Journal of Science, Technology, and Engineering (JSTE)
Vol. 2, No. 1, April 2022
P-ISSN: 2828-4747, E-ISSN: 2828-4658

Smart Blockchain Technology in Image Processing Between Challenges, Transformation and Digital-Based Learning Solutions

Muhammad Rifqi[1], Muhammad Isradi[2] , Otto Fajarianto[3]

[1]Faculty of Computer Science, Universitas Mercu Buana Jakarta, Indonesia
[2]Faculty of Engineering, Universitas Mercu Buana Jakarta, Indonesia
[3]Educational Technology Department, State University of Malang, Indonesia

m.rifqi@mercubuana.ac.id, m.isradi@mercubuana.ac.id, ofajarianto@gmail.com

ARTICLE INFO

Article history:
Received: Feb 27, 2022
Revised: March 28, 2022
Accepted: Apr 27, 2022

Keywords:
Information security, Data, Blockchain, Data transmission, DOS

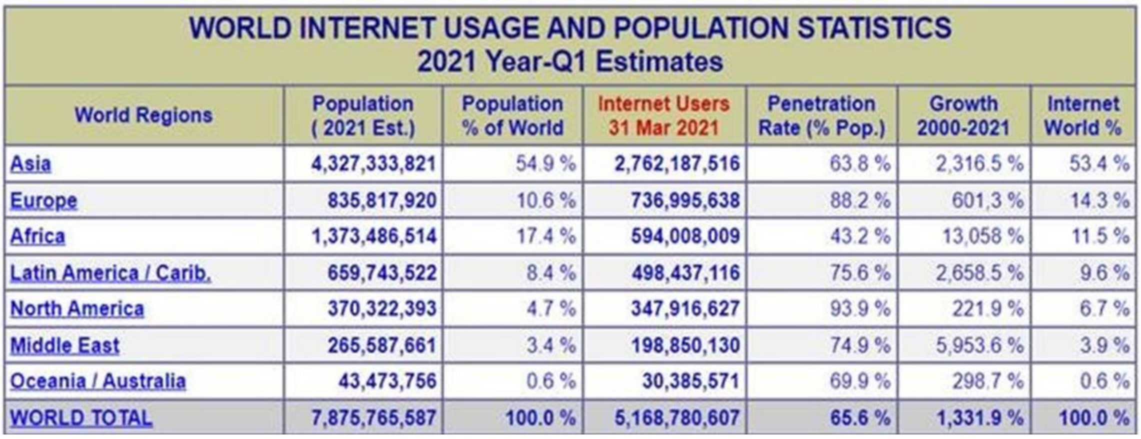
ABSTRACT

The rapid growth of cellular phone and internet users today, but not yet fully accompanied by the growing public awareness of protecting personal data, with the increase in the flow of data transmission packets via email or other media has a direct impact on increasing threats and theft of personal data. The higher the benefits of technology, the greater the risk that will be faced, meaning that there is no perfectly designed information technology that is free from vulnerability to data theft. With the inclusion of the concept of personal data as part of privacy, the protection of personal data becomes part of the protection of privacy. So the protection of personal data is part of the protection of human rights. Moreover, data has a high economic value. Based on these problems, the researchers conducted experiments with data collection techniques using literature studies and documentation. The problem-solving approach uses problem identification to find solutions. The presence of blockchain technology in the form of consensus in the form of a smart contract or chain code can make one solution in answering existing problems. The design method used is rapid application development by applying 5 design steps, namely business modeling, data modeling, process modeling, generation, and application testing. This software is built using the Disk Operating system (DOS) command. With this technique, it is hoped that the confidentiality of confidential information messages can be guaranteed.

1. Introduction

With the inclusion of the concept of personal data as part of privacy, the protection of personal data becomes part of the protection of privacy. The Universal Declaration of Human Rights, 1948, states that “no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honors and reputation. Everyone has the right to the protection of the law against such interference or attacks. Referring to this formulation, the protection of personal data is part of the protection of human rights. Moreover, data has a high economic value. Abu Bakar Munir (2015) reveals that "data has become the raw material of production and a new source of immense economic and social values". The sale of data in the case above is one simple proof from the economic side of the data. Naturally, supply arises because of demand.

