Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024
DOI : https://doi.org/10.33395/sinkron.v9i1.13054
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Text and Image Encryption Using Symmetric Cryptography Ron Rivest Cipher 2 (RC2)

Saniya Rahma Pratiwi[1)*], Chtristy Atika Sari[2)], Eko Hari Rachmawanto[3)]
[1,2,3)]Informatics Engineering, University of Dian Nuswantoro, Semarang, Indonesia
[1)]111202214858@mhs.dinus.ac.id, [2)]christy.atika.sari@dsn.dinus.ac.id, [3)]eko.hari@dsn.dinus.ac.id

Submitted : Sep 27, 2023 | **Accepted** : Nov 6, 2023 | **Published** : Jan 1, 2024

Abstract: In the current context, ensuring the secure transmission of data over the internet has become a critical concern, with information technology playing a fundamental role. As society advances into the digital information age, the importance of network security issues continues to increase. Therefore, the need for cryptographic technology has emerged to overcome these challenges. Cryptography includes symmetric and asymmetric cryptography. An example of symmetric cryptography is the RC2 algorithm. RC2 is a symmetric encryption algorithm that uses a single key to encrypt and decrypt data. The ciphertext is then concealed within an image using the Stepic technique. The RC2 encryption method also utilizes symmetric encryption, ensuring the security of the encryption process while maintaining efficient encryption and decryption speeds. The result of this research is that the average percentage of MSE is 0.00%, and for PSNR and AVA are 70.85% and 34.93%. However, the AVA value is quite unstable because the average value is below 40%. Meanwhile, image encryption results in the longer the text that needs to be hidden in the image, the higher the UACI percentage. This is inversely proportional to the NPCR, the longer the text that needs to be hidden in the image, the lower the NPCR percentage. The average results obtained for UACI and NPCR values are 41.46% dan 98.13%.

Keywords: RC2 Algorithm, Cryptography, PSNR, AVA, UACI, NPCR

INTRODUCTION

In the current situation, information technology is the most fundamental issue in ensuring the secure transmission of data over the Internet. As society moves into the digital information age, network security issues are also becoming more and more important (B. Savant & D. Kasar, 2021). In addition to these problems, humans also cannot be separated from communication. Communication is critical for accelerating daily human performance in order to maintain community productivity and performance. Chat Messenger is a mefrom cybercriminals or hackers (Farissi et al., 2023). So, we need technology in the form of cryptography that can overcome these problems. Cryptography is the protection of Information and communication through code that leaves only those who need it can read and process information intended for this purpose (Naser, 2021).

Based on the type of key used, cryptography can be divided into symmetric and asymmetric cryptography (Vashi* et al., 2019). Symmetric algorithms use identical keys to encrypt and decrypt (Sood & Kaur, 2023). The strength of the symmetric approach is determined by the security of the key exchange between the sender and recipient. Asymmetric algorithms employ two kinds of keys: public keys and private keys. Because private keys are never transmitted over the network, they are safe and secure(Pujeri* & Pujeri, 2020). Symmetric algorithms can be categorized as either block ciphers or stream ciphers (Yang et al., 2020). A stream cipher encrypts the plaintext bit by bit, while a block cipher uses a group of bits as the unit of encryption. For speedier processing, the block cipher algorithm is

*Saniya Rahma Pratiwi

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v9i1.13054 p-ISSN : 2541-044X

preferable over the stream cipher approach (Rajesh et al., 2019). The majority of widely used symmetric ciphers are block ciphers, such as the Data Encryption Standard (DES), 3DES, RC2, AES, BLOWFISH, and TWOFISH ciphers. On the other hand, RC4 is the most well-known stream cipher. Additional examples of stream ciphers include SALSA20, GRAIN, and TRIVIUM (Abed et al., 2019).

RC2 is a block cipher algorithm that was initially introduced in 1987 (Murugan, 2021). It is also referred to as ARC2. Rivest Cipher or Ron's Code is abbreviated as RC. (Musa, 2023). The primary purpose of RC2 is to serve as a potential replacement for DES (Al-Shabi, 2019). RC2 encryption method very fast about 10 times faster than DES. It operates on data blocks consisting of 8 bytes (64-bits), which are further divided into four words, each with a size of 2 bytes (16 bits). This is referred to as R[0], R[1], R[2], and R[3].(Alenezi et al., 2020).

