UTM UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

Comparative Study on Encryption Algorithms for Autism MRI Scan Images

Pavunraj Sivakumar[1*] & Yusliza Yusoff[2]
Faculty of Computing
Universiti Teknologi Malaysia,
81310 UTM Johor Bahru,
Johor, Malaysia
Email: mr.pavun01@gmail.com[1]; yusliza@utm.my[2]

Submitted: 2/7/2024. Revised edition: 3/10/2024. Accepted: 6/10/2024. Published online: 25/11/2024
DOI: https://doi.org/10.11113/ijic.v14n2.471

***Abstract*—Healthcare centre is the most susceptible sctor. Cyber-attack on medical institutions, such as hospitals and health care centre have increased year after year. Autism health care centre is one of the victims. Autism MRI scan images include sensitive and confidential information about a patient's health and other personal information. Therefore, image encryption is a fundamental aspect of information security, especially in today's digital era where the proliferation of images and the need to protect sensitive visual content are of paramount importance. In order to protect the confidentiality and integrity of images, image encryption techniques work to make sure that only authorised users can view and understand the visual data while prohibiting unauthorised access and modification. The pixel values and spatial properties of the image are hidden using a variety of cryptographic methods and key-based actions. Symmetric encryption algorithm, like Advanced Encryption Standard (AES), which use the same key for encryption and decryption operations, are among the famous image encryption techniques. After that, asymmetric encryption algorithm like Rivest-Shamir-Adleman (RSA), which employ two distinct keys for both encryption and decryption. Next, the research includes a hybridization method of Elliptic Curve Cryptography (ECC) with the Hill Cypher (HC) for image encryption and decryption. There are five different Autism MRI Scan images selected to be used as the input image for encryption process. Then, each image will have two different file format which is PNG and BMP and two different file size which is 256*256px and 512*512px. This research's goal is to compare how well symmetric encryption, asymmetric encryption and hybrid encryption work as three separate image encryption techniques. This can help users rapidly and efficiently speed up the encryption and decryption of images and enhance the security of MRI scan images. By applying differential analysis parameters like Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI) and statistical analysis parameters like Histogram Analysis (HA), the characteristics of the image encryption approach are examined. At the end of the experiment, AES encryption proves to be the best among the three types of encryption with better performance in terms of security with NPCR percentage of 99.72%, UACI percentage of 32.68% and has a higher speed of encryption which only takes 0.0238s but has the second-best distribution in HA of pixel value to frequency compares to ECC with HC.**

***Keywords*—AES, RSA, ECC with HC, NPCR, UACI, HA**

I. Introduction

In the modern world, data has grown more essential among human beings since it may be a dangerous asset if misused for illegal uses. Data may be presented in a variety of forms, including text, video, and images. In today's technological environment, data evolution has been quick and unmatched. Moreover, cybercrime also has evolved into a big menace in today's globe. Cyber-attack on medical institutions, such as hospitals and health care center have increased year after year [1]. Autism health care center is one of the victims, among many others.

Cybercriminals usually target the network of autism healthcare system in order to obtain the system's data like MRI scan images. It is because, MRI scan images include sensitive and confidential information about a patient's health and other personal information like name, contact information and insurance information [2]. Not only that, the attacker also leaked the data obtained and made available for unauthorized access. For example, an incident of cyberattacks on medical imaging services provider which is Longhorn Imaging. The hackers got into the company's servers, gaining access to a massive database containing over 280,000 patient records [3]. Moreover, cyber attackers also modify data stored in the system. It can lead to wrong diagnoses or inappropriate treatment choices for patient. This worsens the patient's condition and leads to additional health complications. For example, a three-year-old kid was given five times the recommended dosage of painkillers after an attacker prevented medical workers from using their electronic devices [4].

This study aims to identify the most suitable and secure image encryption technique between AES, RSA and ECC with HC algorithm in term of speed of encryption and security which can prevent cyber attackers from stealing the autism MRI scan images. The study focuses on the security and timing of encryption. The image encryption security's qualities are assessed using differential analysis parameters such as NPCR, UACI, and statistical analysis parameters such as HA.

A study is being carried out to figure out which of the three types of image encryption technology is preferable for the autism care center to use to preserve the patient's MRI scan images. The outcome of this study might help in keeping the patient's data safe and secure. Keeping MRI scan pictures secure from cyber attackers helps to maintain the integrity and quality of medical data, ensuring that patients receive appropriate and safe medical care. The benefits of this study include the ability to determine which of the three encryption approaches is more successful. This study can assist not just the autism care center sector, but also other firms who need to preserve their data especially in image format.

II. Literature Review

A. Cryptography

Encryption is the technical phrase for converting the original text into a string of unintelligible characters. The secret communication would be encrypted and decrypted only by the sender and recipient. According to several experts, writing and cryptography were both created about the same period. Moreover, data can appear in a variety of ways in modern technology, including text, images, files, videos, and music. Despite the fact that there are several varieties of encryption algorithms, all of them use the same structure of plaintext, ciphertext, and algorithm [5]. Image encryption is the practice of converting a digital image into an unreadable and secret form known as a cipher image in order to safeguard its secrecy and privacy. Image encryption can be done using three different technique like symmetric, asymmetric and hybrid method encryption.

Symmetric encryption is a time-tested and widely used technique. Due to the fact that it only requires one secret key to encode and decode data, this sort of encryption is the simplest. Both the sender and the receiver must be aware of the secret key that is used to encrypt and decrypt all of the communications. The technique of symmetric encryption is two-way [6].

