Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024
DOI : https://doi.org/10.33395/sinkron.v9i1.13175
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Implementation of the Arnold Catmap on a Combination of Symmetric and Asymmetric Cryptography

F.Riza[1)*], Martiano[2)], Farid Akbar Siregar[3)]
[1,2,3)]Fakultas Ilmu Komputer dan Teknologi Informasi, Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara, Medan, Indonesia
[1)]ferdyriza@umsu.ac.id, [2)] martiano@umsu.ac.id, [3)]faridakbar@umsu.ac.id

Submitted : Nov 22, 2023 | **Accepted** : Nov 23, 2023 | **Published** : Jan 1, 2024

Abstract: The escalating need for robust data security has propelled cyber security practitioners into a perpetual quest for innovative solutions. This endeavor involves the strategic amalgamation of cryptographic algorithms with meticulously customized alterations to specific algorithmic processes. In this pursuit of heightened data protection, the Arnold Cat Map emerges as a pivotal tool, a mathematical transformation that gracefully elucidates the intricate movement of points within a two-dimensional plane. This movement occurs in a systematic and repetitive manner, rendering it an indispensable asset in the domains of cryptography and image scrambling. The Arnold Cat Map operates by meticulously relocating each point within the two-dimensional plane to a fresh coordinate, all the while adhering to an intricately structured pattern. The result is a formidable "mixing" effect that enhances data security. When applied theoretically to widely employed encryption methods like Advanced Encryption Standard (AES) for symmetric encryption and the Rivest-Shamir-Adleman (RSA) algorithm for asymmetric encryption, the Arnold Cat Map exhibits the potential to significantly augment the randomness of the encrypted output. This augmentation of randomness, in turn, fortifies the security of digital assets and communications, making them more resilient against adversarial attacks. By introducing this innovative concept into the realm of cryptography, cyber security practitioners endeavor to fortify data security, offering a higher degree of confidence in the protection of sensitive information and digital assets against a backdrop of ever-evolving cyber threats.

Keywords: AES, RSA, Arnold Map, Digital Image

INTRODUCTION

Encryption is one of the alternatives to secure information contained in digital images, whether it's for secure storage (Chidambaram, Raj, Thenmozhi, & Amirtharajan, 2020) or transmission through communication media (Abdelfatah, 2019). Just like other types of data such as text, documents, and other digital files, digital images are a common medium for storing or conveying information in communication, making the security of the information they contain crucial in today's global communication era.

Securing digital images using encryption is not a new concept in the present era. Many applications and research efforts have been conducted to implement the security of digital images. This ranges from the use of simple cryptography methods like the Vigenere cipher (Riadi, Fadlil, & Tsani, 2022) and the Hill cipher (Sujjada & Juniar, 2021) to modern cryptography techniques like AES-Rijndael (Azanuddin, Yakub, & Prayudha, 2022) and RC5 (Purnama, 2019). Furthermore, contemporary

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v9i1.13175 p-ISSN : 2541-044X

research has also leveraged neural networks in the encryption and decryption processes (Man, Li, Di, Sheng, & Liu, 2021).

In most conventional encryption applications for digital images, symmetric cryptography methods are commonly used. These methods align with the characteristics of digital images, such as the value range and the input and output sizes used. The limitations imposed by the characteristics of digital image data, where values are stored in pixels with a range of 0 to 255, make it challenging to apply all cryptography methods directly to the encryption and decryption processes, especially asymmetric cryptography methods that employ public and private keys.

Asymmetric cryptography offers advantages compared to conventional symmetric cryptography. With a pair of public and private keys, it ensures that only the rightful recipient with the matching private key can perform the decryption process. This differs from symmetric cryptography, where the encryption key must be sent to the recipient, allowing them to conduct decryption.

Considering these challenges, some research adopts a different approach by using the public key to generate chaotic sequences, which are then used as key streams in the encryption process. This approach can be seen in two distinct studies by Jiao et al. (Jiao, Ye, Dong, Huang, & He, 2020) and Lin (Lin & Li, 2021). The encryption model used by Jiao et al. is quite effective, utilizing cyclic scrambling in addition to XOR diffusion to shuffle the positions of encrypted pixel results. This model can be further enhanced in two aspects: firstly, by modifying the four randomly selected secret numbers and secondly, by replacing the XOR diffusion operation with another symmetric cryptography method like AES. This research aims to reduce the number of chaotic sequence values generated, originally one value per pixel, to one value per pixel block. It also seeks to minimize the cyclic scrambling process while enhancing the randomness of the results compared to standard XOR diffusion.

