CHAPTER 2
LITERATURE REVIEW

2.1 Theoretical Framework

The theoretical framework used in this research is a conceptual basis for compiling research. The theoretical framework of this research is in the form of Grand Theory (Cyber Defense), Middle Theory (Cryptography, Steganography, Compression Method and Classified Document) and Applied Theory (Triple Data Encryption Standard, Least Significant Bit and Zipped Information Package) which will be explained further in this chapter.

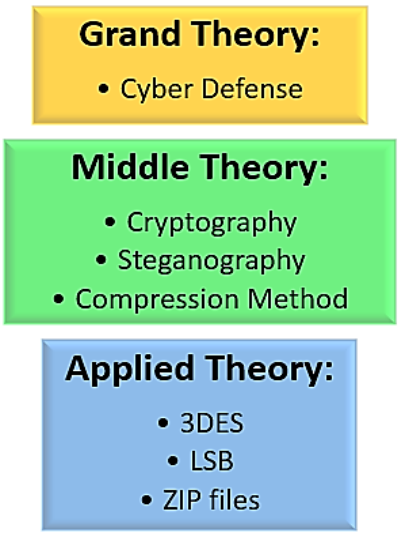


Chart 2. 1 Theoretical Framework

Source: Processed by the Researcher (2024)

2.1.1 Cyber Defense

Defense science is a branch of discipline studied to maintain and develop the sustainability of the country in terms of resilience and security in order to achieve state defense on a national and international scale. In a problem that occurs in a country, defense science can be used as a guide to find a solution. This is because defense science contains scientific principles (Virgiawan, 2018):

a. Multidisciplinary: Defense science can be integrated with other scientific clumps such as religion, humanities, social, natural, formal and applied which aim to realize national defense (UU RI No 12 Tahun 2012)
b. Interdisciplinary: Defense science can use the perspective approach of each expert based on the theory put forward by considering the causal factors of national defense.
c. Transdisciplinary: Defense science can be developed beyond the boundaries of more complex knowledge so as to create new, more creative and innovative ideas for national defense.

Because of that principle of defense science, the study of national resilience was created. According to Dictionary of Indonesian Languange or KBBI (2023), national resilience is the strength, ability, endurance and tenacity that is the goal of a nation to face challenges, threats, obstacles, and disturbances that come from outside or from within, which directly or indirectly endanger the survival of the nation and state. National resilience is formed by the properties and guided by the principles based on Pancasila, The 1945 Constitution and The Archipelago Concept (Safarudin, 2022), namely:

a. Properties of national resilience:
    1) Independence. National resilience must believe in the strength and ability of the country in the face of global developments.
    2) Dynamic. Can rise and fall depending on the situation and conditions of the country, for that national resilience must be oriented to the future to be able to improve national resilience.
    3) Single. Integrated towards the unity and integrity of the nation in the aspects of social life, nation and state.
    4) Authority. National resilience should be able to increase the authority of the nation in the eyes of other nations.

5) Cooperation. National resilience is not an individualism or egoism, but a form of cooperation to strengthen each other

b. Principles of national resilience:

1) Welfare and security. This principle is a very basic need for every individual and group. With the achievement of this principle, national resilience becomes a good benchmark in national life.

2) Inward-looking and outward-looking. Inward-looking is interpreted as an effort to improve the quality of national life independently, resiliently and resiliently. Meanwhile, outward watchfulness is defined as a form of anticipation in facing the foreign strategic environment that enters the country.

3) Kinship. The principle of kinship is a form of cooperation, mutual cooperation, togetherness, tolerance in the midst of diverse differences by maintaining justice without causing disputes.

4) Comprehensive integral. Integration in the aspects of life in society, nation and state is realized in the form of unity and integrity so as to create balance and harmony.

Apart from these properties and principles, Dwi Sulisworo et al (2012) also argued concept of national resilience contains astagatra elements consisting of Trigatra (Geography, Demography and Natural Resources) and Pancagatra (Ideology, Politics, Economy, Social - Culture and Defense - Security) aspects that are interconnected as follows:

a. Geography. An overview of the geographical location of land and water, the area and its parameters, up to the regional borders.

b. Demography. The dominant elements of population quantity and quality.

c. Natural Resources. Potential and types of natural resources (flora, fauna, minerals, soil, atmosphere, aerospace, natural energy, water and sea) that are renewable, non-renewable and permanent.

d. Ideology. Pancasila is an ideology that originates from the ideals of the ancestors and is implemented as a system of philosophy of the Indonesian Nation.

e. Politics. The political system in Indonesia is guided by the principles, directions, efforts and policies of the state both domestically and abroad. Indonesia adheres to a free - active political system in the foreign policy system.

f. Economy. This gatra explains how the condition of the national economy affects the economic growth of the Indonesian people.

g. Social - Culture. There are 4 important elements for the social life of society, namely: structure, supervision, relations and social standards. Meanwhile, culture is interpreted as the result of creation, taste and creativity to foster ideas in running life.

h. Defense - Security. All forms of efforts to protect the interests of the nation and state are carried out through the Universal People's Security Defense System (Sishankamrata).

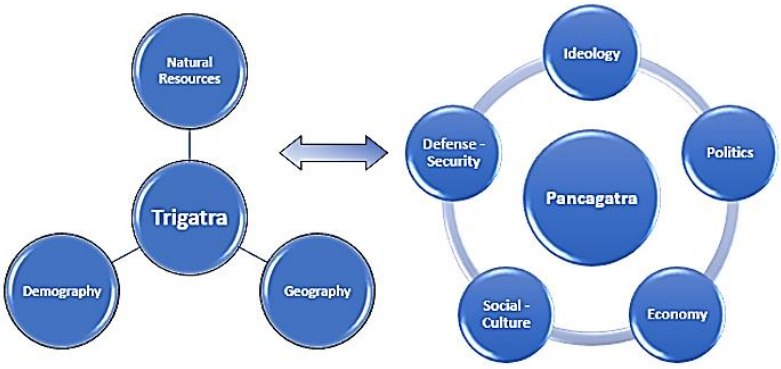


Chart 2. 2 Astagatra Aspects of National Resilience

Source: Sulisworo (2012)

Defense - security in the astagatra aspect is defined as 2 (two) different things. According to Mardhani et al (2020), security means freedom from danger, fear and threats from the perspective of traditional security and non-traditional security. Meanwhile, defense is defined as the main instrument of a country to create national security. Since August 18th, 2000, the institutions that carry out defense and security tasks have been separated, namely the Indonesian National Military (TNI) acts as a state instrument in national defense, while the Indonesian National Police (Polri) is a state instrument in maintaining state security (Tap MPR RI Nomor VI/MPR/2000 Tahun 2000 concerning Separation of TNI and Polri). Nevertheless, these two institutions must work together in the field of defense and security for the realization of national resilience (Iswardani et al, 2015)

In defense and security, Suhirwan (2023) summarizes the opinions of several experts on defense theory, including:

a. Absolute Defense Theory: State must prepare defense to the maximum without regard to cost or consequences (Smoke, 1975).
b. Total Defense Theory: National defense must involve all citizens and national resources to strengthen defense (Hilsman, 1967).
c. Integrated Defense Theory: National defense should integrate various aspects of defense, including military, economic, political, and social, to create a stronger and more effective defense (Nathan, 1983).
d. Cooperative Defense Theory: National defense should involve colaboration with other countries to strengthen security and stability at regional and global levels (Clarke, 1999).
e. Self Defense Theory: National defense must allow the use of force to protect itself from external threats that threaten national security and integrity (Posner and Vermeule, 2007).

From several expert opinions on defense theory, it can be concluded that a country needs a national defense system.

National defense is all efforts to defend the sovereignty of the state, the territorial integrity of the Unitary State of the Republic of Indonesia (NKRI), and the safety of the entire nation from threats and disturbances to the integrity of the nation and state (UU RI No 3 Tahun 2002). National defense is organized by the Indonesian National Army as the main component. In addition to the main component, there are also citizens, natural resources, artificial resources, and national infrastructure facilities which are part of the reserve component to strengthen the main component. Then there are also supporting components that can directly or indirectly support the other two components. This means that efforts in national defense are not only the duties and responsibilities of the main component, but are an obligation for all elements in the Republic of Indonesia.

Chart 2. 3 Components of National Defense

Source: Undang – Undang RI No 3 Tahun 2002

National defense is currently used to deal with the dynamics of threats that will occur at any time. The threat dynamics in question are actual threats (military, non-military and hybrid threats that are developing today and will continue to develop from year to year both from within and outside the country) and potential threats (threats that have not yet occurred, but can occur at any time to become actual threats). Currently, The Ministry of Defense (2020) has formulated the strategic objectives of national defense which consist of:

a. The maintenance of the sovereignty and territorial integrity of the Republic of Indonesia and the protection of the safety of the entire nation from all forms of threats.
b. The establishment of an integrated and modern Universal People's Defense and Security System (Sishankamrata).
c. The realization of National Resource Management (PSDN), for National Defense.
d. Implementation of defense area management.

One of the policy targets to build an integrated and modern Sishankamrata is through increasing cyber technology capabilities that are able to protect the country by following the change of new forms of warfare. In other words, it is necessary to develop cyber defense as a form of state defense efforts.

Cyber defense is defined as an effort to overcome cyber attacks that cause interference with the implementation of national defense. (Permenhan RI No 82 Tahun 2014). Cyber defense needs can be improved through development in the aspects of: policy, institutions, technology and supporting infrastructure and human resources. Cyber defense is organized through phases:

a. Attack Prevention. This stage focuses on prevention activities that have the potential to cause cyber threats and attacks.
b. Information Security Monitoring. At this stage it is necessary to monitor the entry and exit of information that can be indicated to disrupt the stability of data security.
c. Attack Analysis. If an indication of an attack is found at the previous stage, then immediately take action to analyze the attack.
d. Defense. From the results of attacks that are considered dangerous or harmless, the next stage must still carry out the defense stage to secure vital data that is at risk of causing adverse effects if leaked.

e. Counterattack. After the data can be secured, then counterattack to reduce the enemy's concentration on attacking, so that they change the focus of the attack to defend their device.

f. Information Security Enhancement. During the counterattack, we can take the opportunity to improve data security.

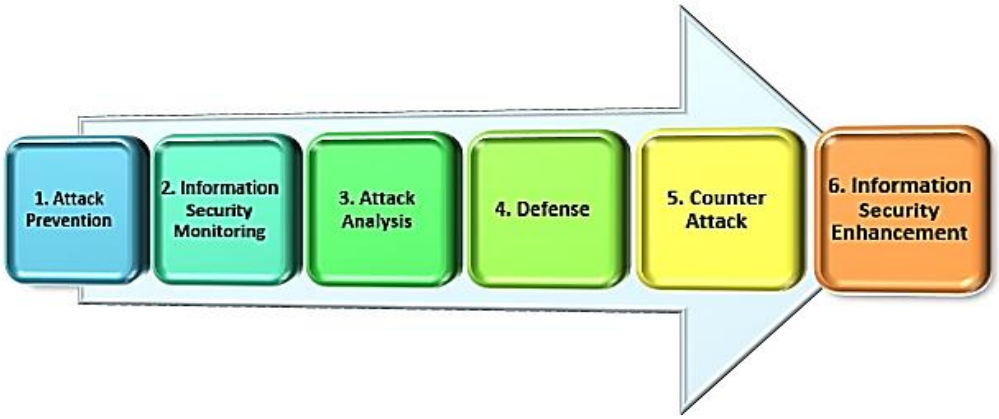


Chart 2. 4 Cyber Defense Phase

Source: Permenhan RI No 82 Tahun 2014

The implementation of cyber defense is carried out as an effort to protect Critical information infrastructure. Critical Information Infrastructure (IIV) is an electronic system that utilizes information technology and/or operational technology, either stand-alone or interdependent with other electronic systems in supporting strategic sectors, which in the event of disruption, damage, and/or destruction of the infrastructure in question has a serious impact on public interests, public services, defense and security, or the national economy (Perpres No 82 Tahun 2022). IIV protection is implemented in sectors divided into: government administration, energy and mineral resources, transportation, finance, health, information and communication technology, food, defense and other sectors determined by the President. To realize IIV protection through cyber incident management efforts in each sector, it is necessary to establish a Cyber Incident Response Team at the national, sectoral and organizational levels.

The Indonesian Cybersecurity Landscape (BSSN, 2022) reveals several recapitulated events that threaten IIV protection in Indonesia during 2022, including:

a. Cyber threat intelligence as many as 399 cases of suspected cyber incidents. This activity attacks through several incidents in several sectors, such as: data leakage and vulnerability, malicious activity, national security issues, malware, phishing, profiling, ransomware, web defacement and Advanced Persistent Threat (APT).
b. Darknet exposure exposed on the darknet with a total of 27,956 data coming from 427 agencies. This condition increases potential for exploitation by irresponsible parties for their interests and results in losses to the exploited agencies.
c. Data breaches that were successfully detected were 311 suspected incidents that impacted government stakeholders as many as 245 incidents.

Table 2. 1 Recapitulation of Cyber Incidents in 2022

Stakeholder	Cyber Threat Intelligence	Darknet Exposure	Data Breach
Government Administration	120	21.302	98
Energy and Mineral Resources	20	143	13
ICT	25	406	20
Defense	20	503	12
Transportation	13	17	14
Finance	14	375	13
Health	11	28	11
Food	3	14	3
Other	59	5.168	61
Total	**399**	**27.956**	**245**

Source: Badan Siber dan Sandi Negara (2022)

The results of the 2022 Cyber Incident Recapitulation, led to predictions of the types of cyber threats that might occur in the following year (BSSN, 2022), including:

a. Ransomware. One type of computer virus where the attacker encrypts data and asks for a ransom from the victim as a substitute for the virus decryption key.

b. Data Breach. A cyber offense that occurs when confidential information is leaked to parties that should not receive it and through unauthorized means.
c. Advanced Persistent Threat (APT). A complex, targeted and sustained attack that aims to hack the target network or system access within a certain time.
d. Phishing. A technique used to obtain personal information such as name, address, ID card, health, financial and other information by posing as a trusted entity through a website.
e. Cryptojacking. A form of cybercrime where a person uses their device to increase the value of cryptocurrency without the owner's permission.
f. Distributed Denial of Service (DDoS). An attack that reduces the number of internet users able to connect to a website or network so that the victim experiences access failure.
g. Remote Desktop Protocol (RDP). A protocol that allows users to access their computers remotely. If protocol is not properly secured, then RDP can be an entry point for cyber attacks.
h. Social Engineering. A psychological manipulation trick where attackers utilize human interaction on social media to obtain confidential information by tricking their victims.
i. Web Defacement. An attack carried out on the appearance of the victim's website to replace or destroy the information.