LITERATURE REVIEW

In this study, we use the RC2 algorithm to encrypt plain text using a single key. The ciphertext generated from RC2 encryption will be stored in an image. In terms of the benefits of cryptography, specifically with respect to the RC2 algorithm, here is a brief overview of the sophistication underlying this research. In this paper (Rasha et al., 2019), the proposed approach involves concealing the ciphertext message within the frequency domain of the frame rate. This method comprises two stages: the initial insertion stage and the subsequent extraction stage. During the image insertion phase, a discrete wavelet decomposition technique (specifically Haar) is employed to transform the image from the time domain to the frequency domain. Text messages undergo encryption using the RC2 and Serpent algorithms. Subsequently, the Least Significant Bit (LSB) algorithm is utilized to conceal the encrypted messages within the high-frequency components (Soni et al., 2020). Research conducted by (Ignatiev et al., 2019) concluded that the RC2 algorithm can be used as an open source by adding a new algorithm, namely the MaxSat algorithm. The merging of the two algorithms aims to help make it easier to implement. From previous research, we had evaluation of this encryption process includes measurements of Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Avalanche (AVA), Unified Average Changing Intensity (UACI), and Number of Pixels Change Rate (NPCR) for encrypted images and using the stepic method in image encryption.

METHOD

Rivest Code 2 (RC2)

The scheme of the RC2 algorithm is as follows: In RC2, the plaintext is divided into separate data blocks. The entire encryption and decryption process takes place on this array, with the input and output also being stored in the same array. RC2 utilizes variable-length keys, ranging from one byte to 128 bytes (Deshpande & Singh, 2019). Upon receiving a key value, RC2 expands it to obtain a new 128-byte key for encryption and decryption operations. Additionally, RC2 accepts another input value called "key bit limits," which determines the maximum suitable key size in bits. Furthermore, keys are generated using both Keys and IV (Initialization Vectors)(Ali et al., 2021). The key consists of 12 characters (96 bits), while the IV consists of 8 characters (64 bits), resulting in a combined synoptic key (Latif, 2020).

The encryption process in RC2 consists of two mashing rounds and a total of 16 mixing rounds. Four words in the intermediate ciphertext are adjusted dependent on the other words in each round. Each mixing cycle employs 16-bit subkeys. The initial plaintext, intermediate result, and final ciphertext are all stored in a four-word 16-bit array R[0],..., R[3]. (Elgeldawi et al., 2019).

For each i = 0, 1, 2, and 3, a round of MIXING is defined as follows:

$$R[i] = R[i] + K[j] + (R[i-1] \,\&\, R[i-2] + (\sim R[i-1] \,\&\, R[i-3]); \quad (1)$$

Equation (1), the symbol "&" represents bitwise AND logic, "⊕" represents bitwise XOR, and "~" represents bitwise complement. In addition, all 16-bit word additions using the "+" operator are done modulo 216.

*Saniya Rahma Pratiwi

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024
DOI : https://doi.org/10.33395/sinkron.v9i1.13054
e-ISSN : 2541-2019
p-ISSN : 2541-044X

$$j = j + 1; \qquad (2)$$

Equation (2) is the variable "j" is a global variable that assures K[j] always represents the first keyword in the expanded key that was not utilized in the MIXING operation.

$$R[i] = R[i] <<< s[i]; \qquad (3)$$

Equation (3)is the provided context is represented where s[0] = 1, s[1] = 2, s[2] = 3, and s[3] = 5. The notation R[i] s[i] denotes that R[i] has been moved left by s[i] bits.

For each i = 0, 1, 2, and 3, the MASHING round is defined as follows:

$$R[i] = R[i] + K[\, R[i - 1] \& 63\,]; \qquad (4)$$

The full procedure of RC2 encryption can be stated as follows:

1. Set words *R[0],..., R[3]* to store 64-bit plaintext chunks.
2. Expand the key to define the phrases *K[0],..., K[63]*.
3. Set the variable j to zero.
4. MIXING should be run five times.
5. Perform one round of MASHING.
6. MASHING should be done six times.
7. One more round of MASHING is required.
8. Repeat MIXING five more times.
9. *R[0],...,R[3]* represent the resulting ciphertext.