LITERATURE REVIEW

Advance Encryption Standard (Rijndael)

AES (Advanced Encryption Standard) is a symmetric cryptographic algorithm commonly used to protect data in military, banking, and government applications. AES operates by encrypting and decrypting data in fixed-size blocks of 128 bits and supports three key sizes: 128, 192, or 256 bits (Azanuddin, A., Yakub, S. & Prayudha, J., 2022).

The AES encryption process begins by breaking the message into 128-bit blocks, with each block being encrypted separately using the same key. AES employs substitution and permutation operations on each data block to enhance data security. This encryption process produces ciphertext.

To decrypt the ciphertext, AES utilizes the same key that was used during the encryption process to transform the ciphertext back into its original form, known as plaintext. The AES decryption process is conducted similarly to the encryption process, but it uses the same key as employed during encryption.

The stages in the AES algorithm encompass key generation, round key addition, byte substitution, row shifting, and column mixing. This process is repeated for each data block, using the same key for each round. The number of rounds employed for each data block depends on the key size: 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys (Azanuddin, A., Yakub, S. & Prayudha, J., 2022).

AES has become a widely adopted symmetric cryptography standard known for its strong performance. It is efficient in terms of processing time and demands minimal computer resources, making it suitable for applications requiring extensive data processing. However, the security of AES relies on factors such as key length and available computational power. It is recommended to use longer key lengths to enhance security.

RSA (Rivest–Shamir–Adleman)

RSA (Rivest–Shamir–Adleman) is an asymmetric cryptographic algorithm used to secure messages through the utilization of a pair of keys: the public key and the private key. RSA relies on

*name of corresponding author

mathematical operations involving modular arithmetic and the factorization of large integers (Lin, R. & Li, S., 2021).

The steps in the RSA algorithm begin with the generation of a key pair, consisting of the public key and the private key. The public key is employed for message encryption, while the private key is used for decryption (Lin, R. & Li, S., 2021). The process of creating the public and private keys encompasses:

1. Select two random large prime numbers, p and q.
2. Calculate n = p x q, where n is the modulus.
3. Compute the totient φ(n) = (p-1) x (q-1).
4. Choose a random integer e, with 1 < e < φ(n), such that e and φ(n) are coprime.
5. Calculate d such that d x e ≡ 1 (mod φ(n)), or mathematically, d = e^(-1) mod φ(n).
6. The public key consists of the pair (e, n), while the private key comprises the pair (d, n).

Once the public and private keys are generated, the RSA encryption process can be performed by converting the message into an integer and computing the ciphertext using the public key. This process involves:

1. Convert the message into an integer format, denoted as m, where 0 ≤ m < n.
2. Calculate the ciphertext using the formula c ≡ m^e (mod n).
3. The ciphertext c is the result of encryption.

The RSA decryption process is carried out by reversing the ciphertext into the original message using the private key. This process entails:

1. Calculate the plaintext m using the formula m ≡ c^d (mod n).
2. The plaintext m is the result of decryption.
3. Convert the integer m back into its original message form.

RSA has become one of the widely adopted cryptographic standards known for its high security level, as it employs large prime numbers as parameters. However, the speed of RSA depends on the key size used, with larger keys potentially affecting RSA's performance.

In summary, the RSA algorithm is an effective and robust cryptographic algorithm for securing messages using a pair of keys: the public key and the private key (Lin, R. & Li, S., 2021). The processes of key pair generation, encryption, and decryption in RSA are vital stages in utilizing this algorithm.

Arnold Map

The Arnold Map is a cryptographic algorithm that employs transformation operations in the realm of integers to secure messages. This algorithm is based on a transformation function that rearranges the positions of pixels in an image using a transformation matrix. The stages in the Arnold Map algorithm include:

1. Prepare an image to be encrypted with dimensions that are multiples of 2, such as 256x256 or 512x512.
2. Define the encryption key values as two integers, a and b.
3. Execute the image transformation using the following equations:
   x' = (x + y) mod N
   y' = (ax + by) mod N

Where x and y are pixel coordinates in the image, x' and y' are the new coordinates after transformation, a and b are the encryption keys, and N is the image size.