To minimize cyber threats that will occur in the following year in Indonesia, it is necessary to have a national cyber security strategy and cyber crisis management as follows:

a. National cyber security strategy is implemented in the focus areas of governance, risk management, preparedness and resilience, strengthening IIV protection, national cryptographic independence, increasing capacity and quality capabilities, cyber security policy and international cooperation.

b. Cyber crisis management that is organized before, during and after a cyber crisis.

Furthermore, this research will discuss cryptography which is one of the efforts of the national cyber security strategy.

2.1.2 Cryptography

Cryptography is a branch of mathematics that studies the field of information security with the goals of confidentiality, integrity, authentication, and non-repudiation (Menezes et al, 1997). Meanwhile, cryptanalysis is a scientific method used to solve information security problems. Both are part of cryptology, which is the study of encryption techniques in securing messages and analyzing message security vulnerabilities. The definition of cryptography has explained its purpose, namely:

a. Confidentiality: It refers to the protection of message information so that it can only be accessed by authorized parties so that confidential messages cannot be accessed or understood by unauthorized parties.
b. Integrity: It refers to the authenticity and integrity of the message where the message should not be modified or manipulated by unauthorized parties.
c. Authentication: It involves verifying the identity of the sender or receiver involved in a communication in order to ensure that the entities involved are the right parties.
d. Non repudiation: It is a guarantee that the message sent comes from the actual sender, so that the sender cannot deny that the message came from him.

A cryptosystem is a set of rules, algorithmic systems and techniques used in cryptography. There are several important components that must be understood in a cryptosystem, among others:

a. Plain message: Plain message is a message that has not gone through the encryption process or a message that has gone through the decryption process. Plain messages can be read and interpreted according to the grammar used.
b. Cipher message: Cipher message is the opposite of plain message. Cipher messages cannot be read and interpreted according to the grammar used.
c. Encrypt: An algorithm used to encode a plain message into a cipher message using a key agreed upon by the sender and receiver.
d. Decrypt: An algorithm to break the cipher used in the cipher message using the key agreed upon by the sender and receiver.
e. Key: The key is a code agreed upon by the sender and receiver to encrypt the plain message and decrypt the cipher message. The key for decryption is the inverse of the key for encryption.
f. Sender: The original party that sends message to receiver.
g. Receiver: A Party that receives message from sender.
h. Interceptor: A party other than the sender and receiver that tries to find out the message content of the communication between the sender and receiver.

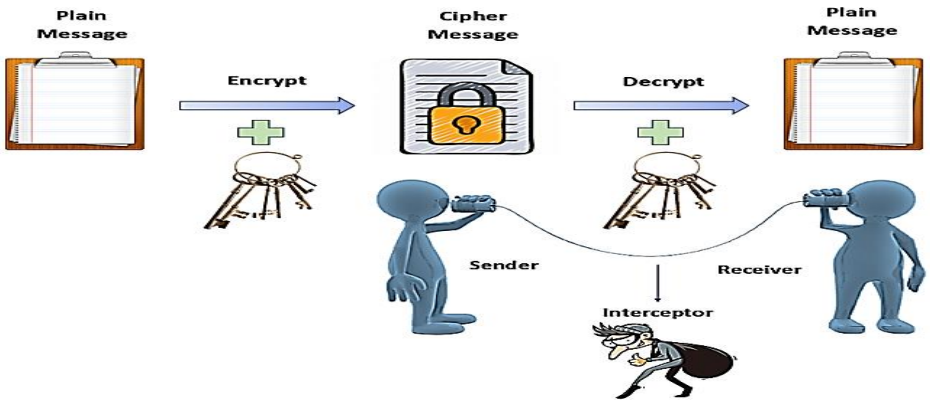


Chart 2. 5 Cryptosystem Flowchart

Source: Processed by the Researcher (2024)

Based on how keys are used in cryptography, there are two different types of keys: symmetric keys and asymmetric keys. Symmetric keys use the same type of key in the encryption and decryption process. Asymmetric keys, on the other hand, use a pair of different keys, a public key and a private key. The private key is only known by the sender and receiver. On the other hand, the public key can be known by anyone other than the sender and receiver. Apart from keys, there are 2 types of algorithms based on their encryption methods, namely stream ciphers and block ciphers. Stream ciphers emphasize the encryption process in sections that flow continuously. Then there are block ciphers that encrypt plain messages through the same blocks.

2.1.3 Steganography

Steganography is one of the subsciences in cryptology that examines techniques for masking secret messages. The important components in steganography are not much different from cryptography, but there are several components and definitions used in stegosystems, including:

a. Secret message. The original message that will be inserted in the encoding process or it can also mean the original message that is deciphered in the decoding process. Thus, secret message before encoding = secret message after decoding.
b. Cover object. The object used as the initial media to insert the secret message using the stego-key.
c. Stego – key. The steganography key used to run the encoding and decoding process.
d. Stego object. Steganography object which is the result of encoding or object that will be used before the decoding process. The stego object contains the secret message and cover object so that the secret message will be hidden.
e. Encoding. The process of disguising the secret message into the cover object into a stego object.

f. Decoding. The opposite of the encoding process.

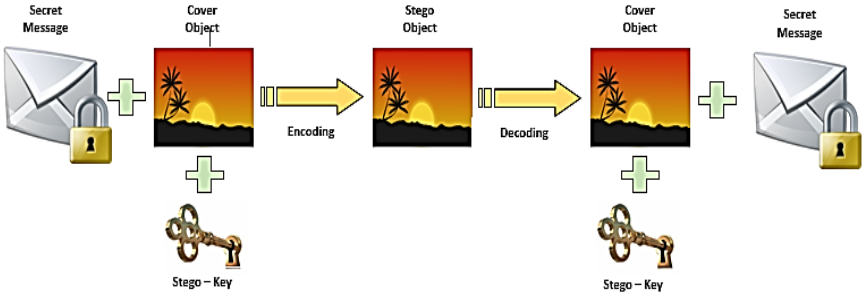


Chart 2. 6 Stegosystem Flowchart

Source: Processed by the Researcher (2024)

According to Munir (2023), good steganography is steganography that meets the criteria:

a. Impeceptible. The interceptor is unaware of the secret message communicated between the sender and receiver.
b. Fidelity. There is no significant change between the cover message that has been inserted with the secret message and the previous one in the conversion process.
c. Recovery. The cover message that has been inserted with a secret message must be able to be converted back to the cover message before the secret message was inserted.
d. Capacity. Capacity of the cover message should be very large so that it can contain a large number of secret messages.

Currently, there are two types of steganography methods based on the domain of operation: spatial domain methods. This type of method uses direct modification of the byte value of the cover object where the value represents the pixel color, intensity or amplitude. An example of this method is Least Significant Bit (LSB). Furthermore, there are transform domain methods. This method modifies the result of the transformation of a message into another message extension (for example, the transformation of a stego message with an image extension and then modified into a signal extension). An example that uses this method is Spread Spectrum.

Steganography is not a new method that aims to replace the role of cryptography. Steganography will actually be a complement in securing information information. This research will apply the use of Least Significant Bit (LSB) Steganography which will be described in the next section of this chapter.

2.1.4 Compression Method

Data has a unit of measurement in bytes and ranges from 1 Kilobyte (KB) = 10^3 bytes; 1 Megabyte (MB) = 10^6 bytes; 1 Gigabyte = 10^9 bytes; 1 Terabyte (TB) = 10^{12} bytes; and 1 Petabyte (PB) = 10^{15} bytes. The data is stored in a storage area. The large size of the data is a problem for every data operator who will perform storage. Therefore, a data compression method is needed to minimize the data capacity. Nan Zhang (2005) classifies compression algorithms into four classes:

a. Basic techniques. Compression methods are simple and do not require any statistical analysis or special understanding of the data to be compressed. They usually rely on recognizing simple patterns in the data. Example: Run-Length Encoding (RLE) is an example of a basic technique that replaces a series of repeated characters with character itself followed by the number of times the character appears.

b. Statistical methods. Statistical methods use statistical analysis on data to identify and model patterns of character occurrence. They attempt to reduce redundancy in the data by replacing frequently occurring characters with shorter codes. Example: Huffman Coding is an example of a statistical method often used in text and other data compression. It replaces frequently occurring characters with shorter codes based on their probability of occurrence.

c. Dictionary methods. Dictionary methods use dictionaries that map a set of raw data to more efficient codes. They are effective

in compressing data with high repetition. Example: Lempel-Ziv-Welch (LZW) is an example of a dictionary method used in compression formats like GIF. It builds a dictionary based on a string of input data and replaces similar strings with shorter dictionary codes.

d. Transform based methods. Transform based methods transform raw data into different representations, often based on mathematical transformations, to identify and reduce redundancies in the data. Example: The Discrete Cosine Transform (DCT) is an example of a transform-based method used in JPEG image compression. It transforms the spatial domain into the frequency domain and allows encoding data with higher precision at lower frequency components.

Data compression techniques can be used to minimize the size of various types of data such as text, documents, images, video, audio and so on. Storer (1992) states that there are several basic theorems in the use of these techniques, among others:

a. Theorem 1. If we use integers from the range $[0, N)$ and use the high precision algorithm for scaling up the sub range, the code length is provably bounded by $\frac{4}{N \ln 2}$ bits per input symbol more than the ideal code length for the file.

b. Theorem 2. The use of a special end – of – file symbol when coding a file of length t using integers from the range $[0, N)$ results in additional code length of less than $\frac{8t}{N \ln 2 + \lg N + 7}$ bits.

c. Theorem 3. For all input files, the adaptive code with initial 1 – weights gives exactly the same code length as the semi – adaptive decrementing code in which the input model is encoded based on the assumption that all symbol distributions are equally likely.

d. Theorem 4. Let L be the compressed length of a file. Then we have

$$B\left(\left(\sum_{m=1}^{b} H_m\right) + H_b - H_0\right) - t\frac{k}{B} < L < B\left(\left(\sum_{m=1}^{b} H_m\right) + H_b - H_0\right) + t\left(\frac{k}{B}\lg\left(\frac{B}{k_{min}}\right) + O\left(\frac{k^2}{B^2}\right)\right) \quad (2.\ 1)$$

Where $H_0 = \lg n$ is the entropy of the initial model, H_m is the (weighted) entropy implied by the scaling model's probability distribution at the end of block m, k is the number of different alphabet symbols that appear in the file and k_{min} is the smallest number of different symbols that occur in any block.

e. Theorem 5. Rounding counts up to next higher integer increases code length for the file by no more than $\frac{n}{2B}$ bits per input symbol.

There are lossless compression and lossy compression algorithms. Lossless compression is the removal of redundancies in data while retaining ability to restore data to its original form. Although lossy compression involves discarding "unimportant" information from the data, which cannot then be recovered. Syahrul (2011) suggest a data compression model consisting of reduction of data redundancy (to reduce file size, remove unnecessary data repetitions), reduction in entropy (Reduce the level of complexity in data to allow for better compression) and entropy coding (A coding method that takes advantage of data's statistical probability characteristics to produce a more space-efficient representation).

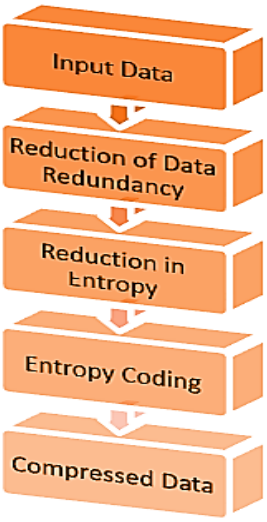


Chart 2. 7 Data Compression Model

Source: Syahrul (2011)

To evaluate the successful performance of loseless and lossly algorithms in data compression techniques, there are 3 ways of measurement mentioned by Himawan et al (2014), namely:

a. Compression Ratio (CR). Comparison of the difference between the size after compression (s_a) to size before compression (s_b).

$$CF = \frac{s_a}{s_b} \tag{2. 2}$$

b. Compression Factor (CF). The opposite of the ratio in compression ratio.

$$CF = \frac{s_b}{s_a} \tag{2. 3}$$

c. Saving Percentage (SP). The percentage of size shrinkage before compression becomes the size after compression.

$$SP = \frac{s_b - s_a}{s_b}.100\% \tag{2. 4}$$

2.1.5 Classified Documents

Electronic information is a collection of electronic data that is not limited to writing, sound, images, maps, designs, photographs, Electronic Data Interchange (EDI), electronic mail, telegram, telex, telecopy or the like that has been processed and has meaning or can be understood by people who are able to understand it. Meanwhile, electronic transactions are legal actions carried out using computers, computer networks, and / or other electronic media. (UU RI No 11 Tahun 2008). The electronic transaction processes documents containing information using an electronic system. In electronic transaction activities, electronic certification is needed to provide legal force. This electronic certification can minimize any individuals or groups who will act against the rule of law. In the Electronic Information and Transaction (ITE) system, there are several prohibited acts, such as violations of decency, gambling, defamation, threatening, false news, issues of Ethnicity, Religion, Race and Intergroup (SARA) and others.

In electronic transaction activities, electronic information about the personal data of individuals and groups is very important. Personal data is defined as data about an identified or identifiable natural person individually or in combination with other information either directly or indirectly through electronic or non-electronic systems. Because personal data is something that is very important, it needs protection. Personal data protection has been regulated in UU RI No 27 Tahun 2022 concerning Personal Data Protection. This personal data protection is based on the principles of: protection, legal certainty, public interest, expediency, caution, balance, responsibility and confidentiality. Personal data according to its type is specific personal data and general personal data. Some examples of specific personal data that are very vital, including health information, biometrics, genetics, criminal records, child data, financial and other data in accordance with the provisions of laws and regulations. If specific personal data from members of an agency is disseminated in the public media, it will increase the risk of data misuse by irresponsible parties. For this reason, information security

can be carried out on the personal data. One of the recommended efforts in securing personal data information is through the implementation of coding.

Information security is all efforts, activities and actions to realize information security, while coding is defined as an activity in the field of data/information security carried out by applying concepts, theories, art and crypto science along with other supporting sciences systematically, methodologically and consistently and related to the ethics of the cipher profession (Peraturan BSSN No 10 Tahun 2019). Information security in coding at least includes the security of information technology resources, access control, data and information, human resources, networks, email, data centers and/or communications. Data regarding information security is contained in classified documents.