The Internet has become an integral part of modern society. In cyberspace, through various information and communication technology devices, individuals and community groups interact, exchange ideas, and collaborate to carry out several life activities. The world which is the point of contact between the physical world and the world of abstraction is getting more and more visitors[1]. The latest statistics show that internet usage and population growth of its users have increased significantly from year to year as shown in the figure below[2].



WORLD INTERNET USAGE AND POPULATION STATISTICS
2021 Year-Q1 Estimates

World Regions	Population (2021 Est.)	Population % of World	Internet Users 31 Mar 2021	Penetration Rate (% Pop.)	Growth 2000-2021	Internet World %
Asia	4,327,333,821	54.9 %	2,762,187,516	63.8 %	2,316.5 %	53.4 %
Europe	835,817,920	10.6 %	736,995,638	88.2 %	601,3 %	14.3 %
Africa	1,373,486,514	17.4 %	594,008,009	43.2 %	13,058 %	11.5 %
Latin America / Carib.	659,743,522	8.4 %	498,437,116	75.6 %	2,658.5 %	9.6 %
North America	370,322,393	4.7 %	347,916,627	93.9 %	221.9 %	6.7 %
Middle East	265,587,661	3.4 %	198,850,130	74.9 %	5,953.6 %	3.9 %
Oceania / Australia	43,473,756	0.6 %	30,385,571	69.9 %	298.7 %	0.6 %
WORLD TOTAL	7,875,765,587	100.0 %	5,168,780,607	65.6 %	1,331.9 %	100.0 %

Fig 1. Statistics of World Internet Use in 2021 [2]

The conclusion that can be drawn from cases like the one above is that the higher the benefits of technology, the greater the risk that will be faced, meaning that there is no perfectly designed information technology that is free from vulnerability to data theft. One of the most important things in communication using computers and computer networks is to ensure the security of messages, data, or information so that they do not fall to unauthorized people [3], the process of exchanging / transmitting data has caused concern for many years. as data that can be attacked and manipulated by third parties.

The rise of internet media around the world, motivates people to hide secret messages in communicating securely through these media or by integrating some important user documents into image media.

Steganography and cryptography are two different techniques that maintain the confidentiality and integrity of data [6]. The purpose of steganography is to hide secret messages in digital media in a way that does not allow anyone to detect the existence of these secret messages [7]. The main purpose of steganography is to communicate securely with secret messages through images [8]. Steganography does not change the structure of the secret message but hides in the media so that the changes are not visible [8]. While cryptography protects messages from unauthorized individuals by changing their meaning [9].

The steganographic technique relies on the secrecy of the data coding system [3] once the coding system is known, the steganographic system can be known or tracked. Stenography technique allows hiding the fact that the message is being sent through digital media, such communication techniques are invisible between the sender and receiver [10], while cryptography obscures the integrity of the information so that it is not understood by anyone except the sender and receiver [6]. Cryptography is a mathematical study that has a relationship with aspects of information security such as data integrity, entity authenticity, and data authenticity [11].

In Steganography only the sender and receiver know the existence of the message, while in cryptography the existence of the encrypted message can be seen by the person [12]. For this reason, steganography can eliminate people's suspicions through hidden messages [13]. Steganography and cryptography differ in how they hide data but they are complementary techniques. Regardless of how strong the encryption algorithm is, if a secret message is found, it will be in the password [14] as well as how well the message is hidden in digital media there is a chance that the hidden message will be discovered by third parties.

By combining steganography and cryptography we can achieve better security by hiding the existence of encrypted messages [15]. Stego-generated objects can be transmitted without disclosing that confidential information is in progress. Furthermore, if an attacker tries to detect a message from a stego object, they must first decode the message from the digital media, and then he or she still needs a cryptographic algorithm to decrypt the message. Data hiding schemes in steganography in general are data or information that is hidden or stored in a container (cover) through certain steganographic algorithms (eg Least Bit)[1]. To increase data-level security, a lock can be assigned, so that not everyone can disclose the data stored in the file container (cover).

The final result of this data storage process is a stego file (stego text).

The characteristics of steganography according to Munir [16] are:

1. Embedded messages (hidden text): hidden messages;
2. Cover-object (cover text): the message used to hide the embedded message;
3. Steno-object (stegotext): messages that already contain embedded messages; and
4. Stthe ego-key: the key used to insert messages and extract messages from stegotext.