4. Repeat step 3 for t times, where t is a predetermined number of iterations.
5. The image with altered pixel positions is the encrypted result.

The decryption process for the Arnold Map involves reversing the pixel positions that were altered during encryption. The steps in the Arnold Map decryption process are as follows:

1. Provide the encrypted image.
2. Determine the encryption key values as two integers, a and b.
3. Apply the inverse transformation to the image using the following equations:
   x' = (by - y) mod N
   y' = (-ax + x + y) mod N

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024
DOI : https://doi.org/10.33395/sinkron.v9i1.13175
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Where x and y are coordinates of pixels in the encrypted image, x' and y' are the new coordinates after the inverse transformation, a and b are the encryption keys, and N is the image size.

4. Repeat step 3 for t times, where t is a predetermined number of iterations.
5. The image with its pixel positions restored to their original state is the decrypted result.

The advantage of the Arnold Map algorithm is its ability to quickly and efficiently process both images and text. However, this algorithm is less secure and vulnerable to decryption when small encryption keys are used. Therefore, the use of large encryption keys is essential to maintain the security of messages encrypted with the Arnold Map algorithm.

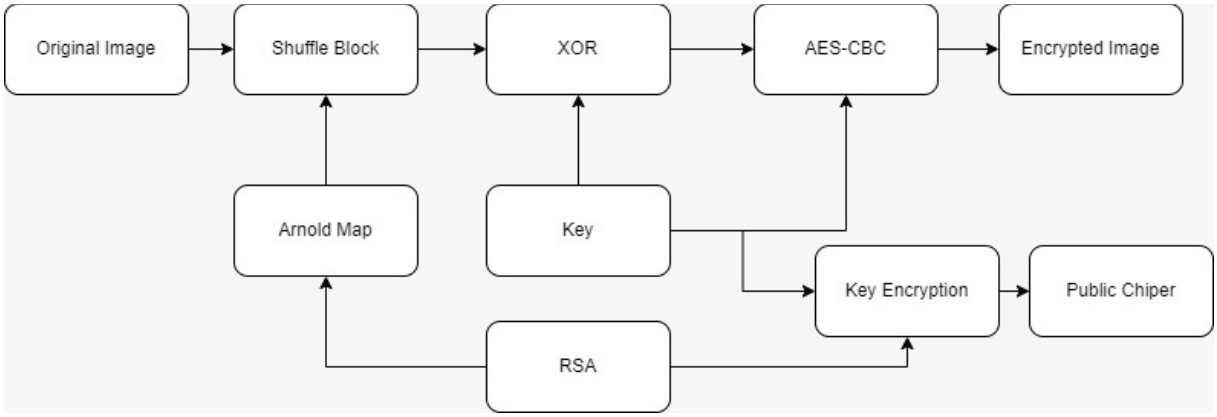


Figure 1. Encryption Steps

In Figure 1. the proposed cryptographic framework, RSA is employed for the generation of private and public keys, where the modulus of the RSA key serves as the foundation for generating a random sequence via the Arnold Catmap algorithm. This random sequence is utilized to shuffle the order of blocks in the input image. The rearranged blocks are subsequently subjected to XOR operation with a symmetric key. The resultant data undergoes encryption using the Cipher Block Chaining (CBC) mode of the Advanced Encryption Standard (AES), culminating in the creation of an encrypted image. Simultaneously, the symmetric key is encrypted using RSA, yielding an encrypted key. This comprehensive approach integrates the strengths of RSA key generation, Arnold Catmap randomness infusion, symmetric key encryption, and CBC AES encryption, providing a robust and multi-layered security paradigm for image encryption.

