

# Data Security Using Color Image Based on Beaufort Cipher, Column Transposition and Least Significant Bit (LSB)

Lekso Budi Handoko\*<sup>1</sup>, Chaerul Umam<sup>2</sup>

*Informatics Engineering, Computer Science Faculty, Dian Nuswantoro University*<sup>\*1,2</sup>

*E-mail : lbudi.handoko@dsn.dinus.ac.id<sup>1</sup>, chaerul@dsn.dinus.ac.id<sup>2</sup>*

*\*Corresponding author*

---

**Abstract** – One of cryptography algorithm which used is beaufort cipher. Beaufort cipher has simple encryption procedure, but this algorithm has good enough endurance to attack. Unauthorized people cannot break up decrypt without know matrix key used. This algorithm used to encrypt data in the form of text called plaintext. The result of this algorithm is string called ciphertext which difficult to understood that can causing suspicious by other people. Beaufort cipher encryption tested with avalanche effect algorithm with modified one, two, three and all key matrix which resulting maximum 31.25% with all key modification so another algorithm is needed to get more secure. Least Significant Bit (LSB) used to insert ciphertext created to form of image. LSB chosen because easy to use and simple, just alter one of last bit image with bit from message. LSB tested with RGB, CMYK, CMY and YUV color modes inserted 6142 characters resulting highest PSNR value 51.2546 on YUV color mode. Applying steganography technique has much advantage in imperceptibility, for example the image product very similar with original cover image so the difference can not differentiate image with human eye vision. Image that tested as much ten images, that consist of five 512 x 512 and five 16 x 16 image. While string message that used is 240, 480 and 960 character to test 512 x 512 image and 24, 48 and 88 character to test 16 x 16 image. The result of experiment measured with Mean Square Error (MSE) and Peak Signal Ratio (PSNR) which has minimum PSNR 51.2907 dB it means stego image that produced hood enough. Computation time calculation using tic toc in matlab resulting fastest value 0.041636 to encrypt 2000 character and the longest time is 4.10699 second to encrypt 6000 character and inserting to image. Amount of character and amount of multi algorithm can affecting computation time calculation.

**Keywords** – cryptography; steganography; beaufort cipher; LSB; avalanche effect, computation time

## 1. INTRODUCTION

The rapid development of technology in recent times allows humans to exchange information quickly and widely. Distance is not an obstacle for humans to exchange information. The media used for exchanging information can be in the form of data, files or files, messages, music, videos, and images. Data is a record of a set of facts. Data in daily use means statements that have been accepted as is. If the data is collected, it will produce information [1]–[4]. Media exchange of information is used because it can simplify and accelerate communication activities. With the smooth communication of humans can solve business, personal, and other matters easily. If the exchange of information by sending data is carried out without securing the data, then the activity of exchanging information can be said to be insecure as shown in Figure 1.

Because the danger of wiretapping can arise anywhere and at any time without the knowledge of the exchanging information. Everyone has their own information; this information can have a level of privacy according to the information owner himself. However, information has become something very valuable. For business people, information can be used to increase business profits. In the military world, information can be priceless. Because it can change the fate of the country that owns the information or seeks the information. For journalists, information is the source of life. Therefore, information can be targeted material for any group. Therefore, security in information is an element that must exist. The security itself basically functions to protect the contents of the information so that anyone who tries to target the information cannot read, change, or transfer ownership and delete it from the original owner.

Data security issues are very important for companies and offices. There is a lot of data related to company secrets, such as employee data, customers, and so on. All this data is usually stored in one place, for example a computer in the office. In general, the computer itself can be given a password in order to limit access rights for unauthorized persons [5]–[9]. However, if there is a smart data manager then that person will double it as a backup in case the main data is accidentally deleted. However, that alone is not enough to secure an important file. Therefore, another way must be added to protect important data or files. Because data confidentiality is mandatory in maintaining data security [5], [6].

