avasare, M. G., & Kelkar, V. V. (2015, January). Image encryption using chaos theory. In *2015 International Conference on Communication, Information & Computing Technology (ICCICT)* (pp. 1-6). IEEE. https://ieeexplore.ieee.org/abstract/document/7045687

Awotunde, J. B., Misra, S., & Pham, Q. T. (2022, November). A Secure Framework for Internet of Medical Things Security Based System Using Lightweight Cryptography Enabled Blockchain. In *Future Data and Security Engineering. Big Data, Security and Privacy, Smart City and Industry 4.0 Applications: 9th International Conference, FDSE 2022, Ho Chi Minh City, Vietnam, November 23-25, 2022, Proceedings* (pp. 258-272). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-19-8069-5_17

Banu, S, A., & Amirtharajan, R. (2020). A robust medical image encryption in dual domain: Chaos-DNA-IWT combined approach. *Medical & Biological Engineering & Computing*, *58*, 1445-1458. https://doi.org/10.1007/s11517-020-02178-w

Bhanot, R., & Hans, R. (2015). A review and comparative analysis of various encryption algorithms. *International Journal of Security and Its Applications*, *9*(4), 289-306. https://www.earticle.net/Article/A245530

Boni, S., Bhatt, J., & Bhat, S. (2015). Improving the Diffie-Hellman key exchange algorithm by proposing the multiplicative key exchange algorithm. *International Journal of Computer Applications*, *130*(15).

Brahim, A. H., Pacha, A. A., & Said, N. H. (2020). Image encryption based on compressive sensing and chaos systems. *Optics & Laser Technology*, *132*, 106489. https://doi.org/10.1016/j.optlastec.2020.106489

Desai, A., Parekh, V., Unadkat, U., & Shekokar, N. (2022). Performance Analysis of Various Asymmetric Public-Key Cryptosystem. In *Pervasive Computing and Social Networking: Proceedings of ICPCSN 2022* (pp. 437-449). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-19-2840-6_34

Gadde, S., Amutharaj, J., & Usha, S. (2023). A security model to protect the isolation of medical data in the cloud using hybrid cryptography. *Journal of Information Security and Applications*, *73*, 103412. https://doi.org/10.1016/j.jisa.2022.103412

Hamza, R., & Titouna, F. (2016). A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map. *Information Security Journal: A Global Perspective*, *25*(4-6), 162-179. https://doi.org/10.1080/19393555.2016.1212954

Hu, G., Xiao, D., Wang, Y., & Li, X. (2017). Cryptanalysis of a chaotic image cipher using Latin square-based confusion and diffusion. *Nonlinear Dynamics*, *88*, 1305-1316. https://doi.org/10.1007/s11071-016-3311-2

Huang, X., Dong, Y., Ye, G., & Shi, Y. (2023). Meaningful image encryption algorithm based on compressive sensing and integer wavelet transform. *Frontiers of Computer Science*, *17*(3), 173804. https://doi.org/10.1007/s11704-022-1419-8

Ibrahim, S., & Alharbi, A. (2020). Efficient image encryption scheme using Henon map, dynamic S-boxes and elliptic curve cryptography. *IEEE Access*, *8*, 194289-194302. https://ieeexplore.ieee.org/abstract/document/9233311

Jan, A., Parah, S. A., & Malik, B. A. (2022). IEFHAC: Image encryption framework based on hessenberg transform and chaotic theory for smart health. *Multimedia Tools and Applications*, *81*(13), 18829-18853. https://doi.org/10.1007/s11042-022-12653-1

Kaur, G., Agarwal, R., & Patidar, V. (2020). Chaos based multiple order optical transform for 2D image encryption. *Engineering Science and Technology, an International Journal*, *23*(5), 998-1014. https://doi.org/10.1016/j.jestch.2020.02.007