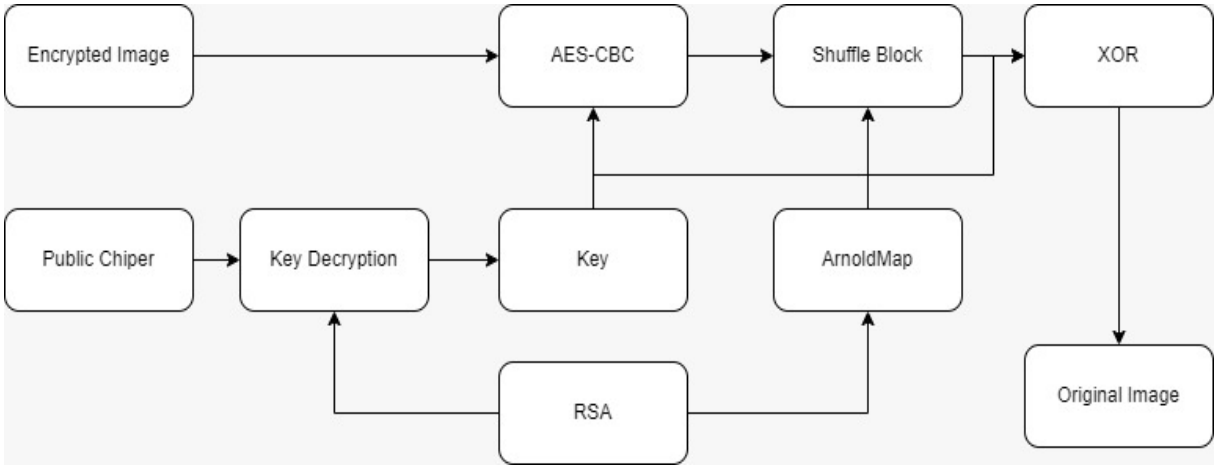


Figure 2. Decryption Steps

While in figure 2. In the devised cryptographic scheme, the decryption process involves reversing the sequence of operations applied during encryption. Initially, the encrypted key, generated through RSA

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v9i1.13175 p-ISSN : 2541-044X

encryption, is decrypted to obtain the symmetric key. Subsequently, the encrypted image, a product of the CBC AES encryption, undergoes decryption using the inverse of the AES algorithm and the CBC mode. The result is a sequence of blocks that were originally XORed with the symmetric key. To revert the shuffling introduced by the Arnold Catmap algorithm, an inverse process is applied to restore the original order of blocks in the image. Finally, the RSA private key is utilized to decrypt the symmetric key, completing the decryption process. This comprehensive reversal ensures the retrieval of the original, unencrypted image from the encrypted counterpart, highlighting the efficacy of the integrated cryptographic processes in both encryption and decryption phases.

in the communication flow from the sender to the receiver, two crucial pieces of encrypted data are transmitted: the image that has been encrypted using the CBC AES algorithm, resulting in an encrypted image, and the symmetric key that has been encrypted using RSA, yielding an encrypted key. This dual-layered encryption strategy enhances the overall security of the communication.

The encrypted image ensures the confidentiality and integrity of the visual content during transmission, while the encrypted key, being transmitted alongside the encrypted image, safeguards the confidentiality of the symmetric key used in the image encryption process. The receiver, possessing the appropriate RSA private key, can decrypt the symmetric key and subsequently decrypt the encrypted image, ultimately restoring the original, unencrypted visual content. This bifurcated approach fortifies the communication channel against unauthorized access and interception, exemplifying a robust encryption methodology for secure image transmission.

METHOD

Here, the research steps, analytical and experimental methods used to obtain comparative results from each pseudo-random number generation algorithm are explained. For details, see Figure 1. as follows:

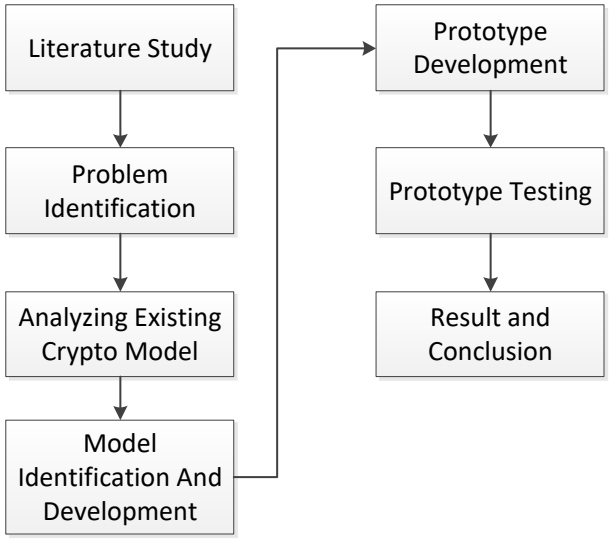


Figure 3. Research Stages

The elaboration of the research stages as seen in the image above is as follows:

1. Literature Review: In this stage, the Head Researcher and Research Members collectively conduct a study and analysis of literature, specifically recent research articles related to digital image security using cryptography. The study results are then gathered, and suitable models are selected for the research needs.
2. Problem Identification: In this stage, an analysis will be carried out regarding the fundamental requirements related to the research roadmap, which is a proficient security model. This involves analyzing the selected models and observing the issues present in these models.
3. Existing Cryptographic Model Analysis: In this stage, an analysis is performed on the models obtained from the literature review and problem identification. The model analyzed in this

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024
DOI : https://doi.org/10.33395/sinkron.v9i1.13175
e-ISSN : 2541-2019
p-ISSN : 2541-044X

research is the one proposed by Jiao et al., which utilizes the generalized Arnold map and RSA cryptography to secure digital images.

4. Model Modification and Development: In this stage, the model is modified and developed using the Jiao et al. model as a base. Initially, the input image pixels will be grouped into matrices or encryption blocks of 128 bits. Then, using RSA, chaos sequences S and R will be generated for the number of blocks formed from the input image. This will result in fewer chaos sequences compared to the Jiao et al. model. The encryption flow stage will then follow the Jiao et al. model with the replacement of the XOR diffusion process with CBC AES encryption operations to enhance the randomness of the encryption process.
4. Prototype Development: In this stage, a digital library and application prototype will be developed to implement the developed model using the Visual Basic .Net programming language.
4. Prototype Testing: In this stage, testing of the built prototype will be conducted by encrypting and decrypting digital images. The quality of the encryption results will be measured using Histogram Analysis, Correlation Coefficient, and Information Entropy.
5. Results and Conclusion: In this stage, all information from the developed model, the constructed prototype, and the analysis of test results will be summarized, leading to the formulation of research conclusions.

RESULT

The determination of alternative sample data is 10 types of images with different color variations as described in Figure 3.

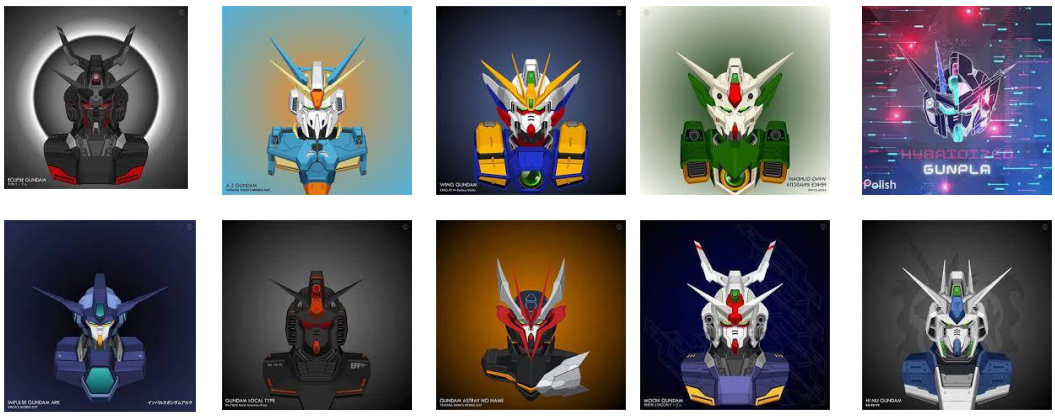


Figure 3. Test Images

The table presented below displays the results of testing images that will be utilized for assessing the system. These images are employed as keys in the encryption and decryption processes of the symmetric algorithms AES, RSA, and Arnold Cat Map. The selection of these images is based on their color similarity, structured color distribution, and the deliberate inclusion of similar elements to facilitate the forthcoming analysis.

The primary purpose of this image selection is to create a diverse and representative dataset for evaluating the performance and security of encryption algorithms. By choosing images with similar color patterns and distribution, we aim to gauge how these algorithms handle various image types, ensuring their adaptability to real-world scenarios. This meticulous selection process also facilitates in-depth analysis and enables a comprehensive assessment of each algorithm's encryption and decryption capabilities.

