Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 1, January 2022
DOI : https://doi.org/10.33395/sinkron.v7i1.11256
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Implementation and Use of Base64 Algorithm in Video File Security

Muhammad Efendi[1)]*, Volvo Sihombing[2)], Sahat Parulian[3)]
[1)2)3)]Labuhanbatu University, North Sumatra, Indonesia
[1)] efendimuhammad02@gmail.com, [2)] volvolumbantoruan@gmail.com, [3)] sahatulb@gmail.com

Submitted: Jan 14, 2022 | **Accepted** : Feb 2, 2022 | **Published** : Feb 2, 2022

Abstract: Personal data is often the target of irresponsible people to misuse. The theft is carried out to profit from the person who has the data. In addition to the theft of work files, theft is also carried out on video files. The research stage conducted in this research is starting from problem analysis, application of methods, method analysis, design and implementation of applications. The theft of this file aims to find out what the contents of the video are. Someone has a private video recording that should not be known by others. Misuse of video files will be fatal for the owner of the video. Cryptographic techniques are needed in video security. The purpose of this research is to provide data by applying the base64 method in data security. On this basis the author will create a system that can encrypt and decrypt a video file so that the information contained in it becomes more secure. Caesar Cipher algorithm can help users in securing the video file. The Base64 algorithm can be used to change the ASCII 256 format to Base64 so that it is easy to send or store in a storage media. This algorithm will make the file structure simpler so that it can be displayed and saved. By applying the Base64 algorithm and Caesar Cipher on video files, the security and confidentiality of the files will be guaranteed.

Keywords: Security, Base64, Encrypt, Decrypt, ASCII

INTRODUCTION

Information security is very important at this time, how to secure data certainly requires techniques, one of which is the use of cryptography, the IDEA algorithm is one of the cryptographic algorithms that can be used to secure messages, and in this study the IDEA algorithm process is shown in stages to facilitate the development of the IDEA algorithm in various needs.(Simarmata et al., 2018)

Nowadays, information technology users who use computers as a medium are very increasing. Effective security of an information technology system is indispensable for daily activities, security and confidentiality issues are one of the important aspects of a message, data, or information. One of them is the image, the image is one of the important forms of multimedia. The image presents information visually and the information presented by an image is richer than that presented textually. One way to secure the image is the encryption process. Encryption is the process of converting plaintext into encrypted text.(Adi, Kitagawa, et al., 2021)

Technological advances that are growing rapidly encourage people to continue to create new breakthroughs in all fields of scientific discipline. The use of a new system that is more practical and faster in service and can provide convenience for users is a trend in itself in such a modern era.(Adi, Sihombing, et al., 2021)

In previous research was the goal by Phillip I Wilson and Mario Garcia. By adding some random bits of padding to each byte, one can ease the retention of statistics found in most messages. The one-way function will determine the right number of pads to remove indistinguishable message bits from padded random bits. This methodology moderately increases the size of the ciphertext, but significantly increases the security of the cipher(Irawan et al., 2020).

according to(Suhandinata et al., 2019) in the cited journal(Fricles Ariwisanto Sianturi, 2013) Random number generator or random number generator is an algorithm used to generate sequences of numbers as a result of calculations with a computer whose distribution is known so that the numbers appear randomly and are used continuously.

Experiments for all types can be carried out as well, before the EoF file process will be converted into a printablet using the Base64 method, the steganography process with the EoF technique can do it with the Base64 encoding text. Subsequent improvements Base64 and EoF methods can be combined with algorithmic compression, so that base64 encoding is compressed by the algorithm and then embedded into a file using EoF(Main & Siahaan, 2021)

* Corresponding Author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 1, January 2022
DOI : https://doi.org/10.33395/sinkron.v7i1.11256
e-ISSN : 2541-2019
p-ISSN : 2541-044X

LITERATURE REVIEW

Cryptography is the science of encryption techniques where data is scrambled using an encryption key into something that is difficult to read by someone who does not have a decryption key. Decryption uses the decryption key to get back the original data. The encryption process is carried out using an algorithm with several parameters.(Novianto & Setiawan, 2019)

Base64 transformation is one of the algorithms for encoding and decoding a data into ASCII format, which is based on the base number 64 or can be said to be one of the methods used to encode (encoding) binary data. according to(Novianto & Setiawan, 2019) quoted by Gunadhi, et al(Novianto & Setiawan, 2019)Base64 transformation is one of the algorithms for encoding and decoding data into ASCII format, which is based on the base 64 number or can be said to be one of the methods used to encode binary data. Base64 transformation cryptography is widely used in the Internet world as a media data format for sending data, this use is because the results of the base64 encode are plaintext, so this data will be much easier to send, compared to binary data formats. The base64 algorithm uses ASCII code and base64 index code in carrying out the encryption or decryption process. In encrypting the website URL, the base64 index code needs to be modified. The "+" symbol is modified to "-" and the "/" symbol becomes "_".