Kayalvizhi, R., Vijayalakshmi, M., & Vaidehi, V. (2010). Energy analysis of RSA and ElGamal algorithms for wireless sensor networks. In *Recent Trends in Network Security and Applications: 3rd International Conference, CNSA 2010, Chennai, India, July 23-25, 2010. Proceedings 3* (pp. 172-180). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-14478-3_18

Khalil, N., Sarhan, A., & Alshewimy, M. A. (2021). An efficient color/grayscale image encryption scheme based on hybrid chaotic maps. *Optics & Laser Technology*, *143*, 107326. https://doi.org/10.1016/j.optlastec.2021.107326

Khedmati, Y., Parvaz, R., & Behroo, Y. (2020). 2D Hybrid chaos map for image security transform based on framelet and cellular automata. *Information Sciences*, *512*, 855-879. https://doi.org/10.1016/j.ins.2019.10.028

Li, C. T., Weng, C. Y., Chen, C. L., Lee, C. C., Deng, Y. Y., & Imoize, A. L. (2022). An Efficient Authenticated Key Agreement Scheme Supporting Privacy-Preservation for Internet of Drones Communications. *Sensors*, *22*(23), 9534. https://doi.org/10.3390/s22239534

Liao, X., Hahsmi, M. A., & Haider, R. (2018). An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos. *Optik-International Journal for Light and Electron Optics*, *153*, 117-134. https://doi.org/10.1016/j.ijleo.2017.09.099

Maddodi, G., Awad, A., Awad, D., Awad, M., & Lee, B. (2018). A new image encryption algorithm based on heterogeneous chaotic neural network generator and dna encoding. *Multimedia tools and applications*, *77*, 24701-24725. https://doi.org/10.1007/s11042-018-5669-2

Meng, F., Lin, R., Wang, Z., Zou, H., & Zhou, S. (2018). A multi-connection encryption algorithm applied in secure channel service system. *EAI Endorsed Transactions on Security and Safety*, *5*(15). http://doi.org/10.4108/eai.15-5-2018.155167

Meshram, C., Imoize, A. L., Aljaedi, A., Alharbi, A. R., Jamal, S. S., & Barve, S. K. (2021). An efficient electronic cash system based on certificateless group signcryption scheme using conformable chaotic maps. *Sensors*, *21*(21), 7039. https://doi.org/10.3390/s21217039

Meshram, C., Imoize, A. L., Jamal, S. S., Alharbi, A. R., Meshram, S. G., & Hussain, I. (2022). CGST: Provably Secure Lightweight Certificateless Group Signcryption Technique Based on Fractional Chaotic Maps. *IEEE Access*, *10*, 39853-39863. https://ieeexplore.ieee.org/abstract/document/9751080

Musanna, F., & Kumar, S. (2020). Image encryption using quantum 3-D Baker map and generalized gray code coupled with fractional Chen's chaotic system. *Quantum Information Processing*, *19*, 1-31. https://doi.org/10.1007/s11128-020-02724-3

Niu, Y., Zhou, Z., & Zhang, X. (2020). An image encryption approach based on chaotic maps and genetic operations. *Multimedia Tools and Applications*, *79*, 25613-25633. https://doi.org/10.1007/s11042-020-09237-2

Nkandeu, Y. P. K., & Tiedeu, A. (2019). An image encryption algorithm based on substitution technique and chaos mixing. *Multimedia Tools and Applications*, *78*(8), 10013-10034. https://doi.org/10.1007/s11042-018-6612-2

Oğraş, H., & Türk, M. (2016). A Robust chaos-based image cryptosystem with an improved key generator and plain image sensitivity mechanism. *Journal of Information Security*, *8*(1), 23-41. https://doi.org/10.4236/jis.2017.81003

Okeyinka, A. E. (2015, October). Computational speeds analysis of RSA and ElGamal algorithms on text data. In *Proceedings of the world congress on engineering and computer science* (Vol. *1*, pp. 21-23). https://www.iaeng.org/publication/WCECS2015/WCECS2015_pp115-118.pdf