Tabel 1. Encryption and Decryption Result

*name of corresponding author

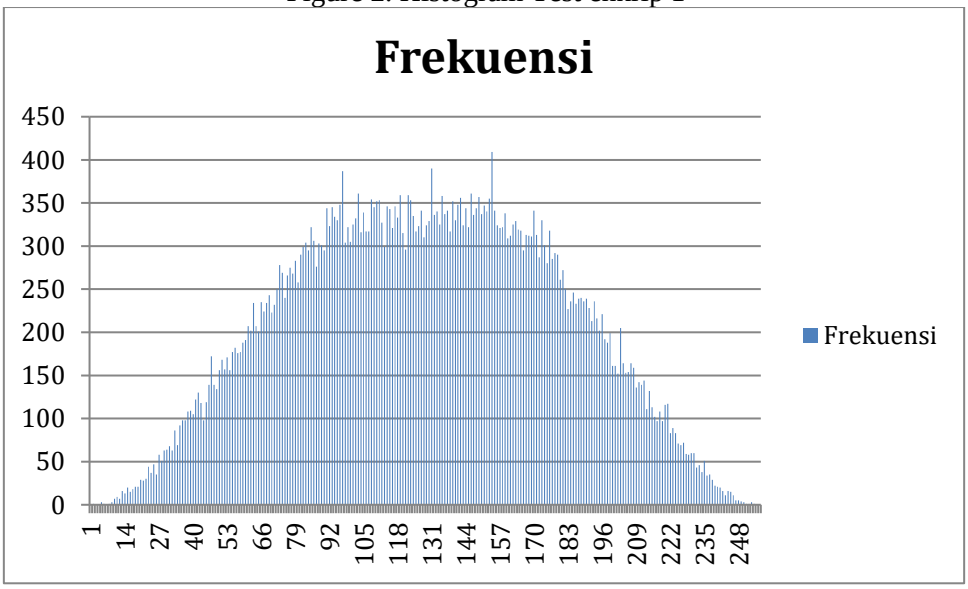
Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024
DOI : https://doi.org/10.33395/sinkron.v9i1.13175
e-ISSN : 2541-2019
p-ISSN : 2541-044X

No	Name	Public Key	Private Key	Public Chiper
1	Uji 1	3-2173	1387-2173	#991#779#1644#1558#1797#1216#1423#30#1036#556#126#1550#1938#1631#1730#1012
2	Uji 2	5-551	101-551	#336#261#309#266#487#386#341#245#121#349#309#23#128#297#311#225
3	Uji 3	3-1219	763-1219	#1077#516#537#1049#1076#820#882#1076#644#1045#941#424#673#152#9#725
4	Uji 4	7-1517	823-1517	#1314#581#1094#969#1413#865#87#618#102#490#228#346#690#1034#1513#341
5	Uji 5	5-629	461-629	#195#601#332#210#172#553#533#593#328#627#484#272#18#165#191#589
6	Uji 6	5-1961	749-1961	#1145#366#273#754#808#1157#387#1847#501#740#1461#477#1646#743#502#171
7	Uji 7	5-1369	1037-1369	#1194#739#1016#131#1366#902#52#1364#1318#1363#682#131#682#46#989#651
8	Uji 8	7-407	103-407	#291#43#187#146#401#226#93#322#333#341#358#22#384#104#352#110
9	Uji 9	5-1961	749-1961	#450#501#893#1912#748#1190#243#117#757#510#796#1414#27#808#1277#1399
10	Uji 10	3-1189	747-1189	#1080#285#373#27#1033#926#331#1023#1059#400#15#208#271#791#986#381

DISCUSSIONS

Testing has been conducted on digital image data uji1, resulting in encrypted data enkrip1. Subsequently, enkrip1 data will undergo histogram analysis. Histogram analysis serves vital functions in data analysis by providing a visual representation of data distribution, enabling the identification of patterns and data characteristics, and aiding in the determination of data central tendencies and spreads. Moreover, histograms are utilized to detect outliers that may indicate unusual or potentially noteworthy data points. By employing histograms, data analysts can rapidly and efficiently comprehend the properties of the data under investigation, ultimately facilitating improved decision-making and more in-depth analysis.