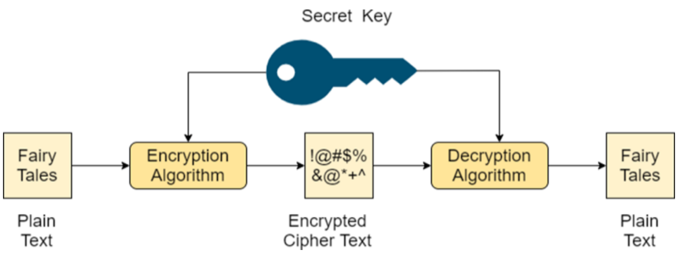


Fig. 1. Symmetric-key encryption [6]

Asymmetric encryption encrypts plain text using two keys. Asymmetric encryption employs two related keys to increase security because the message may be decoded by anybody who has access to the secret key. Anyone wishing to message you has free access to your public key. The second private key is kept a secret so that only you have access to it.

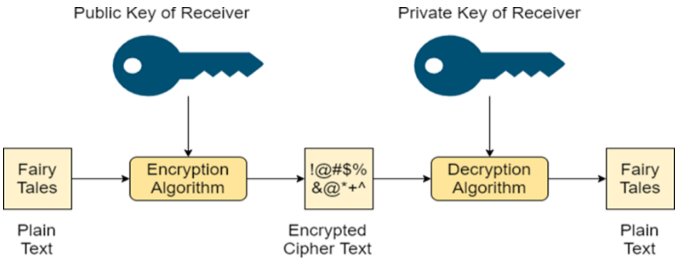


Fig. 2. Asymmetric-key encryption [6]

B. Comparison between symmetric algorithm

TABLE 1. Performance analysis and comparison of DES, AES and Blowfish symmetric key cryptography algorithms [7]

Factor	DES	AES	Blowfish
Encryption speed	Slow due to its 56-bit key size	High speed and efficiency in both software and hardware.	Faster than DES but it is slower than AES
Key Size	Has fixed key size of 56 bits	Supports key sizes of 128, 192, and 256 bits, providing a high level of security.	Supports a key size from 32 bits to 448 bits, offering flexibility.
Security	Insecure due to its small key size.	Highly secure	Less secure than AES.
Hardware and software	Easy to implement in both hardware and software	Excels in both hardware and software implementations.	Simple and fast to implement in software, but the hardware implementation is not as efficient

C. Comparison between asymmetric algorithm

TABLE 2. Performance analysis and comparison of RSA, Diffie-Hellman and ELGAMAL asymmetric key cryptography algorithms [8]

Factor	**RSA**	**Diffie-Hellman**	**El Gamal**
Security	Widely trusted for its security	Focuses on secure key exchange rather than encryption.	Uses a larger key size than RSA for equivalent security.
Encryption speed	Generally slower than symmetric algorithms but faster than El Gamal.	Not typically used for encryption/ decryption.	Slower compared to RSA because it requires more complex calculations
Key Size	2048 bits or larger for secure encryption. Smaller key sizes can provide equivalent security.	Need to be larger than RSA keys.	Larger than RSA keys to achieve the same security level
Compatibility	Widely adopted and supported across various platforms, software, and hardware.	Less suitable for image encryption without additional symmetric encryption mechanisms.	Produces larger ciphertexts than RSA, which can be problematic for large images.

D. Comparison between asymmetric algorithm

TABLE 3. Performance analysis and comparison of ECC with Hill Cipher, ECC with AES and El Gamal with Double Playfair Cipher [9]

Factor	ECC with HC	ECC with AES	El Gamal with Double Playfair Cipher
Security	Strong encryption algorithm. The addition of the Hill Cipher further enhances the encryption process.	ECC combined with AES also offers solid security. But, ECC doesn't provide an additional layer of security.	El Gamal encryption is secure, but the Double Playfair Cipher may not offer the same level of security.
Complexity	Requires handling both elliptic curve arithmetic and matrix operations. While it may seem complex, it's manageable with proper implementation.	While ECC with AES may involve slightly more complexity in key management due to the combination of asymmetric and symmetric cryptography.	Require dealing with both asymmetric and symmetric cryptographic techniques, making it more complex to implement and manage.
Efficiency	High security with relatively small key sizes, making it efficient for encryption.	AES is highly efficient and fast in both software and hardware implementations.	El Gamal encryption can be expensive, especially for large images

III. Methodology

Fig. 3 showed the planned study project's research framework. There were 3 phases in total. In phase 1, I examined current literature and research articles to better understand various image encryption algorithms and their practical implementations. Then, I evaluated and determined the best efficient image encryption technique based on current technology breakthroughs. Next, the chosen three techniques were reviewed. In phase 2, I collected the data and sources required for the experiment, such as image datasets and algorithm implementations. Then, I planned and arranged an experiment to test and compare the chosen image encryption techniques. After that, I carried out the experiment by applying the selected encryption methods to the acquired data and documented the results. In phase 3, I assessed each algorithm's performance in terms of security and speed based on obtained result. Finally, I examined the experiment results, generating judgments regarding the efficiency of the tested algorithms. This research framework outlined the processes and procedures that were taken in this investigation.