Encryption is an algorithm process that converts initial data into data in the form of strings at random, without encryption, information can be monitored by someone remotely. Base64 is not really encryption, but just an encoding standard.(Sitompul, 2019)

One of the important things in communication using a computer is to ensure the confidentiality of data. Information which is the result of processing from data, has a different value for each person. Often an information becomes very valuable, and not everyone is allowed to know it. However, there are always parties who try to find out information in inappropriate ways and even intend to destroy it.(Main & Siahaan, 2021)

METHOD

The research stage is how the research flow is carried out. The stages are carried out by grouping tasks into several phases, namely:

a. Literature study, in this thesis the author took from several sources such as journals and books.
b. Data collection, in this thesis the author collects data by searching and downloading videos with a maximum size of 30Mb.
c. System analysis, the problem raised in this thesis is how to secure a video file using the Base64 algorithm.
d. Analysis of the proposed system, the author will create a system that can be used to encrypt and decrypt video files so that they can be sent more securely.
e. Needs analysis, to make this system the author requires some hardware and software such as visual studio code software and a laptop.
f. The method, the algorithm method that the author uses in writing this thesis is the Base64 method.
g. System design, the author starts the process of designing the system using UML to see the process flow of the video file data that will be encrypted or decrypted.
h. Making the system, the author makes a system using the Microsoft Visual Basic.Net 2010 programming language.
i. Implementation, after making the system is complete, the author implements the system by trying and evaluating whether there are errors or are running correctly.

The stages above can be seen in Figure 1 below.

* Corresponding Author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 1, January 2022
DOI : https://doi.org/10.33395/sinkron.v7i1.11256
e-ISSN : 2541-2019
p-ISSN : 2541-044X

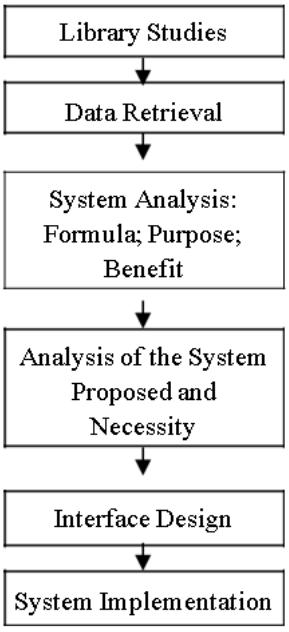

Fig. 1 Research Stage

RESULT

System analysis is the decomposition of an information system that is divided into component parts with the aim of identifying problems and evaluating problems that occur so that they are expected or can be proposed. Activity analysis is an information system with the aim of identifying and evaluating problems that will arise, which may occur so that they become the expected needs and technological developments. Currently, many of the video transmission processes are not encrypted so that the video file is easily viewed by anyone. With the insecurity of sending this video file, the file information can often be seen publicly by anyone so that the level of confidentiality of the information is not maintained(Fricles Ariwisanto Sianturi, 2018).

On this basis the author will create a system that can encrypt and decrypt a video file so that the information contained in it becomes more secure. Base64 encoding technique is actually simple, if there is one (string) bytes to be encoded to Base64 then the method is as follows:

Suppose we want to encode the text MAN

a. Change the letters to be encrypted into ASCII codes Text Content : M – A – N
   ASCII: 77 – 97 - 110
   The ASCII codes are converted into binary codes
b. Text Content : M – A – N
   ASCII: 77 – 97 – 110
   Bit Pattern: 01001101 – 01100001 - 01101110
c. Divide the binary code into only 6 numbers per block and the number is a multiple of 4 blocks.
d. If the binary number does not add up to 6 digits and 4 blocks, a binary code of 0 will be added so that it becomes 4 blocks.
e. The blocks are converted back into decimal code (data is read as index) Text Content : M – A – N
   ASCII: 77 – 97 – 110
   Bit Pattern: 010011 – 010110 – 000101 – 101110
   Index: 19 – 22 – 5 – 46
f. The results of the index code are converted to letters in the Text Content index: M – A – N
   ASCII: 77 – 97 – 110
   Bit Pattern: 010011 – 010110 – 000101 – 101110
   Index: 19 – 22 – 5 – 46
   Base64 Encoded: T – W – F – u
g. If the block value is an additional result (0) then the result of the index is '=' Text Content : M – "(Empty)" – "(Empty)"
   ASCII: 77 – "(Empty)" – "(Blank)"
   Bit Pattern: 010011 - 010000 – 000000 – 000000
   Index: 19 – 16 – (Blank) – (Blank)

* Corresponding Author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 1, January 2022
DOI : https://doi.org/10.33395/sinkron.v7i1.11256
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Base64 Encode: T – Q - = - =

Analysis of the Encryption System

The following is a use case diagram used in the video file encryption process:

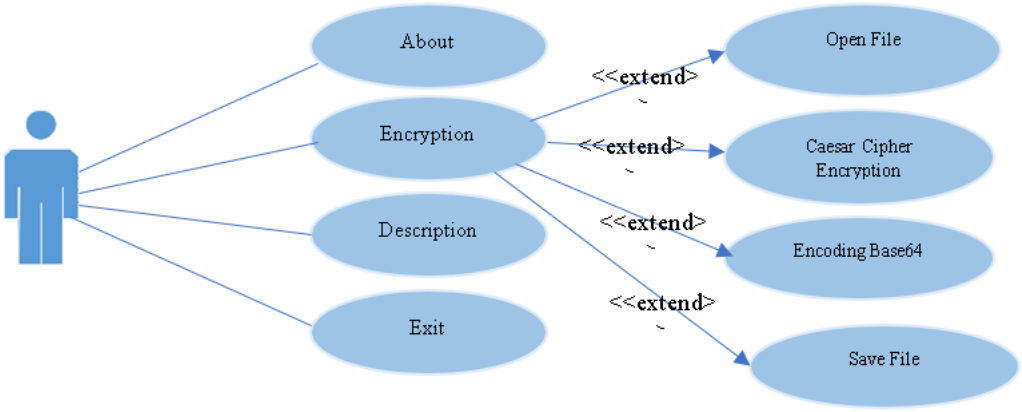

Fig.2 Use Case Diagram of the Encryption Process

System Analysis Description

The following is a use case diagram used in the video file decryption process:

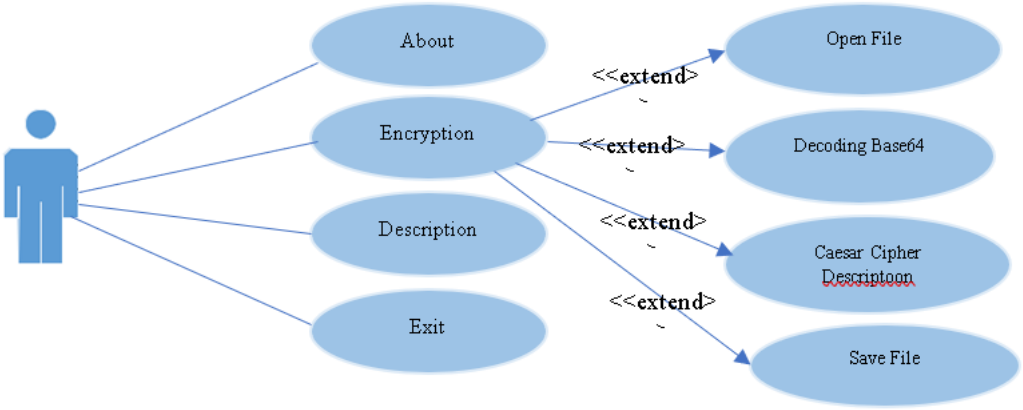

Fig.3 Use Case Process Diagram Description

DISCUSSIONS

From the results of calculations used with the Base64 algorithm obtained the result that with the calculation of base64 algorithm carried out obtained the results of encryption from video files used by decrypting video files so that the information contained in it becomes more secure. The Base64 encoding technique is actually simple, if there is one (string) byte to be encoded to Base64. In a simple encoding security system, you can use the base64 method to encrypt and description data or passwords. Based on the test data used, the quality of encryption and description increases by using the application created. This research is planned in the future will improve the encryption system and description with base64 algorithm not only on video files but will try with audio files in the process of encryption and description.