Proposed Method

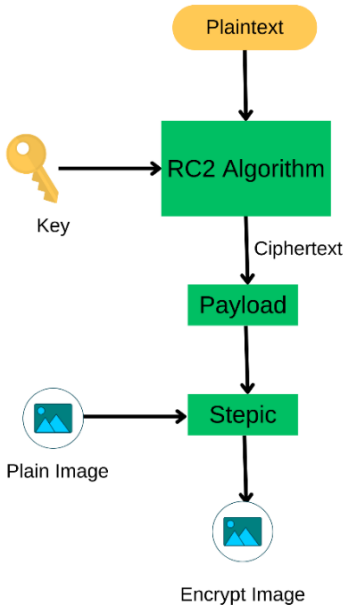

Fig 1. Encryption process with RC2 algorithm

In the picture, there is an encryption process, in which there is a plaintext and key which will be processed by the RC2 algorithm which then produces ciphertext which will be stored in the payload. Next, it had been add an image to carry out the encryption process as well, so that the ciphertext will be

*Saniya Rahma Pratiwi

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024
DOI : https://doi.org/10.33395/sinkron.v9i1.13054
e-ISSN : 2541-2019
p-ISSN : 2541-044X

inserted into the image and the results obtained from the encryption are in the form of an image as illustrated in Fig. 1.

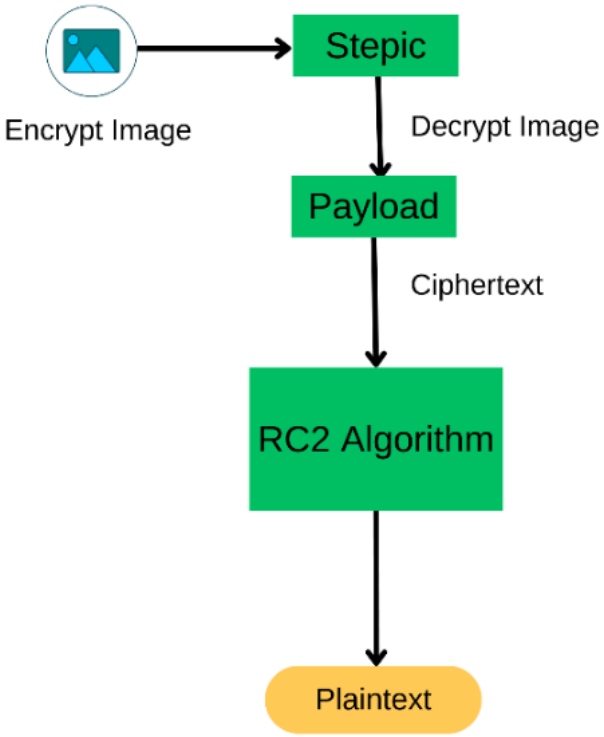

Fig 2. Decryption process with RC2 algorithm

The next picture illustrated in Fig. 2 is the process of decryption. Where encrypted images containing ciphertext inserts will be decrypted to produce a plaintext as before. The process is that the result of the encryption image is carried out by a stepic conversion process first, then generates a payload in the form of payload which produces ciphertext then the RC2 algorithm will carry out the decryption process then produce plaintext.

RESULT

RC2, which is generally used for text data protection only, has been implemented in this study for text and images. In addition, there is a test that will be carried out on encrypted text using MSE, PSNR, and Avalanche. We have conducted an assessment on text encryption using a diverse range of sentence variations. The word count for the shortest sentence was 64 words, while the longest sentence consisted of 512 words. While testing the encrypted images using Histogram, UACI, and PCNR. In this study, testing will be carried out on variations in text length for image encryption using one image and 3 different size images. RC2, which is generally used for text data protection only, in this research has been implemented for text and images. In addition, testing will be carried out on encrypted text using MSE, PSNR, and Avalanche. We have assessed text encryption using a wide variety of sentences. The number of words for the shortest sentence is 64 words, while the longest sentence is 512 words. Meanwhile, testing encrypted images uses Histogram, UACI, and PCNR. In this research, we will test variations in text length for image encryption using one image and 3 images of different sizes. The original image was obtained from the wizardingworld website with an initial size of 1920 x 1080 pixels.