Figure 2. Histogram Test enkrip 1



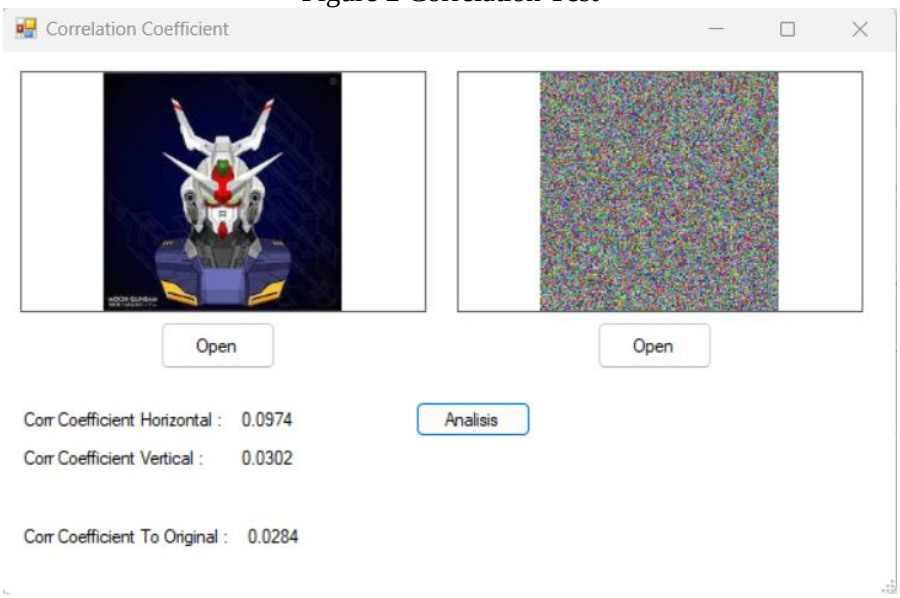
Correlation analysis in cryptography involves the use of statistical methods to identify relationships or correlations between data, encryption keys, or elements within a security system. This may encompass

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024
DOI : https://doi.org/10.33395/sinkron.v9i1.13175
e-ISSN : 2541-2019
p-ISSN : 2541-044X

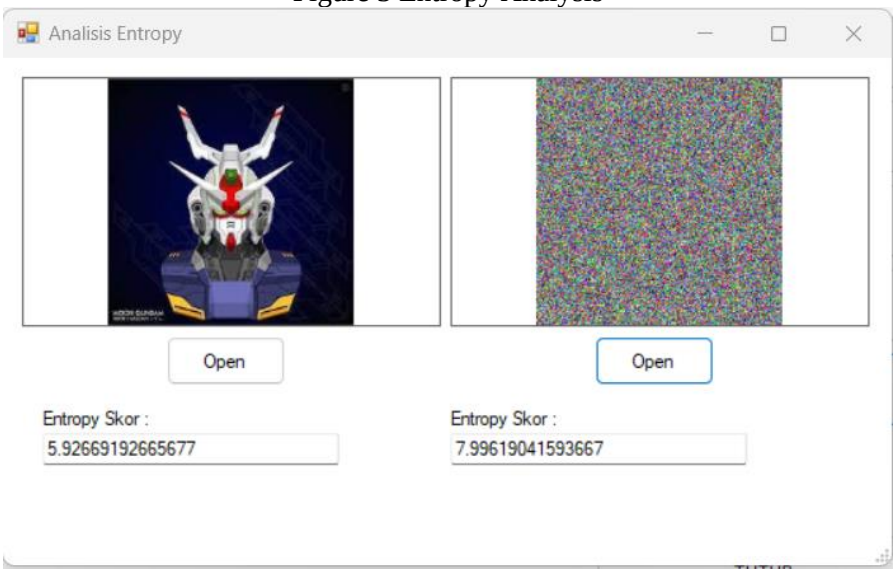
evaluating the correlation between encrypted data and plaintext, correlations in the use of encryption keys, as well as observations of time patterns that may indicate vulnerabilities or patterns within the system. Correlation analysis plays a crucial role in identifying potential security issues, attacks, or vulnerabilities in cryptographic protocols, allowing for improvements and strengthening the security level of the system.