Oladipupo, E. T., Abikoye, O. C., Imoize, A. L., Awotunde, J. B., Chang, T. Y., Lee, C. C., & Do, D. T. (2023). An Efficient Authenticated Elliptic Curve Cryptography Scheme for Multicore Wireless Sensor Networks. *IEEE Access*, *11*, 1306-1323. https://ieeexplore.ieee.org/abstract/document/10004924

Panda, M., & Nag, A. (2015, May). Plain text encryption using AES, DES and SALSA20 by java based bouncy castle API on Windows and Linux. In *2015 Second International Conference on Advances in Computing and Communication Engineering* (pp. 541-548). IEEE. https://ieeexplore.ieee.org/abstract/document/7306744

Parenreng, J. M., & Wahid, A. (2022). The E-mail Security System Using ElGamal Hybrid Algorithm and AES (Advanced Encryption Standard) Algorithm. *Internet of Things and Artificial Intelligence Journal*, *2*(1), 1-9. https://pubs.ascee.org/index.php/iota/article/view/510

Pourjabbar Kari, A., Habibizad Navin, A., Bidgoli, A. M., & Mirnia, M. (2021). A new image encryption scheme based on hybrid chaotic maps. *Multimedia Tools and Applications*, *80*, 2753-2772. https://doi.org/10.1007/s11042-020-09648-1

Rajabi, A., Bobba, R. B., Rosulek, M., Wright, C., & Feng, W. C. (2021). On the (im) practicality of adversarial perturbation for image privacy. *Proceedings on Privacy Enhancing Technologies*. https://doi.org/10.2478/popets-2021-0006

Sari, P. P., Nababan, E. B., & Zarlis, M. (2020, June). Comparative study of luc, ElGamal and rsa algorithms in encoding texts. In *2020 3rd International Conference on Mechanical, Electronics, Computer and Industrial Technology (MECnIT)* (pp. 148-151). IEEE. https://ieeexplore.ieee.org/abstract/document/9166586

Singh, S., Rathore, S., Alfarraj, O., Tolba, A., & Yoon, B. (2022). A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Generation Computer Systems*, *129*, 380-388. https://doi.org/10.1016/j.future.2021.11.028

Talhaoui, M. Z., & Wang, X. (2021). A new fractional one-dimensional chaotic map and its application in high-speed image encryption. *Information Sciences*, *550*, 13-26. https://doi.org/10.1016/j.ins.2020.10.048

Thu, K. M., Hlaing, K. S., & Aung, N. A. (2019). Time Performance Analysis of RSA and ElGamal Public-Key Cryptosystems. *Int. J. of Trend in Scientific Research and Development*.

Ullah, S., Zheng, J., Din, N., Hussain, M. T., Ullah, F., & Yousaf, M. (2023). Elliptic Curve Cryptography; Applications, challenges, recent advances and future trends: A comprehensive survey. *Computer Science Review*, *47*, 100530. https://doi.org/10.1016/j.cosrev.2022.100530

Ye, G., Pan, C., Dong, Y., Jiao, K., & Huang, X. (2021). A novel multi-image visually meaningful encryption algorithm based on compressive sensing and Schur decomposition. *Transactions on Emerging Telecommunications Technologies*, *32*(2), e4071. https://doi.org/10.1002/ett.4071

Ye, G., Wu, H., Liu, M., & Shi, Y. (2022). Image encryption scheme based on blind signature and an improved Lorenz system. *Expert Systems with Applications*, *205*, 117709. https://doi.org/10.1016/j.eswa.2022.117709

Yu, Y., Au, M. H., Ateniese, G., Huang, X., Susilo, W., Dai, Y., & Min, G. (2016). Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. *IEEE Transactions on Information Forensics and Security*, *12*(4), 767-778. https://ieeexplore.ieee.org/abstract/document/7586112

Zhang, Q., Guo, L., & Wei, X. (2013). A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. *Optik-International Journal for Light and Electron Optics*, *124*(18), 3596-3600. https://doi.org/10.1016/j.ijleo.2012.11.018