*Saniya Rahma Pratiwi

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024
DOI : https://doi.org/10.33395/sinkron.v9i1.13054
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Fig 3. Original image

In the following table are the results of the tests that have been carried out. The values of MSE, PSNR, AVA, UACI and NPCR can be seen in Table 1.

Table 1. MSE, PSNR, AVA, UACI and NPCR Calculation Results

Image Size	*Word*	*MSE*	*PSNR*	*AVA*	*UACI*	*NPCR*
1920 x 1080	64	0.00%	81.40%	35.31%	43.46 %	99.91%
	256	0.00%	76.08%	35.00%	43.47%	99.71%
	512	0.00%	74.97%	34.96%	43.47%	99.63%
AVG 1		0.00%	77.48%	35.09%	43.46%	99.75%
512 x 288	64	0.00%	70.05%	34.93%	39.95%	98.87%
	256	0.00%	64.63%	34.77%	39.97%	96.06%
	512	0.00%	63.48%	35.06%	40.00%	94.90%
AVG 2		0.00%	66.05%	34.92%	39.97%	96.61%
720 x 450	64	0.00%	73.01%	34.79%	40.95%	99.43%
	256	0.00%	67.59%	34.56%	40.97%	98.02%
	512	0.00%	66.50%	35.01%	40.97%	97.45%
AVG 3		0.00%	69.03%	34.78%	40.96%	98.03%
TOTAL AVG		**0.00%**	**70.85%**	**34.93%**	**41.46%**	**98.13%**

Based on the table above, the result of text encryption is that the more words that must be encrypted, the more MSE we have. This means that the more words that need to be encrypted the less the proportion of PSNR and AVA. Using the table data, we average each proportion in each evaluation. The average percentage of MSE is 0.00%, for PSNR and AVA are 70.85% and 34.93%. Meanwhile, image encryption results in the longer the text that needs to be hidden in the image, the higher the UACI percentage. This is relevant to the image size, the smaller the image, the more it changes from short text to longer text. This is inversely proportional to the NPCR, the longer the text that needs to be hidden in the image, the lower the NPCR percentage. The smaller the image, the more it changes from short text to long text. Using the table data, we averaged each percentage in each evaluation. UACI average percentage is 41.46%, for NPCR is 98.13%

*Saniya Rahma Pratiwi

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024
DOI : https://doi.org/10.33395/sinkron.v9i1.13054
e-ISSN : 2541-2019
p-ISSN : 2541-044X

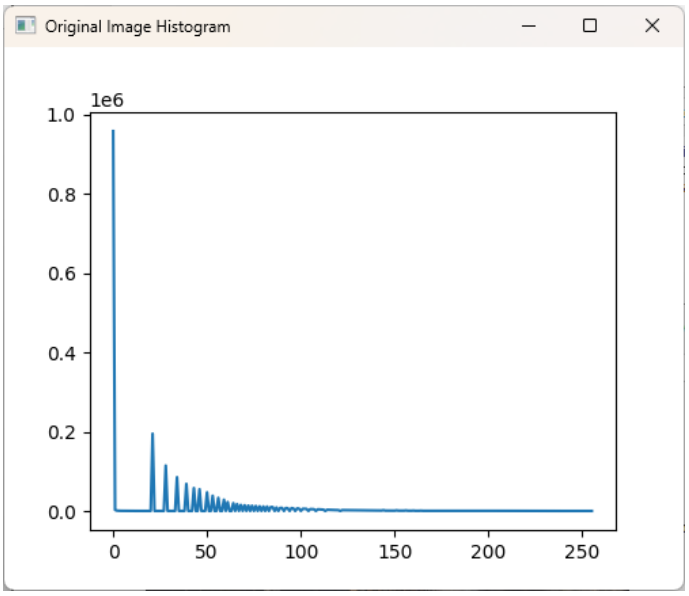

Fig 4. Original image histogram of 1920 x 1080

In addition, we tried to evaluate the histogram. The histograms to be compared are the original image histogram and cipher histograms that have text lengths. For the text itself, use 512 words as shown in Fig. 4. As we can see there are many useful histograms between 20(x) until 90(x) and 0(y) until 0.2(y). Fig 5, shows the histogram of a ciphertext image that has a resolution of 1920 x 1080 pixels and contains 512 words of text. When comparing the cipher image to the original unencrypted image, the encryption process becomes clear. So, it can be concluded that the original image when encrypted will experience a very significant histogram change