Classified documents are defined as a record of activities or events in the form of archives that have been classified by the government, organizations or institutions that manage them with the aim of protecting the information contained in them from unauthorized access. The classification of documents is divided into 4 levels from the highest, namely:

a. Top Secret: If known by unauthorized parties, it can endanger the sovereignty of the state, the territorial integrity of the Unitary State of the Republic of Indonesia (NKRI) and the safety of the nation.
b. Secret: If known by unauthorized parties, it may result in disruption of the function of state administration, national resources, public order, including macroeconomic impacts.
c. Limited: If known by unauthorized parties, it may result in disruption of the implementation of the functions and duties of government agencies, such as significant financial losses.

d. Ordinary: If disclosed to the public, it does not have any impact on state security.

In the Peraturan Kepala ANRI No 17 Tahun 2011, it is emphasized that there are internal and external parties who have the right to access classified documents as listed in the Table 2.2.

Table 2. 2 Classified Document Access Users

No	Class Lvl	Internal		External		
		Determinant Policy	Executive Policy	Supervisor	Public	Law Enforcement
1	Top Secret	√	-	√	-	√
2	Secret	√	-	√	-	√
3	Limited	√	-	√	-	√
4	Ordinary	√	√	√	√	√

Source: Processed by the Researcher (2024)

In order to implement the protection of classified documents, it is necessary to guide the rules for managing and protecting classified information by paying attention to the principles of security, integrity, availability, speed and accuracy as well as effectiveness and efficiency. The management of classified information is carried out through the stages of: making, labeling, sending and storing classified documents. In addition, the protection of classified documents is also carried out against: physical, administrative and logic protection.

2.1.6 Data Encryption Standard (DES)

Data Encryption Standard (DES) is one of the information security standards in the Federal Information Processing Standard (FIPS) established by the National Institute of Standards and Technology (NIST) in 1977. The DES cryptographic algorithm is used in all sectors of agencies in the United States government. Based on the type of key and cipher, DES is a type of cryptographic algorithm that uses symmetric keys and block ciphers. The advantages of symmetric keys include:

a. Has a high data processing speed.

b. The key used is relatively short.

c. Can be used to generate keys.

d. Since the symmetric key is simple, it can be extended to build stronger algorithms.

e. Widely applied in the information security industry.

The DES encryption algorithm globally consists of 3 main parts, namely: Initial Permutation (IP), Enciphering and Inverse Initial Permutation (IP^{-1}). At first glance, this process seems simple, but if we break it down, we will find a repetitive and complex process as shown in the DES encryption algorithm flowchart.

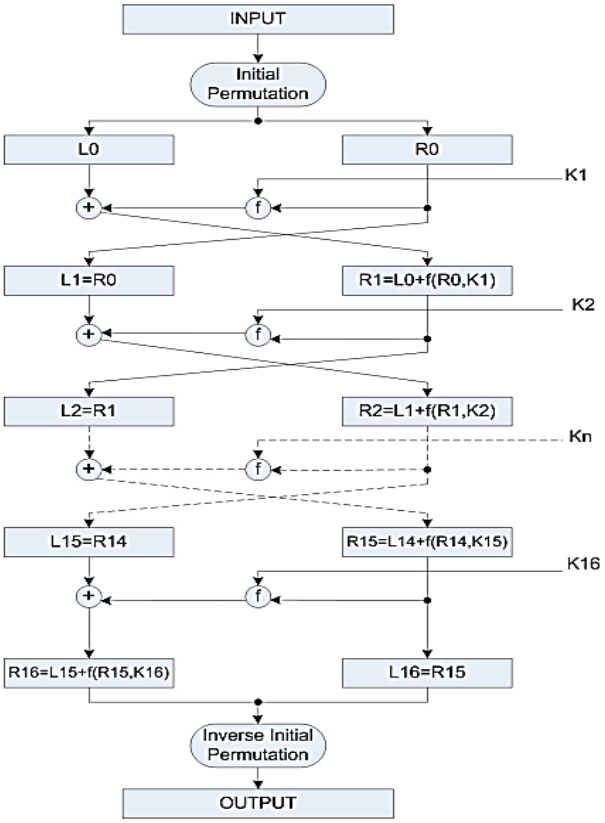


Chart 2. 8 DES Encryption Flowchart

Source: Kromodimoeljo (2009)

Next, we will explain the DES encryption algorithm starting from the IP, Enchipering and IP-1 stages as follows:

a. Initial Permutation (IP)

Before starting DES enciphering, the Initial Permutation (IP) step will be performed as follows:

1) Determine the plain message P to be encrypted.
   a) If $P < 64$ bit then padding is done
   b) If $P > 64$ bit then split every 64 bits.
2) Determine the key K of 64 bits.
3) Convert P and K into binary characters (See ASCII Table), so that it is obtained:

$$P = (p_1\ p_2\ p_3\ \dots\ p_{64}), \forall p_i \in Binary\ Char \quad (2.5)$$

$$K = (k_1\ k_2\ k_3\ \dots\ k_{64}), \forall k_i \in Binary\ Char \quad (2.6)$$

4) Sort the interger number 1 to 64 into an 8 x 8 table as in the Table 2.3.

Table 2. 3 Initial Bit

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Source: Processed by the Researcher (2024)

5) Modify the Initial Bit Table into an Initial Permutation Table.

Table 2. 4 Initial Permutation (IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Source: Processed by the Researcher (2024)

6) Perform the permutation in Equation (2.5) on Table 2.4 to obtain Table 2.5.

Table 2. 5 Initial Permutation (IP) Result

p_{58}	p_{50}	p_{42}	p_{34}	p_{26}	p_{18}	p_{10}	p_2
p_{60}	p_{52}	p_{44}	p_{36}	p_{28}	p_{20}	p_{12}	p_4
p_{62}	p_{54}	p_{46}	p_{38}	p_{30}	p_{22}	p_{14}	p_6
p_{64}	p_{56}	p_{48}	p_{40}	p_{32}	p_{24}	p_{16}	p_8
p_{57}	p_{49}	p_{41}	p_{33}	p_{25}	p_{17}	p_9	p_1
p_{59}	p_{51}	p_{43}	p_{35}	p_{27}	p_{19}	p_{11}	p_3
p_{61}	p_{53}	p_{45}	p_{37}	p_{29}	p_{21}	p_{13}	p_5
p_{63}	p_{55}	p_{47}	p_{39}	p_{31}	p_{23}	p_{15}	p_7

Source: Processed by the Researcher (2024)

7) Split Table 2.5 into L_0 and R_0 in order from top left to bottom right thus obtain Equation (2.7) and (2.8).

$$L_0 = \begin{matrix} p_{58}p_{50}p_{42}p_{34}p_{26}p_{18}p_{10}p_2 & p_{60}p_{52}p_{44}p_{36}p_{28}p_{20}p_{12}p_4 \\ p_{62}p_{54}p_{46}p_{38}p_{30}p_{22}p_{14}p_6 & p_{64}p_{56}p_{48}p_{40}p_{32}p_{24}p_{16}p_8 \end{matrix} \quad (2.7)$$

$$R_0 = \begin{matrix} p_{57}p_{49}p_{41}p_{33}p_{25}p_{17}p_9p_1 & p_{59}p_{51}p_{43}p_{35}p_{27}p_{19}p_{11}p_3 \\ p_{61}p_{53}p_{45}p_{37}p_{29}p_{21}p_{13}p_5 & p_{63}p_{55}p_{47}p_{39}p_{31}p_{23}p_{15}p_7 \end{matrix} \quad (2.8)$$

8) Reorder Table 2.3 without 8th Column to get Table 2.6.

Table 2. 6 Initial Bit Without Column 8

1	2	3	4	5	6	7
9	10	11	12	13	14	15
17	18	19	20	21	22	23
25	26	27	28	29	30	31
33	34	35	36	37	38	39
41	42	43	44	45	46	47
49	50	51	52	53	54	55
57	58	59	60	61	62	63

Source: Processed by the Researcher (2024)

9) From the Table 2.6, organize it into a Permuted Choice - 1 (PC-1) Table 2.7 as follows:

Table 2. 7 Permuted Choice - 1 (PC-1)

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Source: Processed by the Researcher (2024)

10) Perform the permutation in Equation (2.6) on Table 2.7 to obtain:

Table 2. 8 Permuted Choice - 1 (PC-1) Result

k_{57}	k_{49}	k_{41}	k_{33}	k_{25}	k_{17}	k_9
k_1	k_{58}	k_{50}	k_{42}	k_{34}	k_{26}	k_{18}
k_{10}	k_2	k_{59}	k_{51}	k_{43}	k_{35}	k_{27}
k_{19}	k_{11}	k_3	k_{60}	k_{52}	k_{44}	k_{36}
k_{63}	k_{55}	k_{47}	k_{39}	k_{31}	k_{23}	k_{15}
k_7	k_{62}	k_{54}	k_{46}	k_{38}	k_{30}	k_{22}
k_{14}	k_6	k_{61}	k_{53}	k_{45}	k_{37}	k_{29}
k_{21}	k_{13}	k_5	k_{28}	k_{20}	k_{12}	k_4

Source: Processed by the Researcher (2024)

11) Break Table 2.8 into C_0 and D_0 in order from top left to bottom right, thus obtain:

$$C_0 = \begin{matrix} k_{57}k_{49}k_{41}k_{33}k_{25}k_{17}k_9 & k_1k_{58}k_{50}k_{42}k_{34}k_{26}k_{18} \\ k_{10}k_2k_{59}k_{51}k_{43}k_{35}k_{27} & k_{19}k_{11}k_3k_{60}k_{52}k_{44}k_{36} \end{matrix} \quad (2.\ 9)$$

$$D_0 = \begin{matrix} k_{63}k_{55}k_{47}k_{39}k_{31}k_{23}k_{15} & k_7k_{62}k_{54}k_{46}k_{38}k_{30}k_{22} \\ k_{14}k_6k_{61}k_{53}k_{45}k_{37}k_{29} & k_{21}k_{13}k_5k_{28}k_{20}k_{12}k_4 \end{matrix} \quad (2.\ 10)$$

12) Use C_{n-1} and D_{n-1} to arrange 16 blocks.

$$C_n \; and \; D_n, \forall n \in [1{,}16], n \in N \quad (2.\ 11)$$

13) Use Table 2.9 to perform the left shift.

Table 2. 9 Wrapping

i-th Iteration	Number of left shift	i-th Iteration	Number of left shift
1	1	9	1
2	1	10	2
3	2	11	2
4	2	12	2
5	2	13	2
6	2	14	2
7	2	15	2
8	2	16	1

Source: Processed by the Researcher (2024)

14) For every i[th] iteration, perform left shift as many times as the number in Table 2.9, starting from Equation (2.9) and (2.10) up to Equation (2.11) so as to obtain the following results:

$$C_1 = \begin{matrix} k_{49}k_{41}k_{33}k_{25}k_{17}k_9k_1 & k_{58}k_{50}k_{42}k_{34}k_{26}k_{18}k_{10} \\ k_2k_{59}k_{51}k_{43}k_{35}k_{27}k_{19} & k_{11}k_3k_{60}k_{52}k_{44}k_{36}k_{57} \end{matrix}$$

$$D_1 = \begin{matrix} k_{55}k_{47}k_{39}k_{31}k_{23}k_{15}k_7 & k_{62}k_{54}k_{46}k_{38}k_{30}k_{22}k_{14} \\ k_6k_{61}k_{53}k_{45}k_{37}k_{29}k_{21} & k_{13}k_5k_{28}k_{20}k_{12}k_4k_{63} \end{matrix}$$

$$C_2 = \begin{matrix} k_{41}k_{33}k_{25}k_{17}k_9k_1k_{58} & k_{50}k_{42}k_{34}k_{26}k_{18}k_{10}k_2 \\ k_{59}k_{51}k_{43}k_{35}k_{27}k_{19}k_{11} & k_3k_{60}k_{52}k_{44}k_{36}k_{57}k_{49} \end{matrix}$$

$$D_2 = \begin{matrix} k_{47}k_{39}k_{31}k_{23}k_{15}k_7k_{62} & k_{54}k_{46}k_{38}k_{30}k_{22}k_{14}k_6 \\ k_{61}k_{53}k_{45}k_{37}k_{29}k_{21}k_{13} & k_5k_{28}k_{20}k_{12}k_4k_{63}k_{55} \end{matrix}$$

$$\vdots$$

$$C_{16} = \begin{matrix} k_{57}k_{49}k_{41}k_{33}k_{25}k_{17}k_9 & k_1k_{58}k_{50}k_{42}k_{34}k_{26}k_{18} \\ k_{10}k_2k_{59}k_{51}k_{43}k_{35}k_{27} & k_{19}k_{11}k_3k_{60}k_{52}k_{44}k_{36} \end{matrix}$$

$$D_{16} = \begin{matrix} k_{63}k_{55}k_{47}k_{39}k_{31}k_{23}k_{15} & k_7k_{62}k_{54}k_{46}k_{38}k_{30}k_{22} \\ k_{14}k_6k_{61}k_{53}k_{45}k_{37}k_{29} & k_{21}k_{13}k_5k_{28}k_{20}k_{12}k_4 \end{matrix}$$

(2. 12)

15) Use Table 2.10 to perform the next permutation.

Table 2. 10 Permuted Choice - 2 (PC-2)

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Source: Processed by the Researcher (2024)

16) Perform the permutation in Equation (2.12) on Table 2.10 to obtain:

$$K_i, \forall i \in [1,16], i \in N \tag{2. 13}$$

and arrange it into 8 blocks with 6 bits per block as follows:

$$K_1 = \begin{matrix} k_{10}k_{51}k_{34}k_{60}k_{49}k_{17}\ k_{33}k_{57}k_2k_9k_{19}k_{42}\ k_3k_{35}k_{26}k_{25}k_{44}k_{58}\ k_{59}k_1k_{36}k_{27}k_{18}k_{41} \\ k_{22}k_{28}k_{39}k_{54}k_{37}k_4\ k_{47}k_{30}k_5k_{53}k_{23}k_{29}\ k_{61}k_{21}k_{30}k_{63}k_{15}k_{20}\ k_{45}k_{14}k_{13}k_{62}k_{55}k_{31} \end{matrix}$$

$$\vdots$$

$$K_{16} = \begin{matrix} k_{18}k_{59}k_{42}k_3k_{57}k_{25}\ k_{41}k_{36}k_{10}k_{17}k_{27}k_{50}\ k_{11}k_{43}k_{34}k_{33}k_{52}k_1\ k_2k_9k_{44}k_{35}k_{26}k_{49} \\ k_{30}k_5k_{47}k_{62}k_{45}k_{12}\ k_{55}k_{38}k_{13}k_{61}k_{31}k_{37}\ k_6k_{29}k_{46}k_4k_{23}k_{28}\ k_{53}k_{22}k_{21}k_7k_{63}k_{39} \end{matrix}$$

(2. 14)

b. Enciphering.