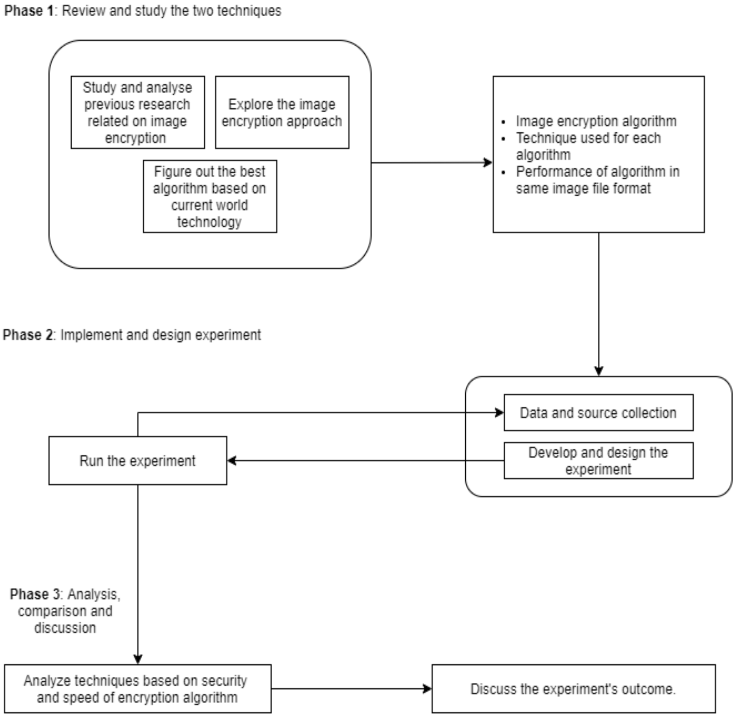

Phase 1: Review and study the two techniques
Study and analyse previous research related on image encryption
Explore the image encryption approach
Figure out the best algorithm based on current world technology
Image encryption algorithm
Technique used for each algorithm
Performance of algorithm in same image file format
Phase 2: Implement and design experiment
Data and source collection
Develop and design the experiment
Run the experiment
Phase 3: Analysis, comparison and discussion
Analyze techniques based on security and speed of encryption algorithm
Discuss the experiment's outcome.

Fig. 3. Research Framework

A. Data collection

Fig. 4 and 5 depicts input pictures for the experiment. Five brain MRI scan images were used. Then, each image will have two different file format which is PNG and BMP and two different file size which is 256*256px and 512*512px.

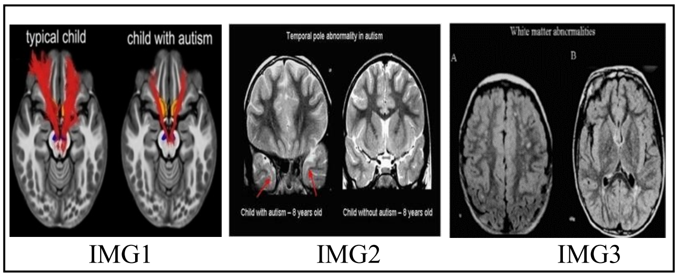

typical child
child with autism
Temporal pole abnormality in autism
Child with autism – 8 years old
Child without autism – 8 years old
White matter abnormalities
A
B
IMG1
IMG2
IMG3

Fig. 4 Input Images

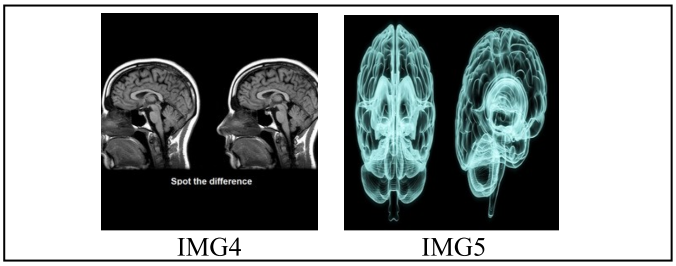


Fig. 5. Input Images

B. *Performance measure*

Three features were evaluated in the testing procedure to assess the efficiency of image encryption techniques, such as differential analysis, statistical analysis, and encryption speed. Differential analysis measured the technique's susceptibility to differential attacks using the Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI). The reason NPCR was chosen as one of the performance measures was that it helped avoid differential attacks and also measured the sensitivity of an encryption algorithm by quantifying the number of pixel differences between the original and encrypted MRI scan images. Higher NPCR values indicated greater pixel diffusion, which enhanced the security of the encrypted MRI scans. Key sensitivity for NPCR was > 99%. Equation below shows the formula to calculate NPCR [9].

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\%$$

The reason UACI was chosen as one of the performance measures was that it helped avoid differential attacks and also measured the change in intensity between pixels adjacent in a picture. Key sensitivity for UACI was around 33%. Equation below shows the formula to calculate UACI [9].

$$UACI = \frac{1}{M \times N}\left[\sum\nolimits_{i,j} \frac{C_{1(i,j)} - C_{2(i,j)}}{255}\right] \times 100\%$$

Afterward, the effectiveness of countermeasures against statistical attacks was assessed using Histogram analysis (HA). HA was chosen as one of the performance measures because it was helpful in the prevention of statistical attacks as well as the evaluation of the visual quality and statistical features of encrypted MRI data. We could guarantee that the encryption method kept the intensity distribution and statistical properties of the original images by examining the histogram of the encrypted MRI images [9].

The time taken to complete the encryption process was an important practical performance measure for real-world applications. It was because, in case we got to know about the attacker plan earlier, then we could implement the encryption process as soon as possible. Therefore, encryption time was really crucial to avoid the attacker from executing their plan. By considering the time taken for encryption, we could evaluate the computational time analysis of the encryption algorithm for encrypting MRI scans [9].

IV. Comparative Analysis

This chapter described the results of implementing image encryption with AES, RSA, and ECC with HC algorithms using the experiment design from the previous chapter. NPCR, UACI, HA, and time of encryption were the measures used to assess how effectively three alternative encryption techniques may help the autism care center handle and manipulate image data. The methods were implemented using MATLAB software for AES and RSA, and Visual Studio Code for ECC with HC. NPCR and UACI were developed in Visual Studio Code and HISTOGRAM was developed in MATLAB with the algorithm to assess performance. Graphs and Tables were used to analyze and discuss the experiment results.

A. *Result based on NPCR*

Table 1 shows the experiment results for NPCR performance measure for the chosen five images in 256x256px. while Table 2 displays the NPCR performance measure for 512x512px image size. NPCR values must be greater than 99% for better image encryption. According to the result for 256x256px and 512x512px image, the AES algorithm produces relatively higher NPCR value compared to RSA and ECC with HC. This indicates that the AES algorithm with both PNG and BMP file format is the best because it enhanced the security of the encrypted MRI scans and more resistant to differential attacks compared with the RSA and ECC with HC algorithm for all images.