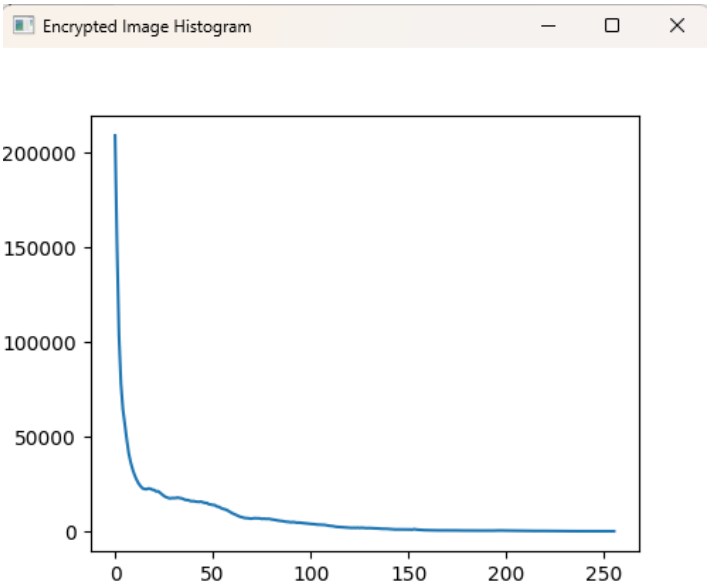

Fig 5. Cipher image histogram of 1920 x 1080 with 512 word

In Fig 6, an important observation is the presence of several significant histograms in the range 20(x) to 80(x) and 0(y) to 15000(y). Compared to the histogram of the original image with an image size of 1920 x 1080, the histogram in Fig 6 has a larger range of values than the histogram in Fig 4. This is because it is influenced by different image sizes, so the smaller the image size, the greater the y value in the histogram.

*Saniya Rahma Pratiwi

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024
DOI : https://doi.org/10.33395/sinkron.v9i1.13054
e-ISSN : 2541-2019
p-ISSN : 2541-044X

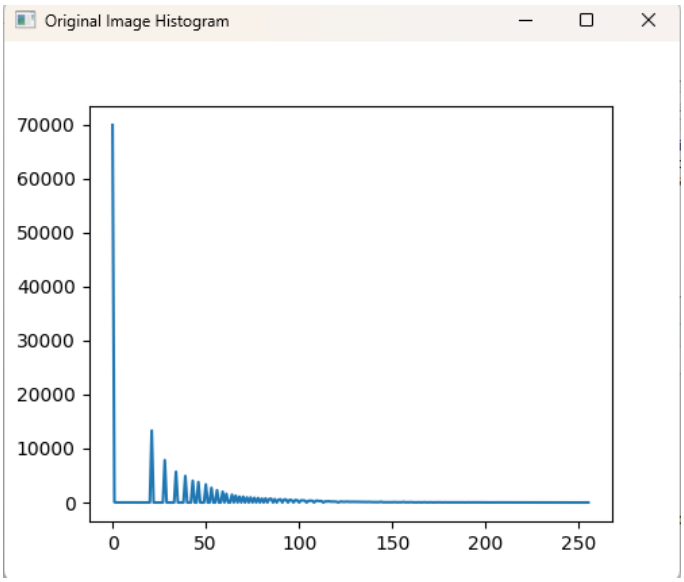

Fig 6. Original image histogram of 512 x 288

Moving on to Fig 7, displays the histogram of the cipher image, which has the same resolution of 512 x 288 pixels and incorporates 512 words of text. When comparing this cipher image with the original unencrypted image, the encryption process becomes clear. Meanwhile, when compared with the cipher histogram at an image size of 1920 x 1080, there is also a difference between the graph values of the histogram results. If in the histogram of Fig 5, the graph results in the y value exceeding 20000(y) while in Fig 6 the value exceeds 2000(y).