From the previous step, we have Equation (2.7), (2.8) and (2.14).

Next, the enciphering step is performed:

1) Arrange The Expansion Table as follows:

Table 2. 11 Expansion

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Source: Processed by the Researcher (2024)

2) Use Table 2.11 to expand R_{i-1} using the formula:

$$E(R_{i-1}), \forall i \in [1;16], i \in N$$

(2. 15)

thus obtained:

$$E(R_0) = \begin{matrix} p_7p_{57}p_{49}p_{41}p_{33}p_{25}\ p_{33}p_{25}p_{17}p_9p_1p_{59} & | p_1p_{59}p_{51}p_{43}p_{35}p_{27}\ p_{35}p_{27}p_{19}p_{11}p_3p_{61} \\ p_3p_{61}p_{53}p_{45}p_{37}p_{29}\ p_{37}p_{29}p_{21}p_{13}p_5p_{63} & |p_5p_{63}p_{55}p_{47}p_{39}p_{31}\ p_{39}p_{31}p_{23}p_{15}p_7p_{57} \end{matrix}$$

$$\vdots$$

$$E(R_{15}) = \begin{matrix} k_{38}k_{18}k_{59}k_{42}k_3k_{57}k_3k_{57}k_{25}\ k_{41}k_{36}k_{10}| & k_{36}k_{10}k_{17}k_{27}k_{50}k_{11}k_{50}k_{11}k_{43}k_{34}k_{33}k_{52} \\ k_{33}k_{52}k_1\ k_2k_9k_{44}k_9k_{44}k_{35}k_{26}k_{49}k_{30}| & k_{49}k_{30}k_5k_{47}k_{62}k_{45}k_{62}k_{45}k_{12}\ k_{55}k_{38}k_{18} \end{matrix}$$

(2. 16)

3) Perform XOR of Equation (2.16) against Equation (2.13) to obtain A_i through equation:

$$A_i = E(R_{i-1}) \oplus K_i, \forall i \in [1;16], i \in N$$

(2. 17)

or can be written:

$$\frac{\begin{matrix} E(R_0) = \begin{matrix} p_7p_{57}p_{49}p_{41}p_{33}p_{25}\ p_{33}p_{25}p_{17}p_9p_1p_{59}\ p_1p_{59}p_{51}p_{43}p_{35}p_{27}\ p_{35}p_{27}p_{19}p_{11}p_3p_{61} \\ p_3p_{61}p_{53}p_{45}p_{37}p_{29}\ p_{37}p_{29}p_{21}p_{13}p_5p_{63}\ p_5p_{63}p_{55}p_{47}p_{39}p_{31}\ p_{39}p_{31}p_{23}p_{15}p_7p_{57} \end{matrix} \\ K_1 = \begin{matrix} k_{10}k_{51}k_{34}k_{60}k_{49}k_{17}\ k_{33}k_{57}k_2k_9k_{19}k_{42}\ k_3k_{35}k_{26}k_{25}k_{44}k_{58}\ k_{59}k_1k_{36}k_{27}k_{18}k_{41} \\ k_{22}k_{28}k_{39}k_{54}k_{37}k_4\ k_{47}k_{30}k_5k_{53}k_{23}k_{29}\ k_{61}k_{21}k_{30}k_{63}k_{15}k_{20}\ k_{45}k_{14}k_{13}k_{62}k_{55}k_{31} \end{matrix} \end{matrix}}{A_1 = a1_1a1_2a1_3 \dots a1_{48}} \oplus$$

(2. 18)

and so on up to:

$$A_{16} = a16_1a16_2a16_3 \dots a16_{48}$$

(2. 19)

4) Equation (2.18) to (2.19) of 48 bits are organized into 8 blocks (each block is 6 bits).

$$A_1 = a1_1a1_2a1_3 \dots a1_6|a1_7a1_8a1_9 \dots a1_{12}| \dots |a1_{43}a1_{44}a1_{45} \dots a1_{48}$$

$$\vdots$$

$$A_{16} = a16_1a16_2a16_3 \dots a16_6|a16_7a16_8a16_9 \dots a16_{12}| \dots |a16_{43}a16_{44}a16_{45} \dots a16_{48}$$

(2. 20)

5) Equation (2.20) split into 2 blocks, namely A_i^{left} of 2 bits and A_i^{right} of 4 bits.

$$A_i^{left} = ai_j ai_k \; \forall i \in [1;16], j = (1,7,13,19,25,31,37,43), k = j+5, i,j,k \in N$$

$$A_i^{right} = ai_l \; \forall i \in [1;16], l = (j+2, j+3, j+4, j+5), i,j,l \in N$$

(2. 21)

so we get:

$$A_1^{left} = a1_1 a1_6 | a1_7 a1_{12} | a1_{13} a1_{18} | a1_{19} a1_{24} | a1_{25} a1_{30} | a1_{31} a1_{36} | a1_{37} a1_{42} | a1_3 a1_{48}$$

$$A_1^{right} = a1_2 a1_3 a1_4 a1_5 | a1_8 a1_9 a1_{10} a1_{11} | a1_{14} a1_{15} a1_{16} a1_{17} | a1_{20} a1_{21} a1_{22} a1_{23}$$
$$a1_{26} a1_{27} a1_{28} a1_{29} | a1_{32} a1_{33} a1_{34} a1_{35} | a1_{38} a1_{39} a1_{40} a1_{41} | a1_{44} a1_{45} a1_{46} a1_{47}$$

$$\vdots$$

$$A_{16}^{left} \; and \; A_{16}^{right}$$

(2. 22)

6) Use the following Table 2.12 to subtitute Equation (2.22) with the formula:

$$S_i, \forall i \in [1;16], i \in N$$

(2. 23)

Table 2. 12 S-Box DES

S_1															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2															
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3															
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4															
7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5															
2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6															
12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7															
4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8															
13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Source: Processed by the Researcher (2024)

7) Arrage the values in Equation (2.24) to Table 2.11 in each column above the first row.

0000| 0001|0010| 0011|0100| 0101|0110| 0111
1000| 1001|1010| 1011|1100| 1101|1110| 1111

(2. 24)

and the following values in Equation (2.25) to each row left the first column.

00 | 01 |10 | 11

(2. 25)

8) Convert all values in Table 2.12 after adding Equation (2.24) and (2. 25) into a 4 bits binary character, thus obtaining Table 2.13.

Table 2. 13 Modified S-Box

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
	S_1															
00	1110	0100	1101	0001	0010	1111	1011	1000	0011	1010	0110	1100	0101	1001	0000	0111
01	0000	1111	0111	0100	1110	0010	1101	0001	1010	0110	1100	1011	1001	0101	0011	1000
10	0100	0001	1110	1000	1101	0110	0010	1011	1111	1100	1001	0111	0011	1010	0101	0000
11	1111	1100	1000	0010	0100	1001	0001	0111	0101	1011	0011	1110	1010	0000	0110	1101
	S_2															
00	1111	0001	1000	1110	0110	1011	0011	0100	1001	0111	0010	1101	1100	0000	0101	1010
01	0011	1101	0100	0111	1111	0010	1000	1110	1100	0000	0001	1010	0110	1001	1011	0101
10	0000	1110	0111	1011	1010	0100	1101	0001	0101	1000	1100	0110	1001	0011	0010	1111
11	1101	1000	1010	0001	0011	1111	0100	0010	1011	0110	0111	1100	0000	0101	1110	1001
	S_3															
00	1010	0000	1001	1110	0110	0011	1111	0101	0001	1101	1100	0111	1011	0100	0010	1000
01	1101	0111	0000	1001	0011	0100	0110	1010	0010	1000	0101	1110	1100	1011	1111	0001
10	1101	0110	0100	1001	1000	1111	0011	0000	1011	0001	0010	1100	0101	1010	1110	0111
11	0001	1010	1101	0000	0110	1001	1000	0111	0100	1111	1110	0011	1011	0101	0010	1100
	S_4															
00	0111	1101	1110	0011	0000	0110	1001	1010	0001	0010	1000	0101	1011	1100	0100	1111
01	1101	1000	1011	0101	0110	1111	0000	0011	0100	0111	0010	1100	0001	1010	1110	1001
10	1010	0110	1001	0000	1100	1011	0111	1101	1111	0001	0011	1110	0101	0010	1000	0100
11	0011	1111	0000	0110	1010	0001	1101	1000	1001	0100	0101	1011	1100	0111	0010	1110

	S_5															
00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011
	S_6															
00	1100	0001	1010	1111	1001	0010	0110	1000	0000	1101	0011	0100	1110	0111	0101	1011
01	1010	1111	0100	0010	0111	1100	1001	0101	0110	0001	1101	1110	0000	1011	0011	1000
10	1001	1110	1111	0101	0010	1000	1100	0011	0111	0000	0100	1010	0001	1101	1011	0110
11	0100	0011	0010	1100	1001	0101	1111	1010	1011	1110	0001	0111	0110	0000	1000	1101
	S_7															
00	0100	1011	0010	1110	1111	0000	1000	1101	0011	1100	1001	0111	0101	1010	0110	0001
01	1101	0000	1011	0111	0100	1001	0001	1010	1110	0011	0101	1100	0010	1111	1000	0110
10	0001	0100	1011	1101	1100	0011	0111	1110	1010	1111	0110	1000	0000	0101	1001	0010
11	0110	1011	1101	1000	0001	0100	1010	0111	1001	0101	0000	1111	1110	0010	0011	1100
	S_8															
00	1101	0010	1000	0100	0110	1111	1011	0001	1010	1001	0011	1110	0101	0000	1100	0111
01	0001	1111	1101	1000	1010	0011	0111	0100	1100	0101	0110	1011	0000	1110	1001	0010
10	0111	1011	0100	0001	1001	1100	1110	0010	0000	0110	1010	1101	1111	0011	0101	1000
11	0010	0001	1110	0111	0100	1010	1000	1101	1111	1100	1001	0000	0011	0101	0110	1011

Source: Processed by the Researcher (2024)

9) Subtitute Equation (2.22) in Table 2.13 according to S_i so we get each of 32 bits long.

$$B_i = S_i\left(A_i^{left}, A_i^{right}\right), \forall i \in [1;16], i \in N \tag{2. 26}$$

with elements of B_i being

$$B_i = bi_j, \forall i \in [1;16], j \in [1,32], i, j \in N \tag{2. 27}$$

thus obtain:

$$B_1 = b1_1 b1_2 b1_3 \dots b1_{32}$$
$$\vdots$$
$$B_{16} = b16_1 b16_2 b16_3 \dots b16_{32} \tag{2. 28}$$

10) Use the P - Box Table to perform the P - Box permutation.

Table 2. 14 P - Box

16	7	20	21	29	12	28	17
1	15	23	26	5	8	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Source: Processed by the Researcher (2024)

11) Perform the permutation of Equation (2.28) on the Table 2.14 using fomula:

$$P(B_i), \forall i \in [1;16], i \in N \tag{2. 29}$$

then we get:

$$P(B_1) = \begin{matrix} b1_{16}b1_{17}b1_{20}b1_{21}b1_{29}b1_{12}b1_{28}b1_{17}b1_1b1_{15}b1_{23}b1_{26}b1_5b1_8b1_{31}b1_{10} \\ b1_2b1_8b1_{24}b1_{14}b1_{32}b1_{27}b1_3b1_9b1_{19}b1_{13}b1_{30}b1_6b1_{22}b1_{11}b1_4b1_{25} \end{matrix}$$

$$\vdots$$

$$P(B_{16}) = \begin{matrix} b16_{16}b16_{17}b16_{20}b16_{21}b16_{29}b16_{12}b16_{28}b16_{17}b16_1b16_{15}b16_{23}b16_{26}b16_5b16_8b16_{31}b16_{10} \\ b16_2b16_8b16_{24}b16_{14}b16_{32}b16_{27}b16_3b16_9b16_{19}b16_{13}b16_{30}b16_6b16_{22}b16_{11}b16_4b16_{25} \end{matrix} \tag{2. 30}$$

12) Do XOR on Equation (2.26) and (2.30) to find R_i:

$$R_i = L_{i-1} \oplus P(B_i), \forall i \in [1;16], i \in N \tag{2. 31}$$

with the elements of R_i being:

$$R_i = ri_j, \forall i \in [1;16], j \in [1,32], i,j \in N \tag{2. 32}$$

then we get:

$$P(B_1) = \begin{matrix} b1_{16}b1_{17}b1_{20}b1_{21}b1_{29}b1_{12}b1_{28}b1_{17} & b1_1b1_{15}b1_{23}b1_{26}b1_5b1_8b1_{31}b1_{10} \\ b1_2b1_8b1_{24}b1_{14}b1_{32}b1_{27}b1_3b1_9 & b1_{19}b1_{13}b1_{30}b1_6b1_{22}b1_{11}b1_4b1_{25} \end{matrix}$$

$$L_0 = \begin{matrix} p_{58}p_{50}p_{42}p_{34}p_{26}p_{18}p_{10}p_2 & p_{60}p_{52}p_{44}p_{36}p_{28}p_{20}p_{12}p_4 \\ p_{62}p_{54}p_{46}p_{38}p_{30}p_{22}p_{14}p_6 & p_{64}p_{56}p_{48}p_{40}p_{32}p_{24}p_{16}p_8 \end{matrix}$$

$$R_1 = r1_1r1_2r1_3 \dots r1_{48} \quad \oplus$$

$$\vdots$$

$$R_{16} = r16_1r16_2r16_3 \dots r16_{48} \tag{2. 33}$$

13) On other hand, to find L_i using formula:

$$L_i = R_{i-1}, \forall i \in [1; 16], i \in N \tag{2. 34}$$

then we get:

$$\begin{matrix} L_1 = R_0 \\ \vdots \\ L_{16} = R_{15} \end{matrix} \tag{2. 35}$$

14) The combination Equation (2.31) and (2.34):

$$(L_i\ , R_i) = \big(R_{i-1}, L_{i-1} \oplus P(B_i)\big), \forall i \in [1; 16], i \in N \tag{2. 36}$$

with:

$$\begin{matrix} (L_1\ , R_1) = \big(R_0, L_0 \oplus P(B_1)\big) \\ \vdots \\ (L_{16}\ , R_{16}) = \big(R_{15}, L_{15} \oplus P(B_{16})\big) \end{matrix} \tag{2. 37}$$

c. Inverse Initial Permutation (IP^{-1})

After the enciphering stage, the last stage is Inverse Initial Permutation (IP^{-1}) as follows:

1) Use Table 2.15 to perform the first step.