TABLE 1. NPCR Readings for 256x256px

NPCR (%)				
Image	Image Format	AES	RSA	ECC with HC
1	PNG	99.60	56.03	70.01
2		99.68	86.79	67.84
3		99.53	90.42	75.60
4		99.71	37.50	48.00
5		99.65	51.04	63.10
1	BMP	99.63	58.95	75.71
2		99.67	86.15	73.60
3		99.56	88.78	74.38
4		99.63	53.12	68.13
5		99.66	55.08	68.98

TABLE 2. NPCR Readings for 512x512px

NPCR (%)				
Image	Image Format	AES	RSA	ECC with HC
1	PNG	99.65	60.33	74.87
2		99.63	87.22	77.05
3		99.55	88.90	75.51
4		99.70	54.99	69.05
5		99.71	56.16	66.60
1	BMP	99.65	56.65	69.18
2		99.65	80.07	72.64
3		99.55	83.76	72.28
4		99.71	51.19	63.17
5		99.72	49.63	59.45

Fig. 5 shows the comparison of NPCR values for Image 5 of PNG and BMP file formats as well as 256 x 256px and 512 x 512px image sizes respectively in AES, RSA and ECC with HC algorithms. Based on the Fig. 5, AES algorithm gave the highest NPCR values which is 99.72%. This shows that the AES method with both PNG and BMP file formats is stronger because it improves the security of encrypted MRI scans and is more resistant to differential attacks than the RSA and ECC with HC algorithms for all pictures.

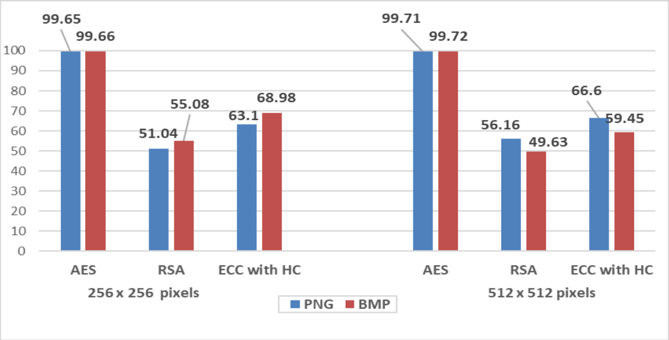


Fig. 5. NPCR Comparison

B. Result based on UACI

Table 3 shows the experiment results for UACI performance measure for chosen five images in 256x256px, while Table 4 depicted the UACI performance measure for 512x512px image size. All results were calculated in percentage (%). UACI values must be around 33% for better image encryption. According to the result for 256x256px and 512x512px image, AES also gave UACI value close to 33%. This shows that, when compared to the RSA and ECC with HC algorithm for all pictures, the AES algorithm with both the PNG and BMP file format is the best since it improved the security of the encrypted MRI scans and is more resistant to differential attacks.

TABLE 3. UACI Readings for 256x256px

UACI (%)				
Image	Image Format	AES	RSA	ECC with HC
1	PNG	40.44	22.84	22.77
2		35.01	56.67	23.95
3		32.68	56.91	20.63
4		49.14	17.99	17.07
5		44.47	23.59	22.67
1	BMP	40.20	25.15	25.98
2		34.85	55.32	27.43
3		32.46	55.44	25.56
4		43.46	25.64	24.39
5		43.26	26.56	25.70

TABLE 4. UACI Readings for 512x512px

UACI (%)				
Image	Image Format	AES	RSA	ECC with HC
1	PNG	41.02	26.34	25.56
2		35.44	55.85	28.79
3		32.53	55.79	26.29
4		44.05	27.20	25.08
5		44.40	28.14	24.44
1	BMP	42.33	23.01	22.58
2		48.62	42.12	26.36
3		46.53	42.78	25.00
4		45.93	22.89	22.13
5		47.37	22.27	20.69

Fig. 6 shows the comparison of UACI values for Image 3 of PNG and BMP file formats as well as 256 x 256px and 512 x 512px image sizes respectively in AES, RSA and ECC with HC algorithms. Based on the Fig. 6, AES algorithm gave the best UACI values which is 32.68%. This result is close to 33%. This indicates that the AES algorithm with BMP file format and 256 x 256px size is the best because it enhanced the security of the encrypted MRI scans and more resistant to differential attacks compared with the RSA and ECC with HC algorithm because BMP files are uncompressed and lossless.

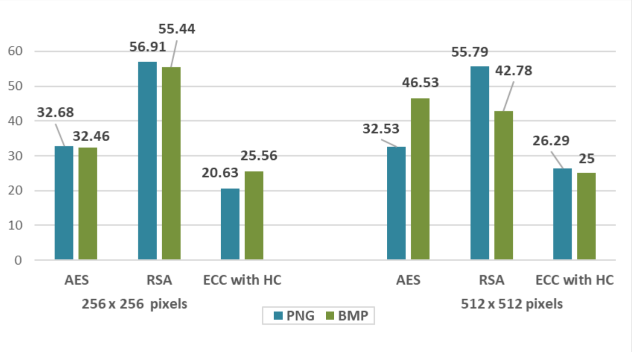


Fig. 6. UACI Comparison

C. *Result based on time of encryption*

Table 5 showed the experiment results for the time of encryption for chosen five images in 256x256px, while Table 6 showed the time of encryption for the 512x512px image size.