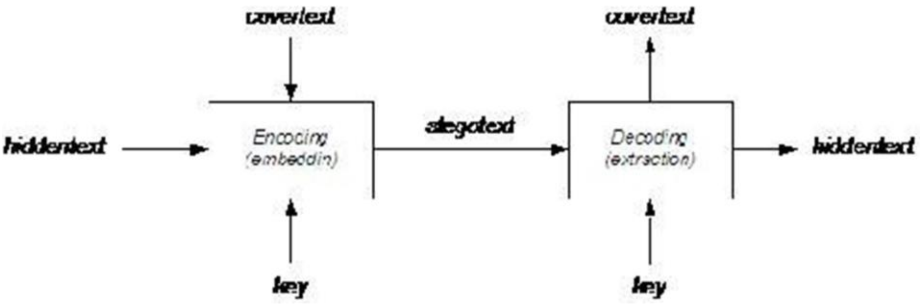


Fig 2. Embedding and Data Extraction Schematic [16].

In this study, the author uses a qualitative descriptive research method. In addition to using a qualitative descriptive method, this study also uses a simulation method to prove the effectiveness of the implementation design that has been made. The qualitative research method is used to examine the effectiveness of this DOS command compared to other applications, researchers in collecting data are emic, that is, based on the view of the data source, not the view of the researchers. In qualitative research, researchers interact with data sources. Although qualitative research does not make generalizations, it does not mean that the results of qualitative research cannot be applied elsewhere.

Generalization in qualitative research is called transferability in Indonesian it is called transferability. The point is that the results of qualitative research can be transferred or applied elsewhere when conditions elsewhere are not much different from the case that the researcher is reviewing. Likewise, the final result of this design is expected to be flexible to be applied anywhere as long as the infrastructure and needs are not much different. In this study, the authors used several techniques in data collection, namely: Librarian Engineering Bibliographic techniques focus on the study of various library sources. Observation Technique Researchers see firsthand the implementation of this system application.

Blockchain is a technology development with a digital system that makes data storage integrated. Blockchain technology solves this problem by ensuring transparency and maintaining the integrity of the stored data. Generally, it is believed that the data is genuine if there is a central server or a third party that maintains the data. It is very important to encrypt data if there is no trusted central system. Therefore, cryptography plays an important role in Blockchain. In Blockchain, cryptography is adapted to ensure data consistency, and maintain user privacy, and transaction information [19].

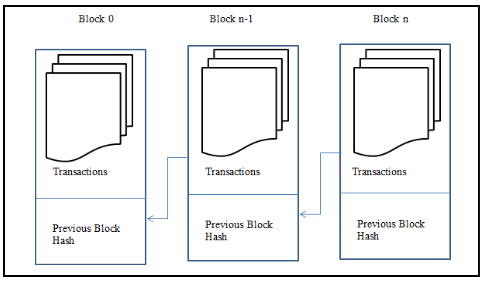


Fig 3. Simple Blockchain Architecture

Blockchain is a disruptive technology that has the potential to revolutionize the way everyone does business. The disturbance is not only in B2B, but B2C, and finally C2C[19].

In simple terms, blockchain technology can be described as a distributed database that records transactions that are shared with people who are members of a distributed database network [17]. Every transaction that occurs must always be by the agreed consensus in the distributed database network which ultimately makes the possibility of fraud to be minimized.

From the beginning of the emergence of blockchain until now, blockchain has undergone a significant evolution although literally, blockchain is a collection of interconnected blocks (chained) and contains information about transactions that occur. The key to blockchain technology is the ability to trace back within a network of distributed databases. In simple terms, the development of blockchain technology has reached 3 phases, namely blockchain 1.0 which initially emerged as a digital currency milestone, then developed into blockchain 2.0 as a form of further development in the digital economy, and the last is blockchain 3.0 as a form of evolution from the digital economy to the digital economy. in the form of associations or digital societies [17]. The last phase is blockchain 3.0 and is better known as the digital society phase. In this phase, those involved are no longer only from the business world, but from other fields that have started to take advantage of blockchain technology such as health, education, government, communication, science, and others[18]. In this phase, one of the things that stands out the most is the emergence of smart cities and IoT as new business platforms [19]. Blockchain other as a collection of blocks that are connected by recording the digital signature/hash of the previous block can be described as follows.