Table 2. 15 Inverse Initial Permutation (IP^{-1})

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Source: Processed by the Researcher (2024)

2) Do permutation $(L_{16}\ , R_{16})$ on Table 2.15 to obtain cipher message C which is the result of the encryption process as follows:

$$C = P(L_{16}, R_{16})$$

(2. 38)

In DES decryption, it is almost similar to the encryption process, namely Initial Permutation (IP), Deciphering and Inverse Initial Permutation (IP^{-1}). Some distinguishing steps in the overall decryption process are as follows:

a. Compose the cipher message to be decrypt.
b. Use the same key as the encryption process.
c. The enciphering stage uses Table Wrapping to perform the left shift, while deciphering uses that for the right shift.
d. Enciphering uses a sequence of keys (1, 2, 3, ...16), while deciphering uses a sequence of keys:

$$K_i, \forall i \in [16; 1], i \in N$$

(2. 39)

e. In 16 iterations of enciphering and deciphering using the formula in Equation (2.36). The difference is when the enciphering stage uses (L_0, R_0) to get (L_{16}, R_{16}). While the deciphering uses (L_{16}, R_{16}) to get (L_0, R_0).
f. In the last step, perform the inverse initial permutation to produce the plain message.

Table 2. 16 Different of Enciphering – Deciphering DES

No	Stage	Enciphering	Deciphering
1.	Message Input	Plain	Cipher
2.	Message Output	Cipher	Plain
3.	Wrapping	Left Shift	Right Shift
4.	Key Sequence	$K_i, \forall i \in [1; 16], i \in N$	$K_i, \forall i \in [16; 1], i \in N$
5.	Input Iteration	(L_0, R_0)	(L_{16}, R_{16})
6.	Output Iteration	(L_{16}, R_{16})	(L_0, R_0)

Source: Processed by the Researcher (2024)

2.1.7 Triple Data Encryption Standard (3DES)

Triple Data Encryption Standard (3DES) is one of the cryptographic algorithms developed from the DES algorithm. This algorithm uses no different from its previous algorithm, the difference is that this algorithm uses 3 keys to encrypt and decrypt. There are 2 types of 3DES cryptography, namely 3DES with 2 keys (K_1, K_2, K_1) and 3DES with 3 keys (K_1, K_2, K_3) where $K_1 \neq K_2 \neq K_3$. The following will explain the 3DES algorithm using 2 keys and 3 keys.

a. Variables Definition.

There are several definitions of variables that will be used in the encryption and decryption formulas, including:

Table 2. 17 Variables Definition of 3DES

Variables	Definition
C	Cipher message
P	Plain message
$K_i, \forall i \in 1,2,3$	Key 1, 2 and 3
$E_{K_i}, \forall i \in 1,2,3$	Encrypt process use K_i
$D_{K_i}, \forall i \in 1,2,3$	Decrypt process use K_i

Source: Processed by the Researcher (2024)

b. 3DES with 2 keys.

The encryption $\left(E_{K_i}\right)$ and decryption (D_{K_i}) formulas of 3DES with 2 keys are represented as follows:

$$C = E_{K_1}\left(E_{K_2}\left(E_{K_1}(P)\right)\right) \tag{2. 40}$$

$$P = D_{K_1}\left(D_{K_2}\left(D_{K_1}(C)\right)\right) \tag{2. 41}$$

c. 3DES with 3 keys.

In 3DES with 3 keys, using the following representation of the encryption $\left(E_{K_i}\right)$ and decryption (D_{K_i}) formulas:

$$C = E_{K_3}\left(E_{K_2}\left(E_{K_1}(P)\right)\right) \quad (2.\ 42)$$

$$P = D_{K_1}\left(D_{K_2}\left(D_{K_3}(C)\right)\right) \quad (2.\ 43)$$

2.1.8 Least Significant Bit (LSB)

Least Significant Bit (LSB) is one of the methods in steganography. This algorithm focuses on how to insert the secret message into the lowest or rightmost bit at the end of the pixel data. Often the LSB algorithm uses a cover message in the form of a digital image (picture) so that the stego object also has an extension picture. The advantages of LSB are that the algorithm is simple, the image change from cover message to stego object has no significant difference when viewed and is widely applied in information transmission systems. In a binary character consisting of 8 bit characters $a_1\, a_2\, a_3 \ldots a_8$, there are Most Significant Bit (MSB) and LSB characters where MSB = a_1 and LSB = a_8. In 1 pixel color image is equivalent to 3 bytes or 24 bits consisting of Red Green Blue (RGB) components. If the MSB bit is changed, it will have a major effect on the color of the image, while if the LSB bit is changed, it does not give a noticeable color change. This is the focus area of the LSB algorithm, which utilizes the weakness of the visual senses to observe very small changes in image color. Next, we will explain the stages of the LSB algorithm in the encoding and decoding process.

a. Capacity.
   1) An RGB cover image of size is Cover = mn pixels = $3mn$ bytes = 24 mn bits, $\forall m, n \in N$ with:
      m ≔ cover image length size
      n ≔ cover image width size
   2) Every 1 byte cover image can hide 1 bit long secret message, thus Secret Message ≤ 24 mn bits Cover

b. Encoding LSB

The LSB Encoding algorithm is explained as follows:

1) Prepare a cover image of mn pixels and convert each pixel into bytes so that $c_{nm}, \forall m, n \in N$ is obtain.

Table 2. 18 Cover Image Size

m pixels

c_{11}	c_{12}	$c_{1\ldots}$	c_{1m}
c_{21}	c_{22}	$c_{2\ldots}$	c_{2m}
$c_{:1}$	$c_{:2}$	$c_{:\ldots}$	$c_{:m}$
c_{n1}	c_{n2}	$c_{n\ldots}$	c_{nm}

n pixels

Source: Processed by the Researcher (2024)

2) Every c_{nm} bytes represent 8 bits or can be written as:

$$c_{nm} = c_{nm1}\, c_{nm2}\, c_{nm\ldots}\, c_{nm8}, \forall m, n \in N \quad (2.\ 44)$$

3) Prepare a secret message s that will be encoded with size ≤ 24 mn bits or can be written as:

$$s = s_1\, s_2\, s_{\ldots}\, s_p, \forall p \in N \quad (2.\ 45)$$

4) Convert each s_p into a binary character so as to obtain:

$$s_p = s_{p1}\, s_{p2}\, s_{p\ldots}\, s_{p8}, \forall p \in N \quad (2.\ 46)$$

5) Substitute each bit of s_{p8} (last bit of s_p) to each bit of c_{nm8} (last bit of c_{nm}) sequentially with $p \leq nm$. If $p \leq nm$ then the remaining c_{nm8} that is not replaced by s_{p8} remains. The result is stego object $o_{nm}, \forall m, n \in N$.

Table 2. 19 Stego Object Size

$c_{11} \rightarrow s_{18} = o_{11}$	$c_{12} \rightarrow s_{28} = o_{12}$	$c_{1\ldots} \rightarrow s_{38} = o_{1..}$	$c_{1m} \rightarrow s_{48} = o_{1m}$
$c_{21} \rightarrow s_{58} = o_{21}$	$c_{22} \rightarrow s_{68} = o_{22}$	$c_{2\ldots} \rightarrow s_{78} = o_{2\ldots}$	$c_{2m} \rightarrow s_{\ldots 8} = o_{2m}$
$c_{:1} \rightarrow s_{p8} = o_{:1}$	$c_{:2} = o_{:2}$	$c_{:\ldots} = o_{:\ldots}$	$c_{:m} = o_{:m}$
$c_{n1} = o_{:m}$	$c_{n2} = o_{n2}$	$c_{n\ldots} = o_{n\ldots}$	$c_{nm} = o_{nm}$

Source: Processed by the Researcher (2024)

6) Convert stego object o_{nm} in binary character to pixels size.

c. Decoding LSB

The stage performed in LSB decoding is the inverse of LSB encoding. The LSB decoding process in steganography is to decipher the stego object into a cover image and secret message. This explains that in deciphering the stego object, a cover image will be obtained that contains certain different parts, so that the decipherment result is not exactly the same as the cover image. The different part that stands out is the secret message.

(a) (b)

Figure 2. 1 (a) Stego Object (b) Cover Image + Secret Message

Source: Processed by the Researcher (2024)

2.1.9 Zipped Information Package (ZIP) File

A file is a set of documents containing specific information that can be read using specific computer programs (Tekno, 2023). It is a sequence of data used for data storage and exchange. Files are data stored in media

and contain information about file size, saved date and change time, file name, file properties, and file attributes. Each piece of information in a classified documents is transmitted via various files. Document, system, image, video and audio are examples of files. The type of classified document files is explained briefly below:

a. A document file is a type of file that stores text, images, and information that humans can read. They are used to store text documents like reports, letters, and presentations. Microsoft Word documents (.docx), PDF documents (.pdf), simple text files (.txt), and PowerPoint presentations (.pptx) are examples of document file types.
b. System files are files that are used by operating system of a computer to manage basic operations and hardware. They are frequently core components of the operating system and should not be edited by the user. Dynamic Link Library (.dll) files in Windows systems, system files (.sys), and program execution files (.exe) are examples of system files.
c. Image Files: Image files are used to store images and graphics. They contain information that defines pixels and colors that comprise the image. JPEG (.jpg), PNG (.png), GIF (.gif), and BMP (.bmp) are examples of image file types.
d. Audio files are a type of file that is used to store audio data such as music or voice. They contain data that defines sound waves that are used to reproduce audio. MP3 (.mp3), WAV (.wav), and FLAC (.flac) are examples of audio file types.
e. A video file is a type of file that is used to store video data that consists of a series of moving images and sound. They contain information about the images and sounds used to make a video. MP4 (.mp4), AVI (.avi), and MKV (.mkv) are examples of video file types.

ZIP files are one of the most commonly used data compression techniques in the digital world to combine 1 or more files for easier archiving. This technique utilizes compression algorithms such as deflate to minimize file size. ZIP files can also be used to back up compressed data to minimize data loss if any data is deleted. Currently, there are many software to support ZIP file operations such as WinZip, 7-Zip and WINRAR. When combining various documents into ZIP, the processed document will change its extension to .zip. This file type will be used in research to support the data compression process of various document formats used.

Researchers chose ZIP as a compression method in the study because it has more advantages:

a. Combined Compression and Encryption: ZIP files can be compressed and encrypted simultaneously. This is advantageous because the file size becomes smaller and the data is encrypted, making it safer when transferred.
b. File Size Masking: Compression hides the original size of the file, which can be useful to avoid detecting hidden content.
c. Selected Encryption Algorithm: ZIP allows the use of various encryption algorithms, such as AES, which can be selected based on the level of security required.
d. Masking Capacity: Files in a ZIP have internal data redundancy, which can be leveraged to hide messages or other data without affecting file integrity or compression.
e. Concealment Granularity: Data can be hidden in multiple files or subdirectories in a ZIP, increasing the difficulty of detection.
f. Natural File Splitter: ZIP files are already fragmented into smaller files, which can help in the Least Significant Bit (LSB) based steganography process.

2.1.10 Peak Signal to Noise Ratio (PSNR)

Before we get into PSNR, it's important to understand MSE. Mean Square Error (MSE) is a digital image processing evaluation metric that measures the level of distortion or error between the original image and the resulting image. MSE is computed by averaging the squares of the pixel intensity differences between the two images. The MSE formula is defined as the sum of the squares of the differences in pixel values between the original and resulting images, divided by the total number of pixels. The lower the MSE value, the less distortion occurs, indicating a high degree of similarity between the original and processed images. MSE is frequently used in a variety of contexts, including image compression quality evaluation, image restoration, and image processing in general.

Peak Signal-to-Noise Ratio (PSNR) is a popular metric for evaluating digital image quality in image processing. PSNR is the ratio of the maximum signal achieved by an image to the amount of noise or error that occurs. PSNR, expressed in decibels (dB), indicates how close the resulting image is to the original image when distortion is taken into account. The higher the PSNR value, the less distortion there is, and thus the image quality is considered better. PSNR is frequently used in the context of image compression, where the main goal is to retain as much image information as possible while compressing it as much as possible. This metric is also useful in evaluating the results of image restoration and other image processing, as it provides a clear picture of how trustworthy and faithful the resulting image is to the original image.

The mathematical transformation that connects Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) in digital images can explain the relationship between the two (Fadillah and Rizka, 2019). MSE, which is the average of the squared pixel intensity differences between the original and generated images, can be used to calculate PSNR. PSNR is calculated by using the MSE value in a formula that calculates the ratio of maximum signal to noise levels. PSNR is defined as 10 times the base 10 logarithm

of the square of the maximum signal divided by the MSE. As a result, the lower the MSE value, the higher the PSNR value, indicating a higher level of image quality. This relationship shows that lowering error (as measured by MSE) leads to an increase in PSNR, which indicates an improvement in digital image quality. Thus, MSE and PSNR are interrelated and are frequently used in digital image evaluation and optimization together, providing a comprehensive view of how faithful the generated image is to the original image. The following will describe the MSE and PSNR formulas that will be used in this research.

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(S_{xy} - C_{xy}\right)^2 \quad (2.\ 47)$$

$$PSNR = 10log_{10}\left(\frac{C_{max}^2}{MSE}\right) \quad (2.\ 48)$$

with definitions:

$MSE \coloneqq Mean\ Square\ Error$

$M \coloneqq Length\ of\ image\ dimension\ on\ x - \ absis$

$N \coloneqq Width\ of\ image\ dimension\ on\ y - ordinat$

$S_{xy} \coloneqq Bit\ of\ stego\ object\ at\ (x, y)$

$C_{xy} \coloneqq Bit\ of\ cover\ object\ at\ (x, y)$

$PSNR \coloneqq Peak\ Signal\ to\ Noise\ Ratio$

$C_{max}^2 \coloneqq Maximum\ C_{xy}\ pixel\ value\ in\ the\ object$

2.2 Previous Research

The study of 3DES Cryptography, LSB Steganography and ZIP files are not something new because all of this method has been created by previous researchers. However, the combination of these three methods is a new innovation. Previously, researchers will explain some previous research results as material for creating the latest innovations.