TABLE 5. Time of encryption for 256x256px

Time (s)				
Image	Image Format	AES	RSA	ECC with HC
1	PNG	0.0339	3.9617	5.3162
2		0.0318	3.2186	5.1451
3		0.0138	3.1211	5.0768
4		0.0399	3.1494	5.2172
5		0.0344	2.9949	5.0859
1	BMP	0.0370	3.4269	5.1925
2		0.0338	3.6243	5.2401
3		0.0142	3.4139	5.0592
4		0.0356	3.4055	5.0135
5		0.0462	2.9060	5.0623

TABLE 6. Time of encryption for 512x512px

Time (s)				
Image	Image Format	AES	RSA	ECC with HC
1		0.1101	4.1505	6.0774
2	PNG	0.1177	3.4072	5.8339
3		0.1131	3.7180	5.9601
4		0.1040	3.3834	5.8894
5		0.1138	3.2819	6.0467
1	BMP	0.1143	3.5441	5.8519
2		0.1187	3.4436	5.9491
3		0.1117	3.6433	5.8291
4		0.1118	3.8115	5.7611
5		0.1196	3.1065	5.6828

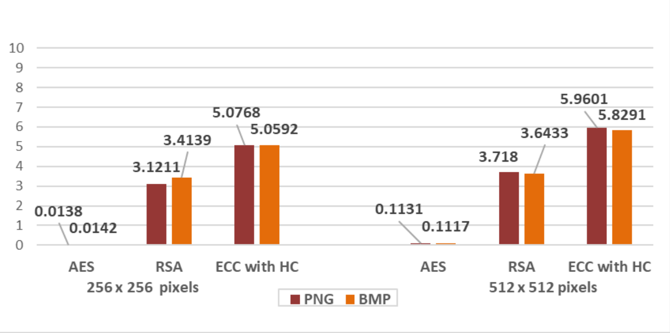


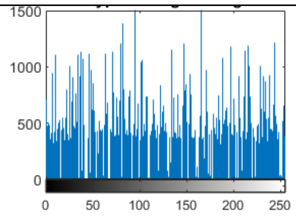
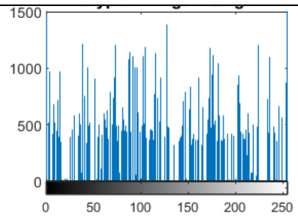
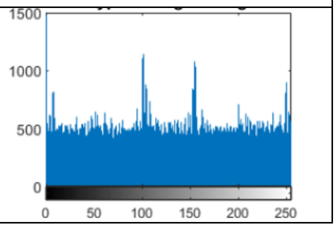
Fig.7. Time of encryption Comparison

Fig. 7 shows the comparison of time of encryption values for Image 3 of PNG and BMP file formats as well as 256 x 256px and 512 x 512px image sizes respectively in AES, RSA and ECC with HC algorithms. Based on the Fig. 7, AES algorithm take the least time of encryption which is 0.0138s. This indicates that the AES algorithm with PNG file format and 256 x 256px size is the best because it only needs least time to encrypt the image for the Image 3. The time of encryption increases, if the image size increases as well.

D. *Result based Histogram Analysis*

Based on the Table 7,8,9, and 10, ECC with HC produce more uniform distribution of pixel values for all five encrypted images compared to AES and RSA algorithms. However, AES has the second-best distribution in HA of pixel value to frequency compares to RSA.