CONCLUSION

Based on the discussion of the previous chapters that have been done, some conclusions can be taken as follows:

1. The process of encrypting the video by selecting the video to be encrypted first. The video format that users can use is the *.mp4 format.
2. The application of the Base64 algorithm to secure messages on video files is done by creating a cryptographic application with the help of a programming language for the process of entering the system and selecting video files. To start encrypting, users can press the encryption button.
3. The message security system depends on the key used, in this study the key used in the string and the author added a hashing function that is part of the cryptographic library of the cryptographic class cryptography.

* Corresponding Author

REFERENCES

Adi, P. D. P., Kitagawa, A., Sihombing, V., Silaen, G. J., Mustamu, N. E., Siregar, V. M. M., Sianturi, F. A., & Purba, W. (2021). A Study of Programmable System on Chip (PSoC) Technology for Engineering Education. *Journal of Physics: Conference Series*, *1899*(1). https://doi.org/10.1088/1742-6596/1899/1/012163

Adi, P. D. P., Sihombing, V., Siregar, V. M. M., Yanris, G. J., Sianturi, F. A., Purba, W., Tamba, S. P., Simatupang, J., Arifuddin, R., Subairi, & Prasetya, D. A. (2021). A Performance Evaluation of ZigBee Mesh Communication on the Internet of Things (IoT). *3rd 2021 East Indonesia Conference on Computer and Information Technology, EIConCIT 2021*. https://doi.org/10.1109/EIConCIT50028.2021.9431875

Fricles Ariwisanto Sianturi. (2013). Perancangan Aplikasi Pengamanan Data Dengan Kriptografi Advanced Encryption Standard (AES). *Pelita Informatika Budi Darma*, *4*(1), 42–46. http://ejurnal.stmik-budidarma.ac.id/index.php/pelita/article/view/208

Fricles Ariwisanto Sianturi, M. S. (2018). ANALISA PENGARUH LOG TRANSAKSI PADA SISTEM KOMPUTER. *Mantik Penusa*, *2*(2), 67–70. http://e-jurnal.pelitanusantara.ac.id/index.php/mantik/article/view/422

Irawan, C., Winarno, A., Studi, P., Informasi, S., Komputer, F. I., & Nuswantoro, U. D. (2020). Kombinasi Algoritma Kriptogarafi Aes Dan Des Untuk Enkripsi. *Proceeding SENDIU*, 28–35.

Novianto, D., & Setiawan, Y. (2019). Aplikasi Pengamanan Informasi Menggunakan Metode Least Significant Bit (Lsb) dan Algoritma Kriptografi Advanced Encryption Standard (AES). *Jurnal Ilmiah Informatika Global*, *9*(2), 83–89. https://doi.org/10.36982/jig.v9i2.561

Simarmata, J., Limbong, T., Tambunan, A. R. S., Simanjuntak, M. P., Limbong, R., Purnomo, A., Kumalasari, R. D., Anam, F., Khoifulloh, K., Nisa, K., Aryni, Y., Purba, O. N., Sianturi, F. A., Tarigan, P., & Napitupulu, E. (2018). Multimedia of number recognition for early childhood using image object. *International Journal of Engineering and Technology(UAE)*, *7*(3.2 Special Issue 2).

Sitompul, J. N. (2019). *Implementasi Metode Kriptografi Advanced Encryption Standard (AES) untuk Proteksi Pesan Audio*. *4*(1), 37–45.

Suhandinata, S., Rizal, R. A., Wijaya, D. O., Warren, P., & Srinjiwi, S. (2019). Analisis Performa Kriptografi Hybrid Algoritma Blowfish Dan Algoritma Rsa. *JURTEKSI (Jurnal Teknologi Dan Sistem Informasi)*, *6*(1), 1–10. https://doi.org/10.33330/jurteksi.v6i1.395

Utama, A., & Siahaan, R. F. (2021). Penerapan Kriptografi untuk Pengamanan Data Transaksi Deposito pada Easy Tronik dengan Metode RC-5. *Jurnal Ilmu Komputer Dan Sistem …*, *3*(3), 29–39. http://ejournal.sisfokomtek.org/index.php/jikom/article/view/86

* Corresponding Author