Table 2. 20 Previous Research of 3DES and LSB

No	Author	Research Title	Year
1.	- Shihab A Shawkat - Israa Al Barazanchi - Bilal A Tuama	Proposed System for Data Security in Distributed Computing in Using Triple Data Encryption Standard and Rivest Shamir Adlemen	2022
2.	- Subhash Chand Gupta - Vikas Kumar	Minimizing the Security Risks in Hybrid Cloud Networks with the Aid of Optimal Triple Data Encryption Standard Algorithm	2019
3.	- Christy Atika Sari - Eko Hari Rachmawanto - Christanto Antonius Haryanto	Cryptography Triple Data Encryption Standard (3DES) for Digital Image Security	2018
4.	- R Ramya Devi -V Vijaya Chamundeeswari	Triple DES: Privacy Preserving in Big Data Healthcare	2018
5.	- Devavrat Agnihotri - Saad Ahmed - Dhanashree Darekar - Chinmay Gadkari - Sagar Jaikar - Mohandas Pawar	A Secure Document Archive Implemented using Multiple Encryption	2020
6.	- Saadi Mohammed Saadi	A Modern Mechanism for Generating 3DES Algorithm Keys Based on Rubik's Cube	2022
7.	- Hasan Kadhim A. Alsuwaiedi - Abdul Monem S. Rahma	A New Modified DES Algorithm Based on The Development of Binary Encryption Functions	2023

8.	- Akshitha Vuppala - R Sai Roshan - Shaik Nawaz - JVR Ravindra	An Efficient Optimization and Secure Triple Data Encryption Standard Using Enhanced Key Scheduling Algorithm	2020
9.	- Mohan Naik Ramachandra - Madala Srinivasa Rao - Wen Cheng Lai - Bidare Divakarachari Parameshachari - Jayachandra Ananda Babu - Kivudujogappa Lingappa Hemalatha	An Efficient and Secure Big Data Storage in Cloud Environment by Using Triple Data Encryption Standard	2022
10.	- Nurdin - Dahlan A - Widia F - R Ratnadewi - Nuning K Dian R - Kusuma R - Edi S - Very K - Febry L - Dian	SMS Encryption Application Using 3DES (Triple Data Encryption Standard) Algorithm Based on Android	2022
11.	- Aditya Kumar Sahu - Gandharba Swain	High Fidelity Based Reversible Data Hiding Using Modified LSB Matching and Pixel Difference	2019
12.	- De Rosal Ignatius Moses Setiadi	Improved Payload Capacity in LSB Image Steganography Uses Dilated Hybrid Edge Detection	2019

13.	- Supriadi Rustad - De Rosal Ignatius Moses Setiadi - Abdul Syukur Pulung Nurtantio Andono	Inverted LSB Image Steganography Using Adaptive Pattern to Improve Imperceptibility	2020
14.	- Yanting Wang - Mingwei Tang - Zhen Wang	High - Capacity Adaptive Steganography based on LSB and Hamming Code	2020
15.	- Pratap Chandra Mandal - Imon Mukherjee - B N Chatterji	High - Capacity Steganography based on IWT Using Eight – Way CVD and n-LSB Ensuring Secure Communication	2021
16.	- Zaid Bin Faheem - Abid Ishaq - Furqan Rustam - Isabel de la Torre Díez - Daniel Gavilanes - Manuel Masias Vergara - Imran Ashraf	Image Watermarking Using Least Significant Bit and Canny Edge Detection	2023
17.	- Shahid Rahman - Jamal Uddin - Hameed Hussain - AftabAhmed - AyazAli Khan - Muhammad Zakarya - Afzal Rahman - Muhammad Haleem	A Hufman Code LSB Based Image Steganography Technique Using Multi-Level Encryption and Achromatic Component of An Image	2023
18.	- Murat Hacimurtazaoglu - Kemal Tutuncu	LSB-Based Pre-Embedding Video Steganography with Rotating & Shifting Poly-Pattern Block Matrix	2022

19.	- Tzu-Chuen Lu - Ping-Chung Yang - Biswapati Jana	Improving The Reversible LSB Matching Scheme Based on The Likelihood Re-Encoding Strategy	2021
20.	- B. S. Shashikiran - K. Shaila - K. R. Venugopal	Minimal Block Knight's Tour and Edge with LSB Pixel Replacement Based Encrypted Image Steganography	2021
21.	- Parma Hadi Rantelinggi - Eka Saputra	Triple DES Cryptography Algorithm and LSB Steganography as a Combined Method in Data Security	2019

Source: Processed by the Researcher (2024)

All of these previous research are good enough, but there are still gaps that need to be improved, namely not combining cryptography, steganography and compression. These three methods are quite influential in sending messages. Cryptography is useful for protecting the confidentiality of messages. Steganography is useful for disguising the existence of the message. While compression is useful for minimizing the size of the message. Thus, this research will be organized to complement the shortcomings of previous research through a combination of the three designs. On other hand, the reasons for choosing 3DES - cryptography and LSB - steganography methods are still reinforced by previous research. The following are some of the advantages of each previous research which are the reasons for choosing the method in this research as follows:

2.2.1 Proposed System for Data Security in Distributed Computing in Using Triple Data Encryption Standard and Rivest Shamir Adlemen

Security issues are a significant concern in distributed computing, and clients should scramble information before being shipped off the cloud. Distributed computing security relies on encryption, and this paper discusses the comparative results of implementing 3DES and 3kRSA encryption algorithms on cloud platforms (eyeOS). The algorithms take data

input of various sizes and are compared using parameters like computation time, output bytes, and time complexity. 3kRSA consumes more time and output bytes than 3DES, but is more security efficient. The 3DES algorithm is executed faster and with higher throughput levels, but 3kRSA is more efficient. Future work will focus on implementing and developing a method for data encryption that uses principles of physics and quantum theories instead of mathematical equations. This would create a more secure environment for data storage and retrieval in various sectors, such as government, banking, military, and security.

Table 2. 21 Time Taken and Output in 3DES and 3kRSA

No	Input Data Size (Bytes)	Encryption		Decryption		Output bytes	
		Computation Time in 3DES	Computation Time in 3kRSA	Computation Time in 3DES	Computation Time in 3kRSA	In 3DES	In 3kRSA
1	25	8	10	4	35	36	65
2	38	4	8	6	51	52	97
3	66	15	35	17	75	92	161
4	79	20	43	22	88	115	180
5	92	28	49	25	102	140	195

Source: Shawkat et al (2022)

2.2.2 Minimizing the Security Risks in Hybrid Cloud Networks with the Aid of Optimal Triple Data Encryption Standard Algorithm

This paper proposes a methodology to securely store and retrieve documents in the cloud without information loss. The methodology aims to reduce security risks in hybrid cloud systems by using de-duplication and encryption algorithms. The method involves collecting documents from different users, storing them in the cloud, removing repeated documents, and encrypting them using the OTDES algorithm. The data is stored in the cloud, and the user retrieves the information through a user interface module. The efficiency of the system is analyzed using various evaluation metrics, including total time consumed, encryption time, number of files uploaded, and MIM attack resolution time. The proposed method outperforms existing methods in all iterations, and the fitness function calculation shows that OMB provides efficient performance. The proposed

method focuses on de-duplicated data and data encryption to increase data security on the cloud.

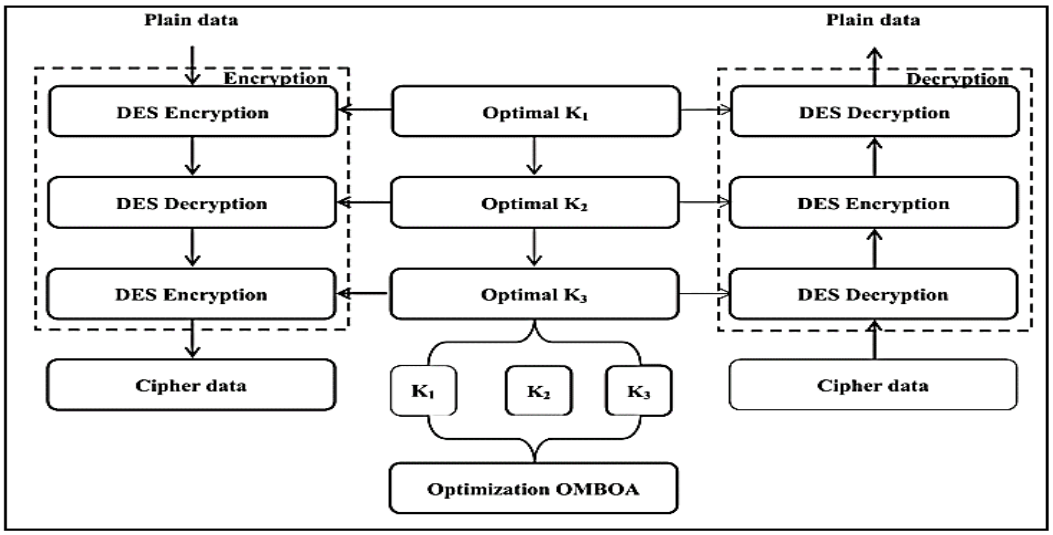


Chart 2. 9 Optimal 3DES Algorithm

Source: Gupta and Kumar (2011)

2.2.3 Cryptography Triple Data Encryption Standard (3DES) for Digital Image Security

Christy Atika et al (2018) conducted 3DES cryptography research on digital image security. They tested 3DES on plain messages with image extensions. The software used in this research is Graphical User Interface (GUI). The research was conducted on 5 types of image objects (png and bmp) using 2 types of sizes, namely 64 x 64 and 128 x 128. The results show that 3DES cryptography can also be used in encrypting plain images. The average time required to encrypt and decrypt a 64 x 64 image is 176,0633 seconds. Meanwhile, the 128 x 128 image takes an average of 685,0948 seconds. The following are the time lapse results from the study.

Table 2. 22 Time Lapse of 3DES

No	Nama of Image	Size	Time Lapse (Second)	
			Encrypt	Decrypt
1.	baboon.png	64 x 64	179,2727	174,2991
2.	bear.bmp		176,2882	175,2932
3.	f16.png		174,1922	179,2991
4.	lochness.png		177,9931	178,9918
5.	papermachine.png		173,0019	172,0014
6.	baboon.png	128 x 128	680,9912	683,2001
7.	bear.bmp		685,0013	689,9913
8.	f16.png		688,1132	681,3305
9.	lochness.png		683,0483	686,9134
10.	papermachine.png		689,1378	683,2213

Source: Atika et al (2018)

2.2.4 Triple DES: Privacy Preserving in Big Data Healthcare

Currently, big data has grown rapidly in healthcare. The use of only one cryptographic method is not optimal for the purpose of securing messages. Ramya Devi and Vijaya Chamundeeswari (2018) have conducted research using anonymization techniques. Anonymization is described as the technique that turns obvious data into an unreadable and irreversible form, including pre-image resistant hashes and encryption methods that discard the decryption key. The study aims to compare 3 cryptographic algorithms: DES, AES and Anonymization 3DES (A3DES). The study tested the security in encryption and decryption. The results showed that A3DES (Combination of Anonymization and 3DES) is superior to DES and AES. Here are the comparison results of the three algorithms.

Table 2. 23 Comparison of DES, AES and A3DES

No	File Size (MB)	DES (%)	AES (%)	A3DES (%)
1.	200	20	40	60
2.	400	30	50	90
3.	600	45	80	110
4.	800	60	95	120
5.	1.000	80	115	145

Source: Ramya and Vijaya (2018)

2.2.5 A Secure Document Archive Implemented using Multiple Encryption

Document archive is something very vital and risky if used by the wrong party. Therefore, it must be protected with cryptography. Each cryptography method has its own advantages. Agnihotri et al (2020) have created a combined cryptography method. They combine AES and 3DES crypthography into one encryption process. The encryption starts with AES and then continues with 3DES as shown in the figure. The research gave amazing results. A document encrypted using AES and 3DES can provide double protection against attacks like brute force.

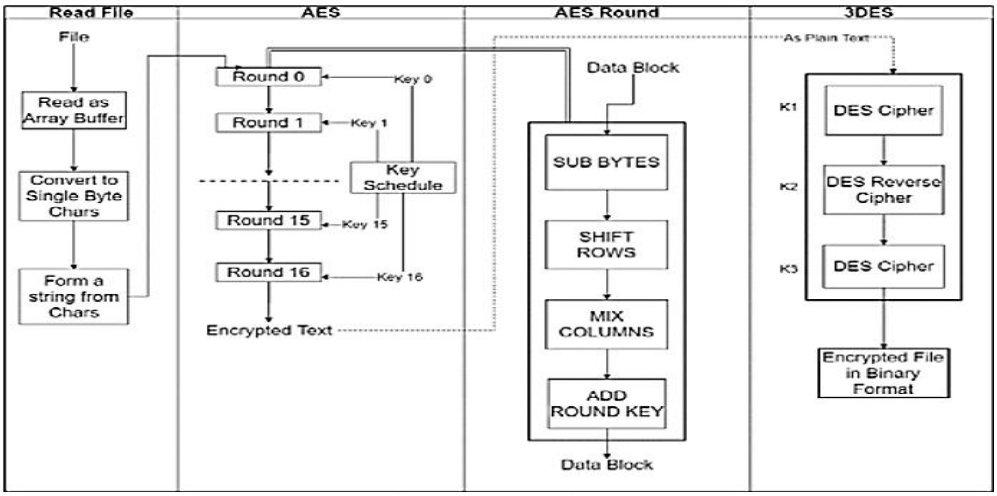


Chart 2. 10 AES - 3DES Encryption

Source: Agnihotri et al (2020)

2.2.6 A Modern Mechanism for Generating 3DES Algorithm Keys Based on Rubik's Cube

This paper discusses the reconfiguration of the key of the 3DES Algorithm, a symmetric encryption technique, to make it more secure, faster, and robust. The improved algorithm has good resistance against brute force attacks, making it more efficient. The paper tests the algorithm's performance with various file sizes and types, comparing it with the traditional method. The results show that the new method increased throughput while enhancing the performance of the original 3DES algorithm

by speeding up encryption and decryption. The rate of encryption increased by 53.54% after using Rubik's Cube to generate keys, demonstrating that the new approach outperforms the old one in terms of productivity, encryption, and decryption speed, resulting in lower battery consumption.