TABLE 7. Histogram Analysis for images in PNG format and 256x256px

Histogram Analysis for Encrypted Image			
IMG	AES	RSA	ECC with HC
1			

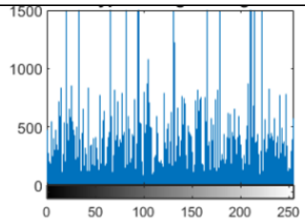
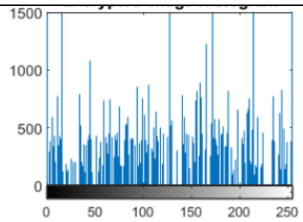
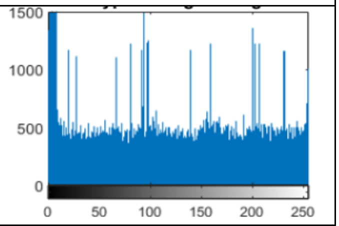
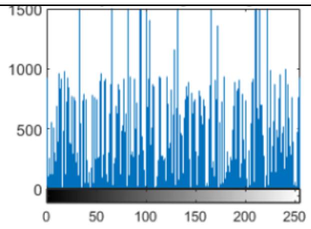
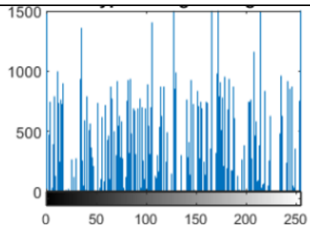
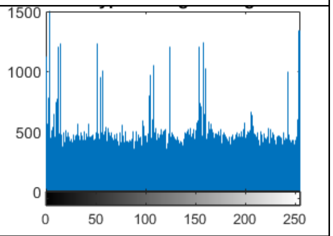
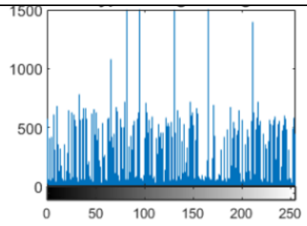
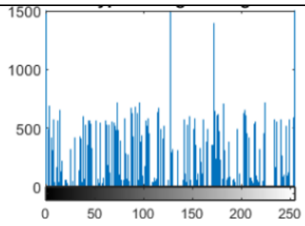
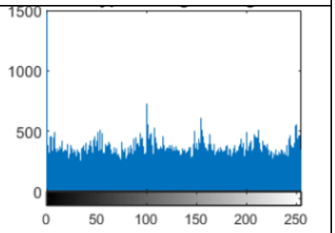
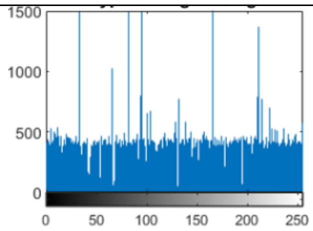
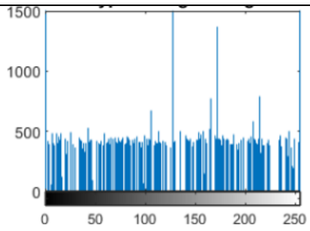
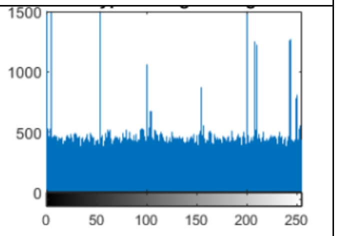
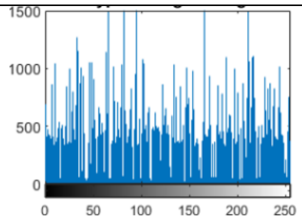
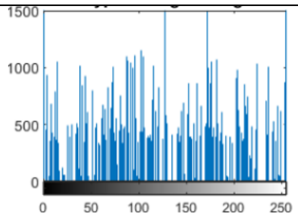
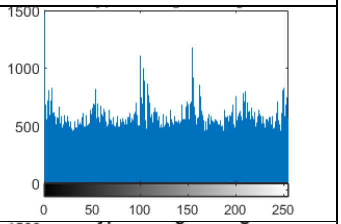
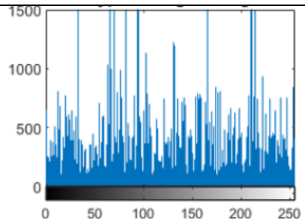
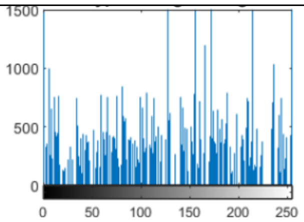
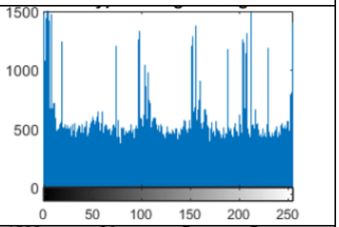
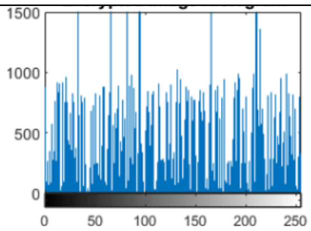
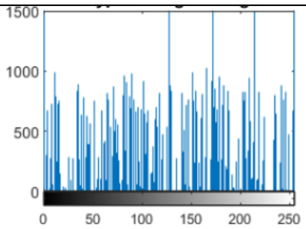
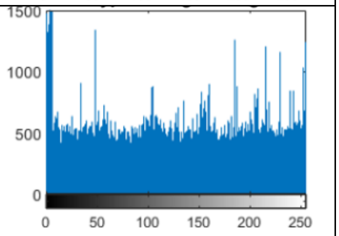
Histogram Analysis for Encrypted Image			
IMG	AES	RSA	ECC with HC
2			
3			
4			
5			

TABLE 8. Histogram Analysis for images in BMP format and 256x256px

Histogram Analysis for Encrypted Image			
IMG	AES	RSA	ECC with HC
1			
2			
3			

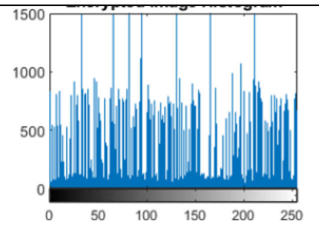
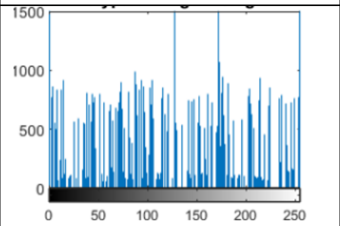
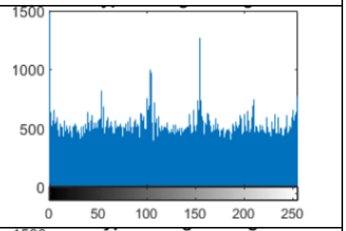
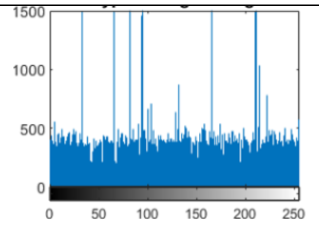
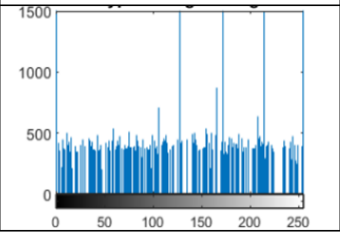
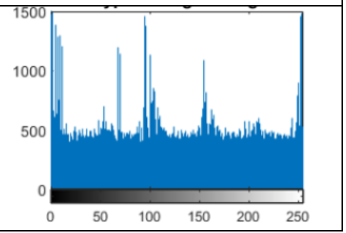
Histogram Analysis for Encrypted Image			
IMG	AES	RSA	ECC with HC
4			
5			