Crimes related to security have occurred a lot. Examples of such crimes are hackers or crackers, thieves and intruders of homes or offices, financial security against economic collapse. As a result, there have been so many cases of wiretapping of information that have made researchers think about how to stop it. One way is to encrypt the information file [10]–[13]. The field of cryptography is very suitable for studying encryption and decryption. With encryption, information that is considered important and confidential can be hidden according to the will of the owner of the information.

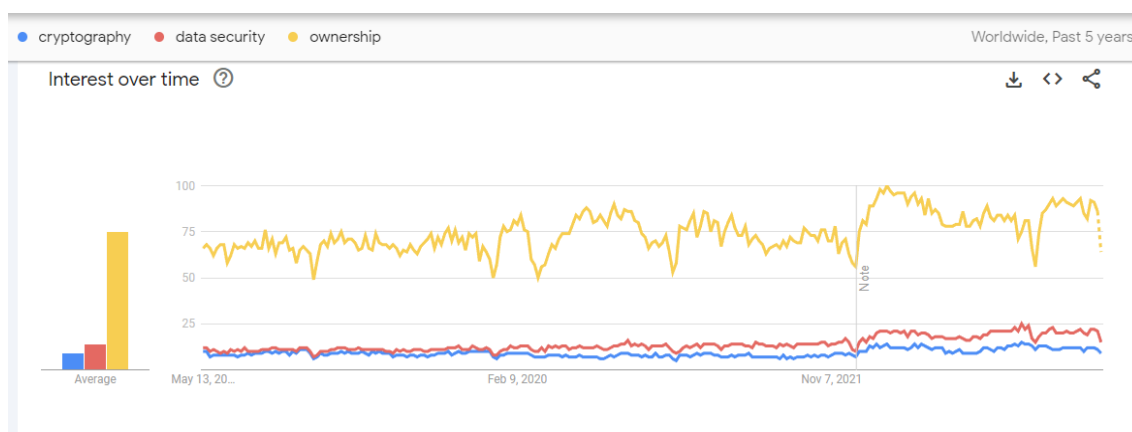


Figure 1. Google trends over cryptography and data security

Based on Figure 1, confidentiality of data or information in two-way communication demands more in terms of security. Then a branch of science was developed that studied the encoding of data and information and became known as Cryptography [14], [15]. Cryptography provides several supporting services in terms of increasing data or information security. Confidentiality is something that is shown to protect information so that it cannot be read or accessed by irresponsible parties. Changing the plaintext or original message into ciphertext or encoded messages is the meaning of the encryption process. To run an encrypted message, someone must have a key or keys. While the meaning of decryption is to change the ciphertext back into plaintext. The key has a secret nature that is only known by the party concerned.

As further information, to reduce or even eliminate suspicion of cryptographic techniques, there is a technique that can be used to hide messages in a medium which is commonly called steganography. In steganography, the media used to hide messages can be images, sounds, text, and others. There is a difference between cryptographic techniques and steganographic techniques, namely messages hidden in a media (cover object) cannot be seen by naked eye if you do not examine carefully that there is data that has been hidden in the message or media. With this technique the level of data security can be increased, sending data or media messages can reach the recipient without anyone being able to intercept the message.