Table 2. 24 Comparison of Original and Improved 3DES Algorithms

Algorithm	Correlation Coefficient			Speed improvement percentage
	Strong	Medium	Weak	
Original 3DES	5.4%	36.3%	58.3%	47.25%
Enhanced 3DES Algorithm	6.4%	36.3%	57.3%	53.54%

Source: Saadi (2022)

2.2.7 A New Modified DES Algorithm Based on The Development of Binary Encryption Functions

This study presents a modified DES algorithm to address flaws in the Data Encryption Standard (DES). The DES algorithm, which uses two functions (XOR) and a finite number of data combinations, has been extended in key space and plaintext using multiple keys. The proposed DES employs three keys, with the first key for encryption or decryption, the second key specifying block size, and the third key representing state tables. The proposed DES employs three keys during each of the 16 DES rounds, improving its difficulty against attack. Unlike a triple DES, which repeats DES three times, the proposed DES employs three keys during the course of 48 rounds. The proposed DES also manipulates bits with a variety of attitudes or states, resulting in a lower level of complexity. The modified DES algorithm strengthens its defenses against all types of deciphering, increasing the effectiveness of the key and increasing its resistance to

brute-force assaults. Although the algorithm increases the complexity of calculating keys, it is considered acceptable for the revival of the DES. algorithm.

Table 2. 25 NIST Test Computation between DES and Suggested DES

Name of Statistical Test	Standard DES		Suggested DES	
	P-Value	Status	P-Value	Status
Approximate Entropy	0.624	Pass	0.810	Pass
Block Frequency	0.639	Pass	0.749	Pass
Cumulative Sums	0.068	Pass	0.330	Pass
FFT	0.082	Pass	0.662	Pass
Frequency	0.116	Pass	0.410	Pass
Linear Complexity	0.884	Pass	0.623	Pass
Longest Run	0.25	Pass	0.847	Pass
Non-Overlapping Template	0.527	Pass	0.517	Pass
Overlapping Template	0.480	Pass	0.787	Pass
Random Excursions	0.591	Pass	0.757	Pass
Random Excursions Variant	0.761	Pass	0.630	Pass
Rank	0.432	Pass	0.434	Pass
Runs	0.001	Pass	0.388	Pass
Serial	0.649	Pass	0.670	Pass
Universal	0.326	Pass	0.973	Pass

Source: Kadhim and Rahma (2023)

2.2.8 An Efficient Optimization and Secure Triple Data Encryption Standard Using Enhanced Key Scheduling Algorithm

This paper proposes a novel FORTIS algorithm to improve the Key Schedule Algorithm. The Verilog code was simulated and designed using Cadence Design Suite, resulting in minimal impact on power and area compared to the existing Triple-DES. Power traces were obtained using Chipwhisperer ® - Lite and CW-305 Artix-7 FPGA boards. The introduction of a Comparator and versatile shifter made it harder to identify operations from power trace, reducing PGE values and making the algorithm more secure.

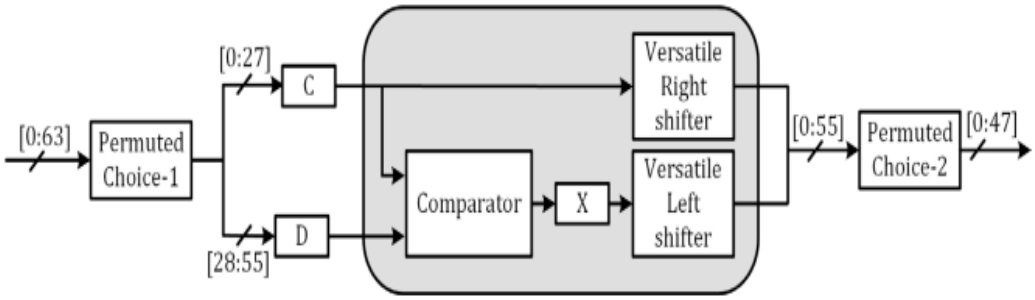


Chart 2. 11 Fortis Algorithm

Source: Vuppala et al (2020)

2.2.9 An Efficient and Secure Big Data Storage in Cloud Environment by Using Triple Data Encryption Standard

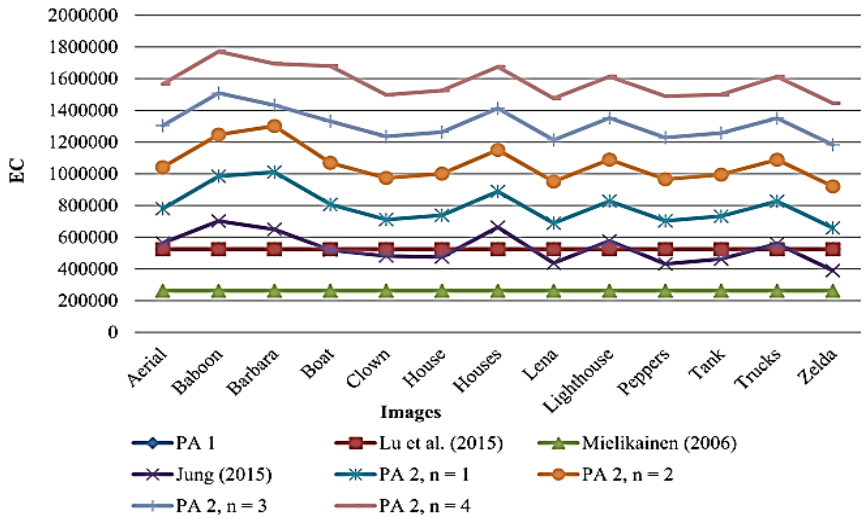
The TDES methodology is proposed to provide security for big data in the cloud environment, particularly in healthcare applications. The methodology involves data selection and encryption using TDES methodology, providing key strength of 112 and 168 bits. The encrypted data is stored in the cloud, and after requesting specific data, the decryption process is performed to retrieve it. The proposed TDES methodology simplifies the process by increasing key sizes to protect against attacks and protect data privacy. Experimental results show the method is effective in providing security and privacy to big healthcare data in the cloud environment. However, it requires higher network and CPU usage. A modified elliptic curve-based cryptographic methodology will be integrated with block-chain technology to reduce CPU usage, network utilization, and computational time in the cloud environment. The model is tested on image and audio files to enhance security for Cloud-based services.

2.2.10 SMS Encryption Application Using 3DES (Triple Data Encryption Standard) Algorithm Based on Android

In this study, Nurdin et al (2022) conducted tests to implement 3DES cryptography on sending messages via SMS. This test shows that sending messages encrypted using 3DES can succeed perfectly as evidenced by sending and receiving the same text message. Testing is done on android - based smartphones.

2.2.11 High Fidelity Based Reversible Data Hiding Using Modified LSB Matching and Pixel Difference

LSB steganography requires secret message length ≤ cover message length. In decryption of stego objects or called Reversible Data Hiding (RDH) is often inefficient against large messages. Therefore, Kumar and Swain (2019) developed research to improve the RDH approach in the form of 2 phases, namely: improvised dual image based LSB matching and n-Rightmost Bit Replacement (n-RBR) and Modified Pixel Value Differencing (MPVD). The first approach extends the ability of LSB matching using dual images. The second approach uses four identical cover images with 2 phase n-RBR and MPVD. The research compared images used by Mielikainen (2006), Lu et al (2015) and Jung (2015). In PA 2, n = 1, 2, 3, and 4 are used. The results of the study are very significant because they increase the Embedding Capacity (EC) by the highest order: PA 2, n = 4; PA 1 and PA 2, n = 2.



Graph 2. 1 Comparison of Embedding Capacity (EC)

Source: Kumar and Swain (2019)

2.2.12 Improved Payload Capacity in LSB Image Steganography Uses Dilated Hybrid Edge Detection

In a good LSB image steganography method, the cover image must be able to completely disguise the secret message. If there is a gap in the stego object that stands out, the stego object can be broken. Often the edge lines on the stego object are ignored. Therefore, Rosal (2019) utilized edge detection on a cover to improve the disguise of the secret message. The research shows that the quality of the stego image imperceptibility can be maintained. Together with that, edge detection can also indirectly increase the payload capacity of the secret message. This research compares the results of previous research conducted by Bai et al (2017), Gaurav and Ghanekar (2018), Setiadi and Jumanto (2018) and Setiadi (2019) using the same cover image. The capacity of the secret message used is 1,024 bits, 4,096 bits, 8,192 bits and 16,284 bits. With the same cover image and secret message, Rosal was able to show that the method he used gave better results with the majority PSNR value increasing and the majority MSE decreasing.

Table 2. 26 Comparison of PSNR and MSE

Comparison of PSNR					
Capacity (bits)	**Previous Research**				**Rosal (2019)**
	Bai et al (2017)	**Setiadi (2019)**	**Gaurav and Ghanekar (2018)**	**Setiadi and Jumanto (2018)**	
1.024	66,2163	69,2603	69,2797	67,8120	**69,7156**
4.096	63,1718	66,2462	66,2631	64,7703	**63,6396**
8.192	60,1287	63,2481	63,1555	61,8675	**63,6114**
16.384	overflow	60,3134	60,2261	overflow	**60,6973**
Comparison of MSE					
Capacity (bits)	**Capacity (bits)**				**Rosal (2019)**
	Bai et al (2017)	**Setiadi (2019)**	**Gaurav and Ghanekar (2018)**	**Setiadi and Jumanto (2018)**	
1.024	0,0155	0,0077	0,0077	0,0108	**0,0070**
4.096	0,0313	0,0154	0,0154	0,0217	**0,0141**
8.192	0,0631	0,0308	0,0315	0,0423	**0,0283**
16.384	overflow	0,0605	0,0618	overflow	**0,0554**

Source: Rosal (2019)

2.2.13 Inverted LSB Image Steganography using Adaptive Pattern to Improve Imperceptibility

Rustad et al (2020) tried to research the use of LSB Steganography algorithm on digital images. This research uses an adaptive pattern of inverted LSB to increase the imperceptibility of the information carried. The arrangement of 1 character is equivalent to 8 bit characters or can be written $a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7\ a_8$. In this study, the reverse pattern of the 8 bit character is used so that it reads $a_8\ a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1$. Thus, the LSB is not operated on a_8, but on a_1. This research tested imperceptibility with message objects of 1.000 and 5.000 characters. The final result shows that by using the inverted LSB, the interceptor will find it harder to detect the secret message in the stego object. This is proven by the results of the calculation of Mean Square of Error (MSE) which decreases and Peak Signal to Noise Ratio (PSNR) which increases.

Table 2. 27 Result of MSE and PSNR

Message Length (Char)	Before		After	
	MSE	PSNR	MSE	PSNR
1.000	0,058887	60,4308	0,019109	66,616314
5.000	0,300461	53,3529	0,103816	58,197853

Source: Rustad et al (2020)

2.2.14 High – Capacity Adaptive Steganography based on LSB and Hamming Code

In LSB, decoding is the process of extracting the stego object into cover image and secret message. This decoding process will become a problem if the extracted stego object turns out to be a different size from the cover image. Another worse condition is if the stego object that is sent is damaged in the file. Of course, this will raise suspicion that there is a size difference or file damage. Yanting Wang et al (2020) proposed their experiment using a combination of several methods. Their research uses edge detection, LSB and hamming code methods. In their experiment, they determine the performance of the proposed method through perceptual quality assessment and histogram analysis. In perceptual quality, they tested the capacity, Mean Square of Error (MSE) and Peak to Signal to Noise Ratio (PSNR). They tested 3 images with each image containing 5 capacity secret messages (in KB): 9.424, 14.768, 16.616, 21.368 and 30.224. They compared their research with previous studies conducted by Shabir et al (2018), Ghosal et al (2018), Junlan et al (2017) and Manashee et al (2019). One of the results shows that the PSNR of the proposed method is better than the previous 4 studies. This shows that the research can improve the disguise of the secret message so that it is difficult to detect.

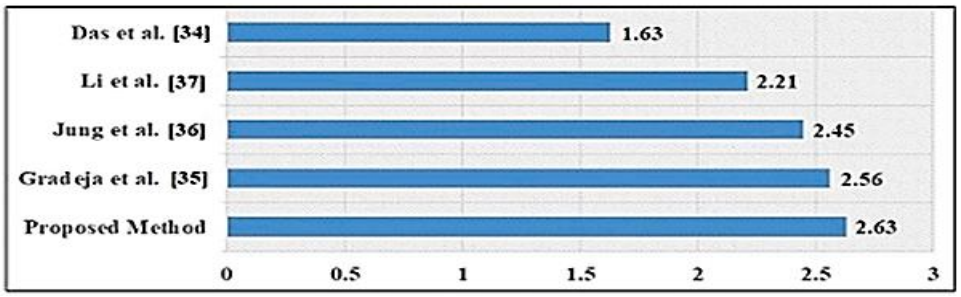
Table 2. 28 PSNR by Edge Detection, LSB and Hamming Code

Images	Capacity	the proposed method PSNR	Shabir et al. [11]	Ghosal et al. [13]	Junlan et al. [14]	Manashee et al. [15]
Lena	9424	68.418	47.448	61.836	62.770	58.189
	14768	66.476	47.442	60.664	60.823	56.256
	16616	66.008	47.440	60.264	60.357	55.841
	21368	64.838	47.434	59.142	59.232	54.653
	30224	63.397	47.424	57.032	57.681	53.196
Baboon	9424	68.417	47.433	61.756	62.882	58.262
	14768	66.523	47.427	60.412	60.924	56.273
	16616	66.024	47.425	60.432	60.357	55.851
	21368	64.891	47.419	59.247	59.502	54.662
	30224	63.430	47.409	57.473	57.818	53.206
Airplane	9424	68.429	47.444	61.852	62.776	58.279
	14768	66.515	47.437	60.704	60.801	56.268
	16616	66.023	47.435	60.397	60.357	55.863
	21368	64.949	47.430	59.243	59.332	54.692
	30224	63.425	47.419	57.132	57.697	53.217

Source: Yanting et al (2020)

2.2.15 High – Capacity Steganography based on IWT Using Eight – Way CVD and n – LSB Ensuring Secure Communication

Integer Wavelet Transform (IWT) is one of the transformation techniques in LSB steganography. The technique referred to here is a form of transformation from cover image to stego object or vice versa. Mandal et al (2021) made research related to high-capacity images based on IWT. This research uses a modification of the LSB technique in the form of n-LSB and also eight-way Cover Value Difference (CVD). CVD is the transformation of an image into an eight-way matrix. They perform the embedding process on 3 subbands, including: Low High (LH), High Low (HL) and High High (HH) subbands. They also used the 2^n correction technique with the formula 2^{n-1} where $3 \leq n \leq 5$, in order to reduce the level of image distortion. This experiment tested several important aspects of steganography, namely: embedding capacity, visual quality, security and comparative analysis with the state of the art. In the security aspect, it is broken down into several assessments based on histogram analysis, color frequency test, divergence test, Pixel Difference Histogram (PDH), StirMark Benchmark 4.0, StegExpose. The object images used are some of the previous studies from Das et al (2020), Li et al (2018), Jung et al (2015) and Gradeja et al (2018). Globally, this experiment produces a better Absolute Edge Change (AEC) rate than the others.