TABLE 9. Histogram Analysis for images in PNG format and 256x256px

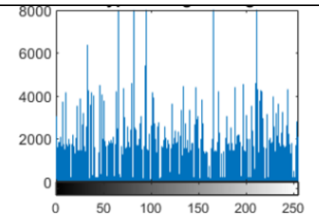
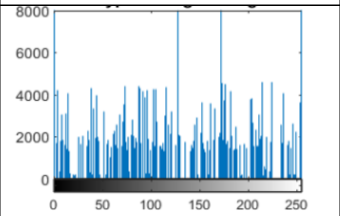
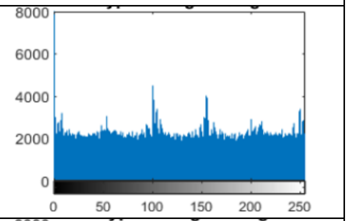
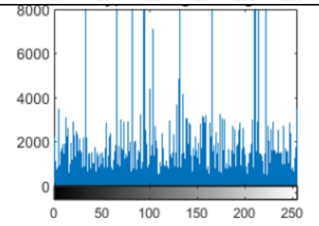
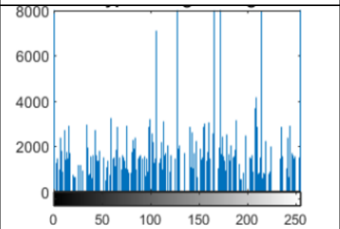
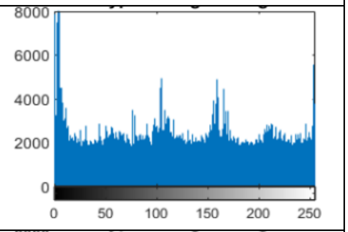
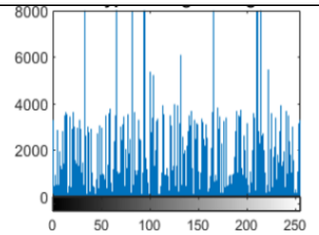
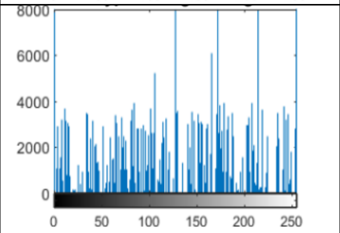
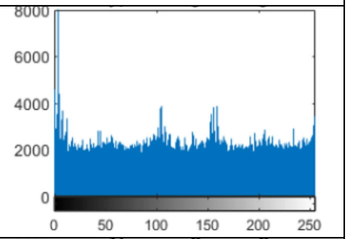
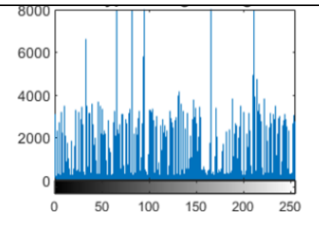
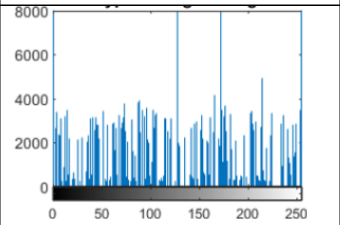
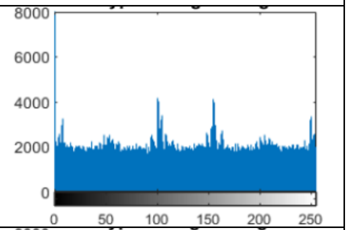
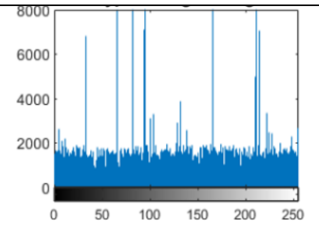
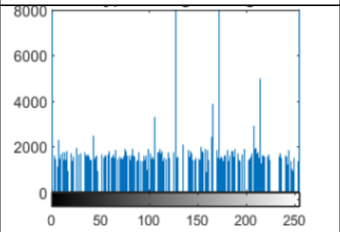
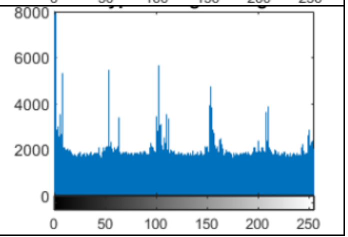
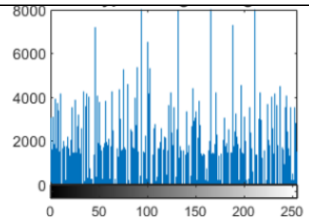
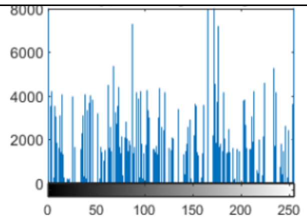
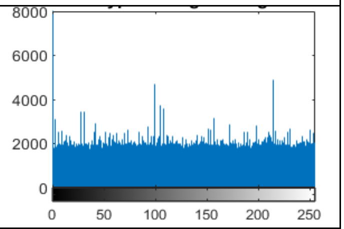
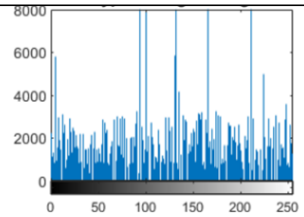
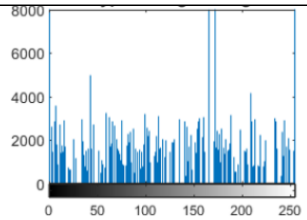
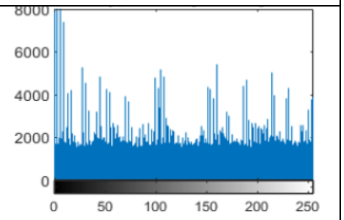
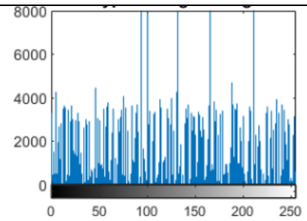
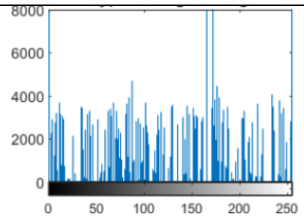
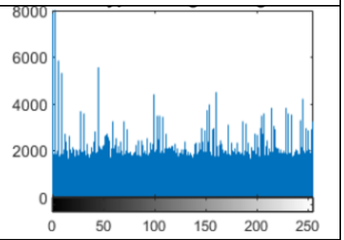
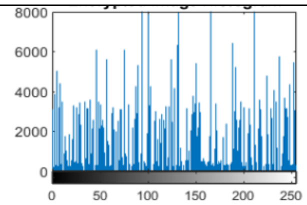
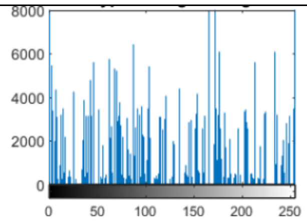
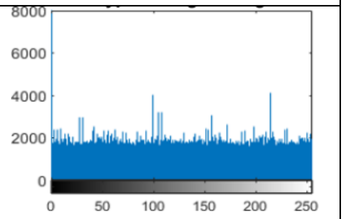
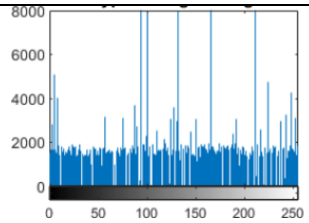
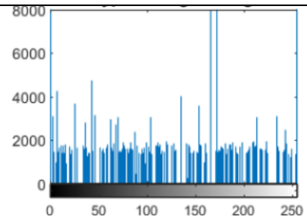
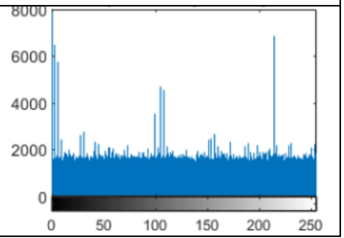
Histogram Analysis for Encrypted Image			
IMG	AES	RSA	ECC with HC
1			
2			
3			
4			
5			