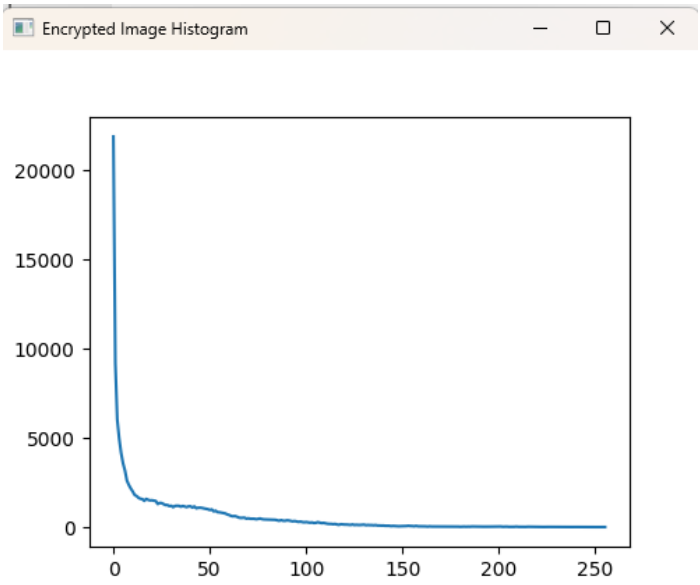

Fig 7. Cipher image histogram of 512 x 288 with 512 word

In Fig 8, there are actual observations of several significant histograms in the range 20(x) to 80(x) and 0(y) to 30000(y). Compared to the original image histograms in Fig 4 and Fig 6, the largest y value is an image that is 720 x 405 in size. This can happen because of the difference in the size of the images which greatly affects the results of the histogram graph. In Fig 8, there are actual observations of several significant histograms in the range 20(x) to 80(x) and 0(y) to 30000(y). Compared to the original image histogram in Fig 4 and Fig 6, the largest y value is the image with a size of 720 x 405.

*Saniya Rahma Pratiwi

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024
DOI : https://doi.org/10.33395/sinkron.v9i1.13054
e-ISSN : 2541-2019
p-ISSN : 2541-044X

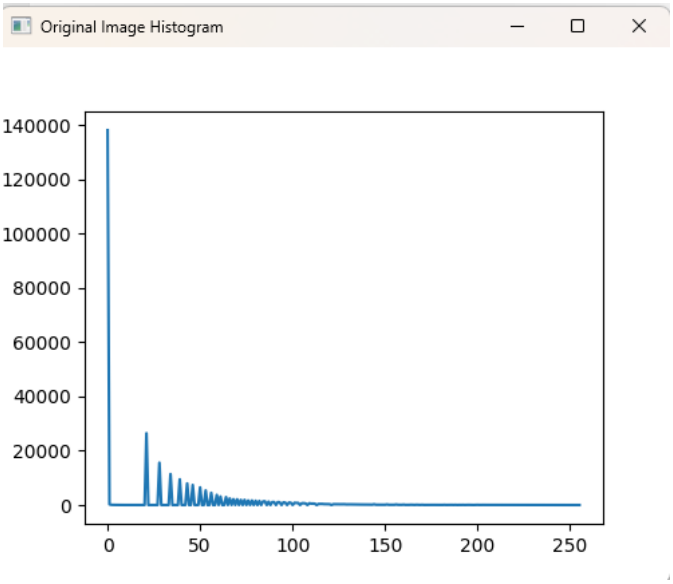

Fig 8. Original image histogram of 720 x 405

This can occur due to the difference in image size which greatly affects the results of the histogram graphics. Whereas if we compare it with the histogram with an image size of 1920 x 1080 and an image size of 512 x 288 it had been seen that the histogram in Fig 9 has a y value which is on average between the two other image sizes.