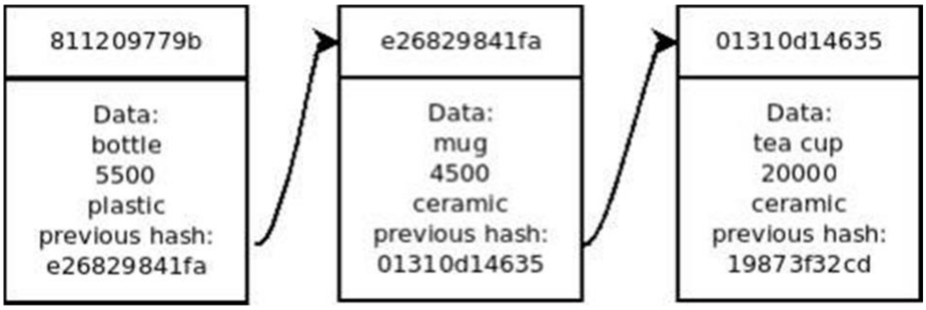


Fig 4. Ilustrasi dari blockchain

Blockchain Characteristics

1. Immutable

One of the characteristics of blockchain is that the data is immutable and immutable due to a decentralized system that causes changes to be made on all computers making it impossible to do so. Therefore, blockchain is not dependent on or controlled by a single person.

2. Can only be added (Append Only)

The blockchain system does not allow changes and deletions because this system can only add data so that the system is more secure.

3. Ledger

Ledger or Distributed Ledger Technology (DLT) is a digital system or protocol that makes decentralized-based data more secure because it is stored using cryptography. This system improves data security so that it is more difficult for unwanted parties to penetrate.

In this study, researchers took steps to identify problems, where researchers tried to study the existing problems which were often found that most of the insertion of documents and messages were not allowed or the same size as the size of the file size with the size of the image media used [1], but this is not the case with this problem, where the size of the image media is not a measure of the success of document/message insertion and does not affect the quality of the image media even though the size of the inserted file can be 3x and even exceed the size of it (image media), will be inserted can be in different formats and different sizes.

The many literature studies that researchers use as reference material in this study, it shows that the image media used must have a larger size, in addition to maintaining the integrity of the inserted document, it also has an impact on the image quality later [1].

Furthermore, the researchers collected data related to the research carried out by direct observation as well as by observing the data from these observations.

From the analysis of the various observations of the data, the researcher concludes that the insertion of one or several documents by executing the DOS command is quite effective and can trick third parties in an attempt to harm the sender to the recipient.

The DOS command syntax that we will examine is as follows:

```
copy /b file.0 + file.1 + file.2 newfile
```

To better understand the research workflow process, the researcher tried to put it in the form of a process diagram that the researcher did, as follows below, and a detailed explanation of the process by process.