TABLE 10. Histogram Analysis for images in BMP format and 512x512px

Histogram Analysis for Encrypted Image			
IMG	AES	RSA	ECC with HC
1			
2			
3			
4			
5			

V. CONCLUSION

Throughout this research, I carefully investigated the underlying principles of image encryption, evaluated the benefits and limits of symmetric, asymmetric, and hybrid method encryption algorithms, and delved into their specific applications in the field of image security. This study focuses on determining the most effective type of image encryption technique among 3 different algorithms in order to improve the security and protection of autism patients' data and information. AES, RSA and ECC with HC are the chosen three algorithms in this research to conduct the image encryption. All three encryption algorithms were successfully executed, compared, and analyzed in this research. The performance of the encryption was evaluated using NPCR, UACI, HA and time of encryption as a performance measure to determine the security and speed of the encryption. Based on the result obtained, we can conclude AES is considered as the best efficient image encryption in terms of security and speed of encryption. This is because, according to the results, AES is more resistant to differential attacks than RSA, ECC with HC. AES also requires the least amount of time to finish the encryption process when compared to other methods. Moreover, AES is also considered as the second best for statistical attack compared to two other algorithms. For the suggestion and improvement, the algorithms' performance can be further evaluated with various encryption methods. This allows for a more detailed comparison and analysis of the encryption algorithm's efficiency. In addition, measurements like Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) can be used to achieve the most accurate results.

Acknowledgement

I would want to convey my heartfelt appreciation to everyone who helped me achieve this project. First of all, I would like to express my sincere gratitude to my supervisor, Dr. Yusliza binti Yusoff, for her constant support, wise counsel, and insightful observations throughout the research process. Their knowledge and helpful criticism were crucial in determining the focus and calibre of this work. Despite having other students to supervise, she took the time to thoroughly comment on and review my work. Additionally, I extend my thanks to my friends and peers who provided me with critical and valuable information that contributed to the success of my project. Lastly, I would like to express my gratitude and appreciation to all individuals who were directly or indirectly involved in this project.

Conflicts of Interest

The author(s) declare(s) that there is no conflict of interest regarding the publication of this paper.

References

[1] Silverwood, J. (2024). Hospital 2040: How healthcare cybercrime is predicted to escalate. https://www.medicaldevice-network.com/features/hospital-2040-how-healthcare-cybercrime-is-predicted-to-escalate/. (Dark Reading Staff, 2023).

[2] Dark Reading Staff, D. R. (2023). Medical imaging patients exposed in cyber incident. https://www.darkreading.com/cyberattacks-data-breaches/healthcare-facility-informs-patients-of-cyber-incident.

[3] Khaitan, A. (2023). Longhorn cyber attack puts data of 28000 patients at risk. https://thecyberexpress.com/longhorn-cyber-attack-data-28000-patients-risk/.

[4] Demberger, A. (2024). Ransomware ravaging health care: Why cybercriminals target these vital institutions. https://riskandinsurance.com/ransomware-ravaging-healthcare-why-cybercriminals-target-vital-institutions/.

[5] Kessler, G. (1998). *An Overview of Cryptography an Overview of Cryptography*. https://www.cs.princeton.edu/~chazelle/courses/BIB/overview-crypto.pdf.

[6] Chandra, S., Paira, S., Alam, S. S., & Sanyal, G. (2014). A comparative survey of symmetric and asymmetric key cryptography. In 2014 international conference on electronics, communication and computational engineering (ICECCE) (pp. 83-93). IEEE.

[7] Devi, A., Sharma, A., & Rangra, A. (2015). A review on DES, AES and blowfish for image encryption & decryption. *International Journal of Computer Science and Information Technologies*, *6*(3), 3034-3036.

[8] Jiao, K., Ye, G., Dong, Y., Huang, X., & He, J. (2020). Image encryption scheme based on a generalized Arnold map and RSA algorithm. *Security and Communication Networks, 2020*, 1-14.

[9] Chowdhary, C. L., Patel, P. V., Kathrotia, K. J., Attique, M., Perumal, K., & Ijaz, M. F. (2020). Analytical study of hybrid techniques for image encryption and decryption. *Sensors*, *20*(18), 5162

[10] Mohammad, O. F., Rahim, M. S. M., Zeebaree, S. R. M., & Ahmed, F. Y. (2017). A survey and analysis of the image encryption methods. *International Journal of Applied Engineering Research*, *12*(23), 13265-13280.