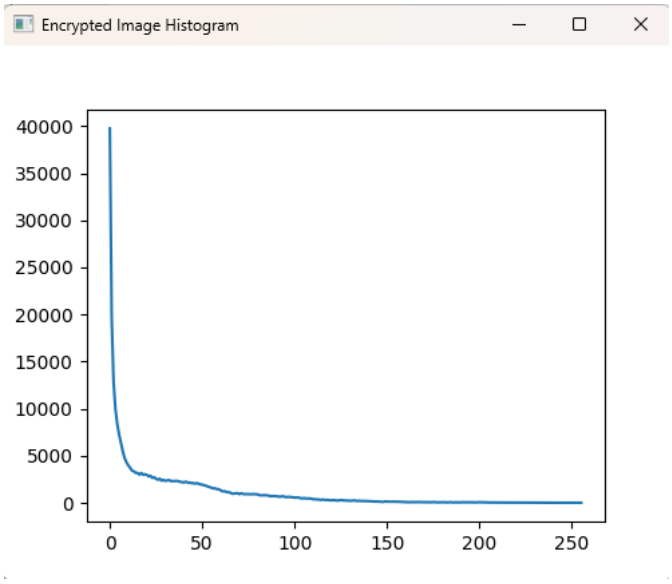

Fig 9. Cipher image histogram of 720 x 405 with 512 word

We concluded based on some of the histogram graphs above that, plain images and cipher images when encrypted, the difference will be seen clearly. From the several cipher histogram graphs above with different image sizes, we can see that the differences in the graph results are not too significant. This means that the bigger the image size, the more changes we can get from the encryption. This is also relevant to hidden text, the longer the text is hidden in the image, the more opportunities the algorithm creates.

*Saniya Rahma Pratiwi

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

DISCUSSIONS

Based on the data obtained, the evaluation of Text Encryption and Image Encryption, we have achieved a satisfactory quality percentage. The results of the text encryption evaluation, based on the MSE (Mean Squared Error) testing, show an average value of 0.00%, indicating good performance. It also averaged 70.85% in the Peak Signal to Noise Ratio (PSNR) evaluation, which indicates a high level of quality. However, the evaluation of the AVA (Average Value Assessment) value shows a slightly less stable value of 34.93%. Moving on to image encryption, the test results indicate good performance. The UACI (Unified Average Changing Intensity) evaluation shows an average value of 41.46%, suggesting satisfactory results. Additionally, the NPCR (Number of Pixels Change Rate) evaluation demonstrates a high average value of 98.13%, indicating a high degree of consistency between encrypted images. Therefore, based on these evaluations, it concluded text and image encryption using the RC2 algorithm provides a secure approach to safeguarding data and maintaining its integrity.

CONCLUSION

This study aims to create an RC2-based encryption technique by embedding the ciphertext in a picture. The findings reveal that as the number of words requiring encryption increases, the MSE (Mean Squared Error) also increases. This implies that a higher number of words results in a lower proportion of PSNR (Peak Signal-to-Noise Ratio) and AVA (Average Value Assessment). By analyzing the tabulated data, the average MSE percentage is determined to be 0.00%, while the average percentages for PSNR and AVA are 70.85% and 34.93%, respectively. Furthermore, the results of image encryption indicate that as the length of the hidden text within the image increases, the UACI (Unified Average Changing Intensity) percentage also increases. This relationship is influenced by the size of the image, where smaller images exhibit more significant changes when transitioning from short to longer texts. Conversely, the NPCR (Number of Pixels Change Rate) percentage decreases as the length of the hidden text within the image increases. Similar with UACI, this is more pronounced in smaller images. The average UACI percentage is 41.46%, while the average NPCR percentage is 98.13%. It is crucial to remember, however, that the RC2 encryption technique has several restrictions. The AVA percentage may exhibit slight instability, falling below 40%. Additionally, when encrypting large amounts of data, RC2 experiences a decrease in performance and may not function properly with small image sizes. To address these challenges, a desktop application utilizing the Python language has been developed to facilitate easier encryption and decryption processes.

REFERENCES

Abed, S., Jaffal, R., Mohd, B. J., & Alshayeji, M. (2019). FPGA modeling and optimization of a SIMON lightweight block cipher. *Sensors (Switzerland)*, *19*(4). https://doi.org/10.3390/s19040913

Al-Shabi, M. A. (2019). A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security. *International Journal of Scientific and Research Publications (IJSRP)*, *9*(3), p8779. https://doi.org/10.29322/ijsrp.9.03.2019.p8779

Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric encryption algorithms: Review and evaluation study. *International Journal of Communication Networks and Information Security*, *12*(2), 256–272.