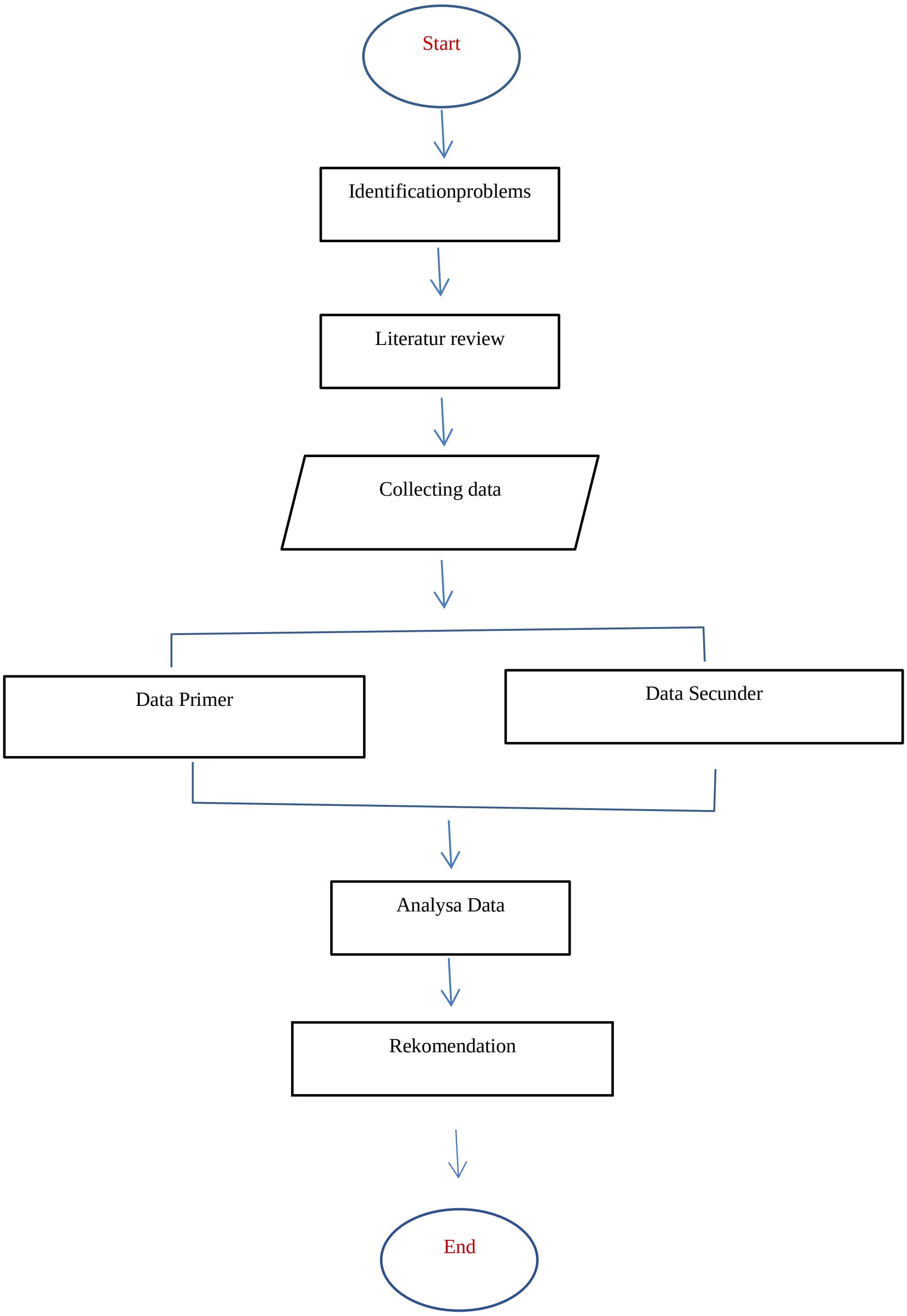


Fig 5. Research flow chart

As we know that the commands in DOS (disk operating system) are very numerous and have various functions, DOS is an operating system that uses a command-line interface used by computer users in the 1980s. For the facility to boot the computer and run several software applications, such as WS and Lotus. There are still many DOS functions that are used today, especially in solving some troubleshooting on computer hardware. Although it can also be done on a GUI-based operating system. The following are DOS functions:

- Organizing or controlling computer activities
- Manage memory
- Manage data input and output processes
- File management
- Management directory

Using DOS requires an understanding of the commands to run DOS. Of the many commands and their functions, we only discuss the COPY function that we often use so far, but we discuss only the Copy / b function or copying several documents into image media.

Figure 5. Copy command in DOS

2. Method

The data collected in this study is the quality of the availability of one data file/document or several that will be inserted into the image media.

To obtain the data is done in two ways or approaches, namely:

1. Prepare image media that is used as the target for document insertion
2. Prepare one document file or several document files with the same type of format or with different types of formats.

The DOS command syntax that we will examine is as follows:

```
copy /b file.0 + file.1 + file.2 newfile
```

Information :

Copy /b : copy files into image media (jpeg, png) with the binary concept

File.0 to file.n: document files to be merged

New file: file that is the result of a combination of merging from one or several files

examples:

```
copy /B Picture.png+Files.zip Picture-Merge.png
```

In the example above, to enter file.zip into the picture.png file, it becomes the new name of the result of the merger, namely picture-merge.png.

3. Results And Discussion

From the stages of data collection obtained data recapitulation is as follows:

A. The percentage of successful insertion of one or several documents with the same format but in different formats does not reduce the quality of the image in the slightest.

B. The percentage of new files generated is a combination of the size of the media files of images and documents accumulated to the size of the new target file.

C. Users are required to merge document files by compressing them first (rar) and the media used in bmp, jpeg, and png formats only.