Graph 2. 2 Comparison of Absolute Edge Change (AEC)

Source: Mandal et al (2021)

2.2.16 Image Watermarking Using Least Significant Bit and Canny Edge Detection

This study proposes a simple and efficient method for image watermarking for security, based on the canny edge detection algorithm and LSB approach. The canny edge detection algorithm is used to find suitable places for watermarks, making it easy for attackers to detect and break them. The LSB approach is used because it works on the pixel level and has a higher capacity to add watermarks. Experimental results show better results than existing state-of-the-art works. Future research aims to apply a new filter to measure watermark image robustness and implement this technique in color image and video watermarking.

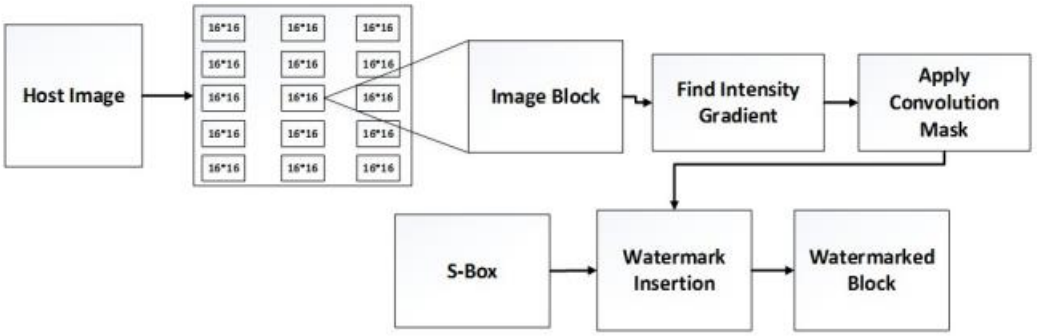


Chart 2. 12 Watermark Embedding Flow Diagram

Source: Faheem et al (2023)

2.2.17 A Hufman Code LSB Based Image Steganography Technique Using Multi-Level Encryption and Achromatic Component of An Image

The proposed method aims to create a secure and efficient encryption system for stego images. The method is tested using cover pictures of peppers and lakes, with 256x256 dimensions. The method is tested against different assaults using Unifed Average Changing Intensity (UACI) and Number of Pixels Changing Rate (NPCR). The results show that the algorithm can effectively resist different attacks, including noise attacks. The algorithm also effectively opposes trimming attacks, demonstrating its ability to resist information editing attacks. The method uses Hufman code, HSI color model, MLEA, Magic matrix, and LSB substitution to embed the secret message in cover images. The results show a PSNR of 79.29 dB over 165 standard images, proving its control and efficiency compared to other methods. The main drawback is the embedding of the secret message in cover objects, which can be confusing and unclear. The method is easy to program and simple, offering transparency and robustness. Further improvements include unsupervised learning, Deep Learning concepts, and statistical and image processing attacks to produce reliable free stego images.

2.2.18 LSB-Based Pre-Embedding Video Steganography with Rotating & Shifting Poly-Pattern Block Matrix

The paper presents LSB-based pre-embedding video steganography with a rotating and shifting poly-pattern block matrix. The method aims to balance robustness, imperceptibility, and payload in video steganography. The combination of non-sequential data embedding in all frames algorithm and shifting-rotating KBM increases robustness and imperceptibility, while acceptable payload and time to implement increase. Combining sequential data embedding with all channels of RGB and fixed KBM decreases security, robustness, and imperceptibility values, while payload increases

and time to implement decreases. The method achieves successful imperceptibility, acceptable payload, and contribution to robustness. However, the complexity of the method makes computational time lengthy, and powerful graphics cards or supercomputers can be used to reduce embedding time. The authors also investigate statistical attacks on the system.

Table 2. 29 Average of PSNRs, MSEs, SSIMs and Payloads

		PSNR (dB)	Payload (%)	MSE	SSIM
1st secret message	Average value	72.63878	8.2%	0.11055	0.99960
	Best value	80.01458	7.5%	0.00066	0.99999
2nd secret message	Average value	69.71885	20.3%	0.24445	0.99907
	Best value	75.72473	19.7%	0.00174	0.99999

Source: Hacimurtazaoglu and Tutuncu (2021)

2.2.19 Improving The Reversible LSB Matching Scheme Based on The Likelihood Re-Encoding Strategy

This paper proposes a modified LSB matching method using dual-image and likelihood recording strategy. The scheme analyzes all possible modifications under hidden conditions and re-encodes each combination according to its frequency of occurrence. The combination with a higher occurrence rate is re-encoded with a lower modification rule. The embedding capacity of the proposed method is similar to Tseng et al.'s scheme, and the image quality of the proposed scheme is the highest among comparison methods. The proposed scheme is effective against steganalysis attacks and transforms the worst cases with better encode results. The worst case is re-encoded with the minimum distortion code 0, reducing image distortion effectively. The proposed scheme is particularly suitable for simple secret images like logos, cartoons, and signatures. In the future, the scheme will need to adapt or elastically change the encoding strategy to encode different cases and filter bad cases, which can cause significant damage in the pre-processing procedure. Additionally, adding

more translation tables can improve image quality.

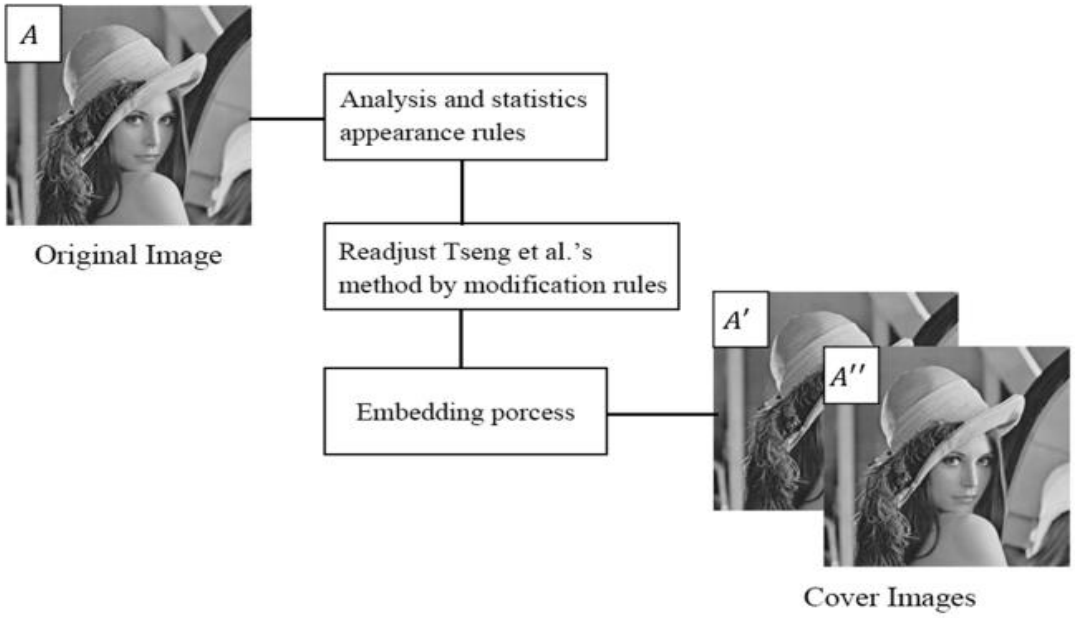


Chart 2. 13 Flowchart of LSB by Lu et al

Source: Lu et al (2021)

2.2.20 Minimal Block Knight's Tour and Edge with LSB Pixel Replacement Based Encrypted Image Steganography

The digital world is increasingly focusing on data security, with cryptography and steganography being widely used. The proposed algorithm uses Knight's Tour Algorithm, a chess move, to perform image encryption and steganography. The minimum block required for a Knight's Tour to reach all squares is a 5x5 block. The generated pattern is used for encryption, which is then embedded into another image and shuffled to obtain a crypto-stego image. This algorithm provides high data security with a good PSNR and SSIM. The encryption process is lossless, involving only replacing pixels without any modification to their value. The encrypted image is embedded into a cover image, which is then shuffled using block shufing or Knight's Tour to obtain a crypto-stego image. This method ensures further security and confidentiality for information in an image with acceptable PSNR and better SSIM.

2.2.21 Triple DES Cryptography Algorithm and LSB Steganography as a Combined Method in Data Security

This journal explores data security in the data communication process. The research uses the Triple DES algorithm to maintain data confidentiality by converting messages into a specific code through encryption three times. The data is then inserted into the LSB (Least Significant Bit) steganography model, which hides the secret message. This combination of cryptographic and steganographic security is expected to make data difficult to crack by unauthorized parties. The study evaluates the performance of the proposed method by measuring file size and encryption-decryption time. The larger the number of encrypted and inserted message characters, the larger the resulting image size. The Triple DES algorithm and LSB steganography provide double security, maintaining data authenticity and allowing only those with the key to access and modify the message.

2.3 Research Framework

Research framework describes the flow of research that begins with input, process, output and ends with research outcomes. This research framework is compiled to facilitate researchers. In the research framework, the input section is a problem identification that is currently happening. From the problem identification, problem formulation will be prepared and supported by theory to conduct research methodology in the process section. The results of the process section provide research outputs and outcomes. The research framework can be depicted in the figure below.

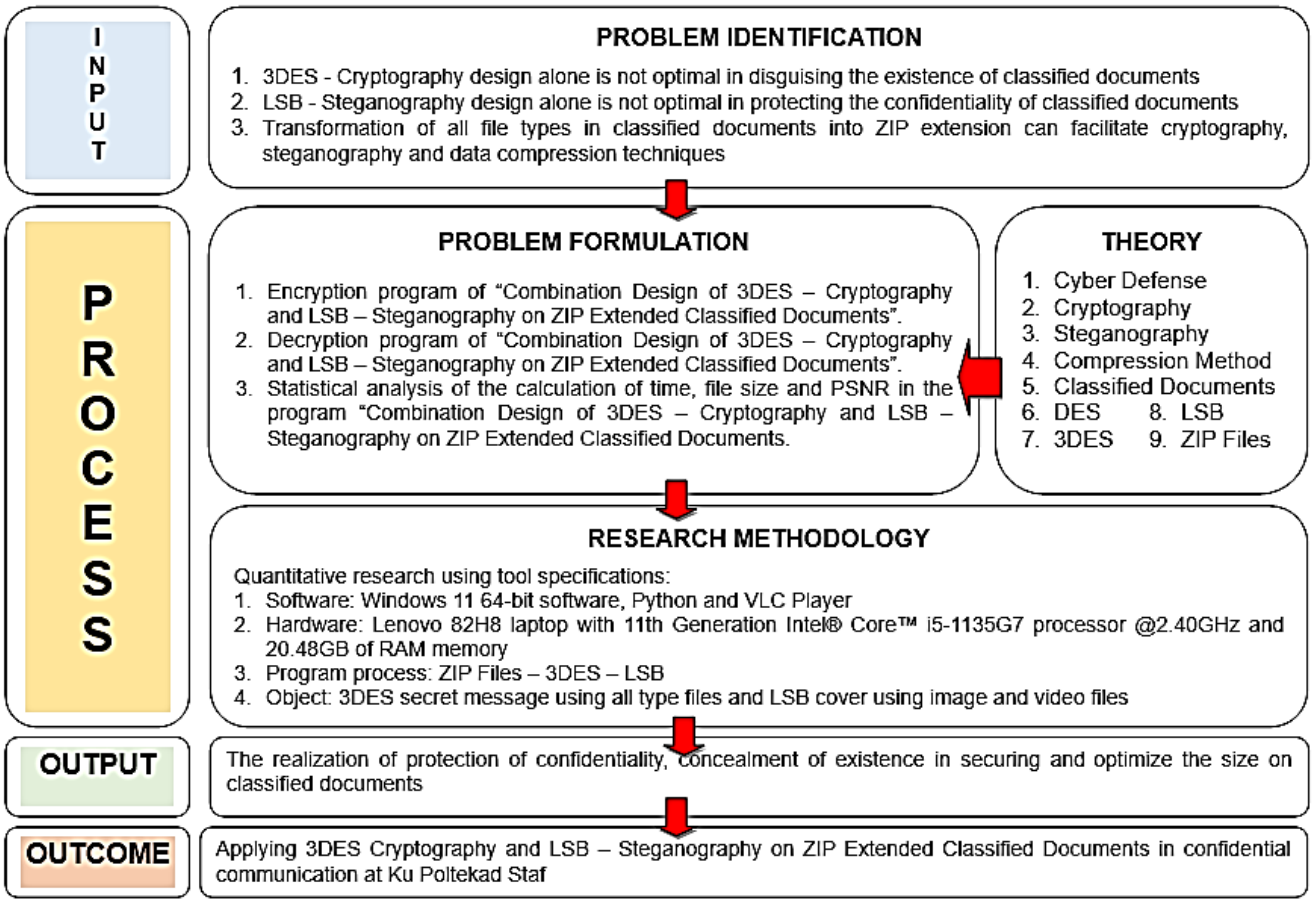


Chart 2. 14 Research Framework

Source: Processed by the Researcher (2024)

2.4 Hypothesis

This research raises temporary hypothesis that are useful as a reference for research is Combination Design of Triple Data Encryption Standard (3DES) – Cryptography and Least Significant Bit (LSB) – Steganography on Zipped Information Package (ZIP) Extended Classified Documents. The success achieved in this research is supported by several calculations, including:

a. Time.

In the encrypt and decrypt program, each time will be measured to run the following processes:

1) ZIP Compression;

2) 3DES Cryptography; and
3) LSB Steganography.

b. File size.

As a result of the encrypt and decrypt programs, we will obtain the file size consisting of:

1) Input message;
2) Cover before stegano;
3) Cover after stegano; and
4) Output message.

c. PSNR

PSNR measurement is done to compare the size of the cover before stegano with the cover after stegano.