Figure 2 Correlation Test



Entropy analysis in cryptography involves assessing the randomness and unpredictability of cryptographic data. It measures the level of uncertainty or disorder in a cryptographic system, such as the distribution of keys, ciphertext, or other cryptographic elements. High entropy signifies a higher degree of randomness and stronger security, while low entropy suggests predictability and potential vulnerabilities. Cryptographers use entropy analysis to ensure that cryptographic systems generate keys and ciphertext with sufficient randomness to withstand attacks and maintain confidentiality and integrity. It's a critical tool for evaluating and enhancing the security of cryptographic algorithms and protocols.

Figure 3 Entropy Analysis



*name of corresponding author

CONCLUSION

The research results have led to the development of a system capable of enhancing the security of digital images through the implementation of RSA, AES, and Arnold Cat Map. The encryption results were then subjected to analysis, including histogram analysis to evaluate the distribution of pixel values within the images, and correlation coefficient analysis to determine the level of correlation between pixels. Low correlation analysis values indicate that the security level of the encrypted images is good. It's important to note that correlation analysis is a statistical method commonly used to evaluate relationships between variables in a dataset, although it's not always directly applied in cryptography. Additionally, entropy analysis was conducted by comparing entropy values, which is a technique used to measure the level of uncertainty or randomness in data. In the context of cryptography, entropy analysis is useful for assessing how well encrypted data or confidential messages maintain a high level of entropy, which is a crucial indicator of cryptographic security. Therefore, this research successfully created a system that combines various analysis methods to enhance the security of digital images.

ACKNOWLEDGMENT

The author would like to thank the Research Institute and Publication Institute of the Muhammadiyah University of North Sumatra Medan Indonesia for supporting the dissemination of novice lecturer research (PDP) with number: 8/II.3-AU/UMSU- LP2M/C/2023

REFERENCES

Abdelfatah, R. I., 2019. Secure image transmission using chaotic-enhanced elliptic curve cryptography. *IEEE Access*, Volume 8, pp. 3875-3890.

Azanuddin, A., Yakub, S. & Prayudha, J., 2022. Implementasi Keamanan Citra Menggunakan Algoritma AES-128 Dengan Aplikasi Client-Server. *Jurasik (Jurnal Riset Sistem Informasi dan Teknik Informatika)*, 7(1), pp. 51-61.

Chidambaram, N., Raj, P., Thenmozhi, K. & Amirtharajan, R., 2020. Advanced framework for highly secure and cloud-based storage of colour images. IET Image Processing, 14(13), pp. 3143-3153.

Jiao, K. et al., 2020. Image encryption scheme based on a generalized Arnold map and RSA algorithm. Security and Communication Networks, Volume 2020, pp. 1-14.

Liang, H. et al., 2021. A novel asymmetric hyperchaotic image encryption scheme based on elliptic curve cryptography. Applied Sciences, 11(12), p. 5691.

Lin, R. & Li, S., 2021. An image encryption scheme based on lorenz hyperchaotic system and RSA algorithm. Security and Communication Networks, Volume 2021, pp. 1-18.

Man, Z. et al., 2021. Double image encryption algorithm based on neural network and chaos. Chaos, Solitons & Fractals, Volume 152, p. 111318.

Parida, P. et al., 2021. Image encryption and authentication with elliptic curve cryptography and multidimensional chaotic maps. IEEE Access, Volume 9, pp. 76191-76204.

Purnama, I. N., 2019. Implementasi Algoritma Enkripsi Rc5 Untuk Mengamankan Gambar Pada Perangkat Android. Jurnal Informatika dan Rekayasa Elektronik, 2(2), pp. 1-9.

Riadi, I., Fadlil, A. & Tsani, F. A., 2022. Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher. JISKA (Jurnal Informatika Sunan Kalijaga), 7(1), pp. 33-45.

Sujjada, A. & Juniar, E., 2021. Implementasi Algoritma Hill Cipher Untuk Proses Enkripsi Data Menggunakan Media Citra Digital. Jurnal RESTIKOM: Riset Teknik Informatika dan Komputer, 3(1), pp. 1-17.

*name of corresponding author