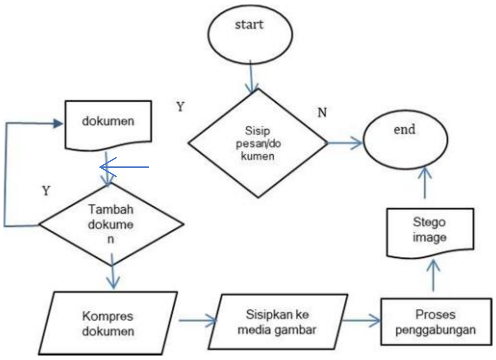
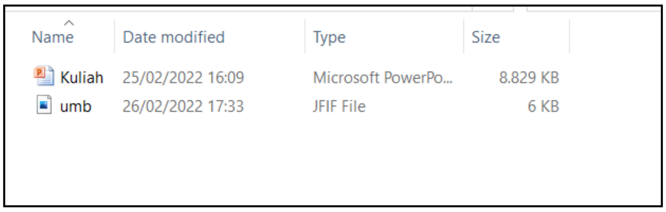


Fig 6. The process of securing messages/documents into pictures

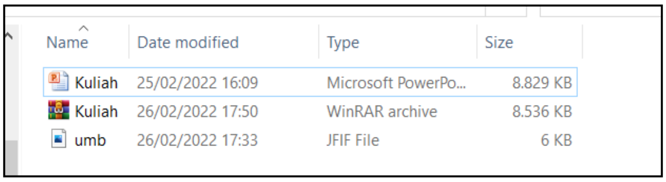
Test results



Name	Date modified	Type	Size
Kuliah	25/02/2022 16:09	Microsoft PowerPo...	8.829 KB
umb	26/02/2022 17:33	JFIF File	6 KB

Fig 7. Initial document insertion process

The researcher inserts a document called Lecture.ppt with a size of 8.8MB to an image media called Umb. jfif(jpeg) whose file size is only 6kb.The researcher's initial step is to compress files from ppt files to rar (winrar), researchers try to run the command copy /b umb.
Like the following picture below



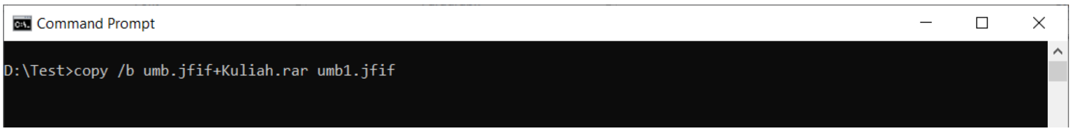
Name	Date modified	Type	Size
Kuliah	25/02/2022 16:09	Microsoft PowerPo...	8.829 KB
Kuliah	26/02/2022 17:50	WinRAR archive	8.536 KB
umb	26/02/2022 17:33	JFIF File	6 KB

Fig 8. The initial process of document compression

After compression and insertion into the image media, it becomes the name of the new image media by collaboratively increasing the document size with the image media size (total). For more details, see the following table:

Nama Media	Size	File Dokumen	Size	Hasil
Umb. jfif	6kb	Kuliah.rar	8.536Mb	8.541Mb

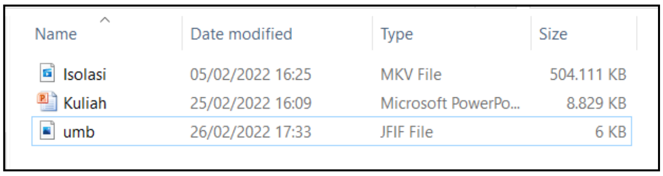
Fig 9. The process of compressing 1 document into a media image



```
D:\Test>copy /b umb.jfif+Kuliah.rar umb1.jfif
```

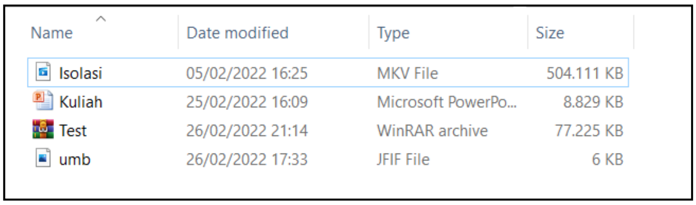
Fig 10. The process of merging documents with image media

How to open a new file that is the result of merging between documents and media images to prove whether the results of merging documents with image media, then we can prove it by using WinRAR to extract it, then after extracting it will get 2 files, the first file is for image media and the other file is a documentation file that has been extracted which is exactly the same as the documentation file as before.
To prove whether the image media can be inserted documentation files that have the format and or the size of the size many times the size can be accommodated by the image media will be explained as follows