Ali, H. J., Jawad, T. M., & Zuhair, H. (2021). Data security using random dynamic salting and AES based on master-slave keys for Iraqi dam management system. *Indonesian Journal of Electrical Engineering and Computer Science*, *23*(2), 1018–1029. https://doi.org/10.11591/ijeecs.v23.i2.pp1018-1029

B. Savant, V., & D. Kasar, R. (2021). A Review on Network Security and Cryptography. In *Research Journal of Engineering and Technology* (pp. 110–114). https://doi.org/10.52711/2321-581x.2021.00019

Deshpande, K., & Singh, P. (2019). *G LOBAL J OURNAL OF E NGINEERING S CIENCE AND R ESEARCHES*. *418*(C), 418–427.

Elgeldawi, E., Mahrous, M., & Sayed, A. (2019). A Comparative Analysis of Symmetric Algorithms in Cloud Computing: A Survey. *International Journal of Computer Applications*, *182*(48), 7–16.

*Saniya Rahma Pratiwi

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

https://doi.org/10.5120/ijca2019918726

Farissi, A., Pradata, A., & Miraswan, K. J. (2023). *Securing Messages Using AES Algorithm and Blockchain Technology on Mobile Devices*. *8*(2), 1166–1171.

Ignatiev, A., Morgado, A., & Marques-Silva, J. (2019). RC2: an Efficient MaxSAT Solver. *Journal on Satisfiability, Boolean Modeling and Computation*, *11*(1), 53–64. https://doi.org/10.3233/sat190116

Latif, I. H. (2020). Time Evaluation of Different Cryptography Algorithms Using Labview. *IOP Conference Series: Materials Science and Engineering*, *745*(1). https://doi.org/10.1088/1757-899X/745/1/012039

Murugan, A. (2021). *A Spiral Pattern Based , DNA Cryptography Encryption Design*. *November*.

Musa, K. (2023). *Evaluating Encryption Algorithm Method Based on Software Encryption Tools for Information Security International Journal of Current Science Research and Review Evaluating Encryption Algorithm Method Based on Software Encryption Tools for Information Secur*. *June*. https://doi.org/10.47191/ijcsrr/V6-i6-12

Naser, S. M. (2021). Cryptography : From the Ancient History To Now , It ' S Applications. *International Journal of Mathematics and Statistics Studies*, *9*(August), 10–30. https://doi.org/10.13140/RG.2.2.13438.51524

Pujeri*, D. U., & Pujeri, D. R. (2020). Symmetric Encryption Algorithm using ASCII Values. *International Journal of Recent Technology and Engineering (IJRTE)*, *8*(5), 2355–2359. https://doi.org/10.35940/ijrte.e5980.018520

Rajesh, S., Paul, V., Menon, V. G., & Khosravi, M. R. (2019). A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices. *Symmetry*, *11*(2). https://doi.org/10.3390/sym11020293

Rasha, A. T., Ali, H., & Jaddoa, S. H. (2019). Hiding Secret Text in Image Using Rc4 and Rijindeal Algorithm. *Online)*, *6*(1), 12–18. www.jifactor.com

Sara, U., Akter, M., & Uddin, M. S. (2019). Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study. *Journal of Computer and Communications*, *07*(03), 8–18. https://doi.org/10.4236/jcc.2019.73002

Soni, G., Rawat, A., Jain, S., & Sharma, S. (2020). *A Pixel-Based Digital Medical Images Protection Using Genetic Algorithm with LSB Watermark Technique* (pp. 483–492). https://doi.org/10.1007/978-981-13-8406-6_46

Sood, R., & Kaur, H. (2023). *A Literature Review on RSA, DES and AES Encryption Algorithms*. 57–63.

Vashi*, D., Bhadka, D. H. B., Patel, D. K., & Garg, D. S. (2019). Performance of Symmetric and Asymmetric Encryption Techniques for Attribute Based Encryption. *International Journal of Recent Technology and Engineering (IJRTE)*, *8*(4), 176–182. https://doi.org/10.35940/ijrte.c6597.118419

Yang, C., Ling, Y., & Li, X. (2020). Information encryption algorithm in power network communication security model. *IOP Conference Series: Materials Science and Engineering*, *750*(1). https://doi.org/10.1088/1757-899X/750/1/012161

*Saniya Rahma Pratiwi

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.