Name	Date modified	Type	Size
Isolasi	05/02/2022 16:25	MKV File	504.111 KB
Kuliah	25/02/2022 16:09	Microsoft PowerPo...	8.829 KB
umb	26/02/2022 17:33	JFIF File	6 KB

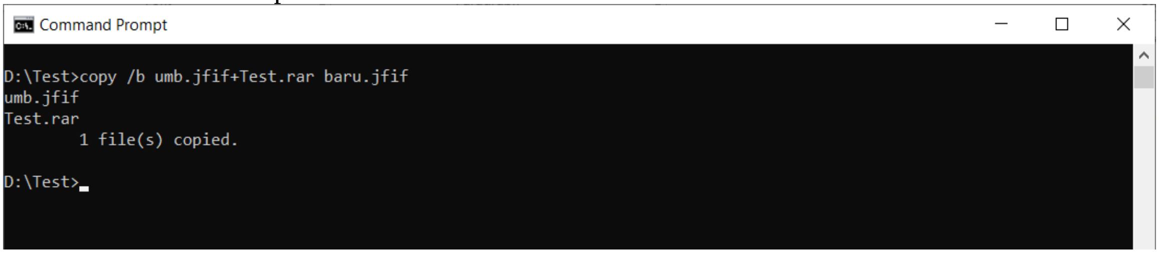
Fig 11 The process of inserting an image with 2 more documents of different formats



Name	Date modified	Type	Size
Isolasi	05/02/2022 16:25	MKV File	504.111 KB
Kuliah	25/02/2022 16:09	Microsoft PowerPo...	8.829 KB
Test	26/02/2022 21:14	WinRAR archive	77.225 KB
umb	26/02/2022 17:33	JFIF File	6 KB

Fig 12 The initial process of inserting an image with 2 more documents of different formats

Then we do the insertion process

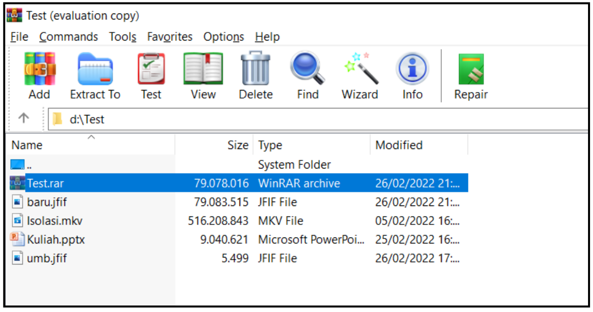


```
D:\Test>copy /b umb.jfif+Test.rar baru.jfif
umb.jfif
Test.rar
        1 file(s) copied.

D:\Test>_
```

Fig 13 The process of inserting an image with 2 more documents of different formats

Now we try to prove whether the file we insert can run as expected.



Name	Size	Type	Modified
..		System Folder	
Test.rar	79.078.016	WinRAR archive	26/02/2022 21:...
baru.jfif	79.083.515	JFIF File	26/02/2022 21:...
Isolasi.mkv	516.208.843	MKV File	05/02/2022 16:...
Kuliah.pptx	9.040.621	Microsoft PowerPoi...	25/02/2022 16:...
umb.jfif	5.499	JFIF File	26/02/2022 17:...

Fig 14 Extraction process

It will be found that the result of the merged file is the accumulation of the total size of the image media file by merging the two files.

After extraction, you will get two files that are the same as before the previous compression.

Nama Media	Size	File Dokumen	Size	Hasil
Umb. jfif	6kb	test.rar (video + ppt)	77.225Mb	77.230Mb

Fig 15 The process of compressing 2 different documents into image media

From the extraction results, it is found that there is no change in the quality of the image on the image media that is inserted by the document whose size exceeds the size of the media.

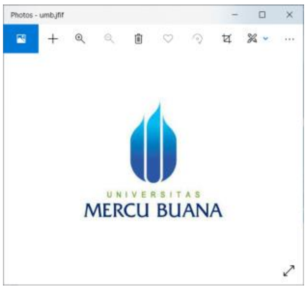


Fig 16 Quality of image media before document insertion

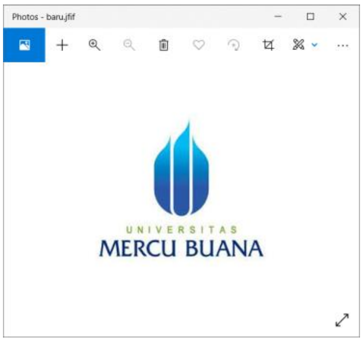


Fig 17 Image media quality after document insertion

In the two images above, it can be concluded that the small size of the image media file does not affect the image quality in the slightest, even though the saved document file exceeds many times the size of the existing image media, unlike in steganography theory, which inserts a message that must be smaller than the image media file. existing [1].

4. Conclusions

The use of just the DOS command with copy / b helps users in encrypting data into image media. Using the DOS command with copy /b, the size of the media image that is the target even though its size is smaller than the size of the inserted file does not affect the image quality. The secret document to be inserted into the image consists of two or more files. The image quality of the existing secret file is the same as the original image quality.

REFERENCES

Rifqi, Muhammad, Combining Steganography And Cryptograph Techniques For Data Security (Case Study In PT XYZ), International Research Journal of Computer Science (IRJCS), Vol.5, Issue 01 January 2018

Internet Usage Statistic, www.internetworldstats.com/stats.html, accessed May 13, 2013.

M. Conway, Code Wars: Steganography, Signals Intelligence, and Terrorism, Knowledge Technology & Policy , Volume 16, Number 2, pp. 45-62, Springer, 2003. 4. RJ Anderson and FAP Petitcolas, On The Limits of Steganography , IEEE Journal of Selected Areas in Communications, 16 (4), pp.474-481, May 1998, ISSN 0733-8716.

C. Hosmer, Discovering Hidden Evidence , Taylor & Francis Group, Journal of Digital Forensic Practice, Vol. No.1, pp.47-56, 2006.

AJ Raphael and V. Sundaram, Cryptography and Steganography - A Survey , Int. J. Comp. Tech. Appl., Vol 2 (3), pp. 626-630, ISSN: 2229-6093.

SA Laskar and K. Hemachandran, An Analysis of Steganography and Steganalysis Techniques, Assam University Journal of Science and Technology, Vol.9, No. II, pp.83- 103, January, 2012, ISSN: 0975-2773.

NF Johnson and S. Jajodia, Exploring Steganography: Seeing the Unseen, IEEE, Computer, vol. 31, no. 2, pp. 26- 34, Feb. 1998.

Menezes. J. Alfred, Paul C. Van Oorschot, Scott A. Vanstone, Applied Cryptography, 1996.

E. Walia, P. Jain and Navdeep, An Analysis of LSB & DCT based Steganography , Global Journal of Computer Science and Technology, Vol. 10 Issue 1 (Ver 1.0), pp 4-8, April , 2010 .

BB Zaidan, AA Zaidan, AK Al-Frajat and HA Jalab, On the Differences between Hiding Information and Cryptography Techniques: An Overview, Journal of Applied Sciences, Vol.10, No.15, pp.1650-1655, 2010.

RS Ramesh, G. Athithan and K. Thiruvengadam, An Automated Approach to Solve Simple Substitution Ciphers , Taylor & Francis, Cryptologia, Vol. XVII, No. 2, pp. 202- 218, April, 1993.

WF Friedman, Cryptology, Encyclopedia Britannica, Vol. 6, pp. 844-851, 1967. 14. Atul Kahate, Cryptography and Network Security, 2nd Edition, Tata McGraw-Hill, 2008.

Fauzan, N.I (2018). Teknologi blockchain dan Peranannya dalam Era Digital. Jurnal BJB University.

AJ Raphael and V. Sundaram, Cryptography and Steganography - A Survey , Int. J. Comp. Tech. Appl., Vol 2 (3), pp. 626-630, ISSN: 2229-6093.

Munir, Rinaldi, 2009, Steganography and Watermarking, http://www.informatika.org/~ rinaldi / Cryptography / Steganography% 20and% 20Watermarking.pdf, accessed on 26 May 2013.

Untung Rahardja, Qurotul Aini, 2020, Penerapan Teknologi Blockchain Sebagai Media Pengamanan Proses Transaksi E-Commerce CESS (Journal of Computer Engineering System and Science) Vol. 5 No. 1 Januari 2020, ISSN :2502-7131

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. Ieee Access, 4, 2292- 2303.

Sutandi, S. (2018). Pengaruh BigData dan Teknologi Blockchain terhadap Model Business Model Canvas. Jurnal Logistik Indonesia, 2(1), 9-20.