The cryptographic technique that will be implemented in this study is the super encryption technique by combining two techniques in cryptography [13], [16]–[19], namely the substitution technique and the transposition technique. Using beaufort cipher and column transposition as the algorithm. The implementation of cryptographic technology in desktop-based applications was chosen because many users work with computers or laptops so that data or files can be secured using these applications without having to use an internet connection. Using the Java programming language, researchers implement this desktop-based application. The size of the application which tends to be small supports the use of this application. The Beaufort algorithm itself is part of the polyalphabetic cipher where its members include the vigenere cipher, autokey cipher and beaufort cipher. Polyalphabetic cipher operates by substituting letters of the alphabet to perform encryption and decryption [12], [14]. Substitution is the replacement of each letter of the original message (plaintext) with another character [1]. Which means, the substitution technique is one of the symmetric cryptographic techniques in which the way it works is to replace each character of the original message (plaintext) with another object. This technique applies the concept of one-to-one correspondence for each character of the original message (plaintext) that is encoded. As for column transposition, it is a type of algorithm that transposes letters to encrypt or decrypt. Other examples of transposition techniques in cryptography are Rail Fence transposition, Route Transposition, Multiple Transposition, and Myszkowski Transposition [14], [20]. The transposition technique works by creating coded messages (ciphertext) by replacing the positions of the original message objects (plaintext) without replacing or changing the original message (plaintext). In this column transposition technique, matrix reading is done by reading column by column according to the key used. The sorting of the encryption process is also sorted based on the key. The numbering on the keys is carried out in alphabetical order. Which then creates a table with as many rows and columns as the length of the key. Next, the original message (plaintext) is entered into the table. After all the original messages (plaintext) fill the table that has been created, the encryption process can be done.

## **2. RESEARCH METHOD**

---

### *2.1. Steganography*

Steganography is a way to hide messages in other digital content such as images, the video or audio so that they are not visible from outside. The word steganography comes from the Greek word Steganos which means "hidden/veiled" and graphein "to write". This type of steganography provides better security than pure steganography [1], [21]. The main problem with using a steganographic system is key sharing. If thieves know the key, it will be easier to decrypt and access the original information. Steganography is applied to media such as text, images, video clips, music and sound.

The Least Significant Bit (LSB) method is a method of hiding messages or information in a medium, by directly inserting the message into the pixels of the cover image. By modifying a small portion of the bits of each pixel, where the bit position will be replaced by a message that

will be hidden on the selected parent media [18], so that changes that occur in color values do not really affect image quality, this method has good imperceptibility so human vision cannot see image changes [4]. The determination and change of bits are carried out sequentially starting from the first bit to the last bit according to the length of the message to be inserted.

## 2.2. Cryptography

Cryptography covers many things in its application media. Applications and methods used have also developed widely. As in the image that has changed the RGB arrangement so that changing the encrypted image will not be visible to the naked eye. The image will return to its original state if it is decrypted with the key that was also used during encryption as shown in Figure 2. The key in the image decryption encryption process can be either an image or text and number. The essence of the process of encrypting a media is randomizing what is contained in the media. For example, text encryption, randomization occurs in the text by using a key. The key is a mandatory component in the encryption and decryption process. Another example on document file encryption and decryption. Documents that have been encrypted will result in not being able to open the document. Because there has been randomization of the arrangement of bits in the document. In this case the document in question can be in .pdf , .doc and .xls format.

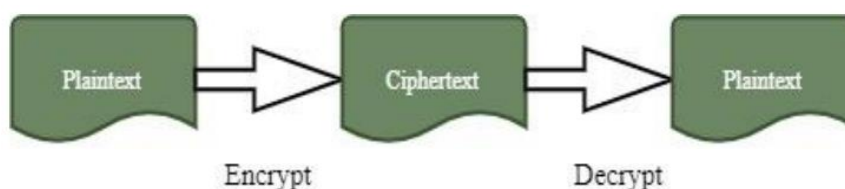


Figure 2. Common Cryptography Scheme

Beaufort cipher is a type of polyalphabetic cipher. As the name suggests, the Beaufort chipper was invented by Sir Francis Beaufort. The Beaufort cipher is almost the same as the Vigenere cipher, the difference is that the Beaufort cipher has the alphabetical order B~Z in the reverse ciphertext. Encryption with Beaufort can be completed with tabula recta tables. To solve a problem about encrypting with a Beaufort cipher we have to create a column where the upper header is filled with letters of the alphabet, then the side header is filled with a key (key) with double letter omissions. The key (key) is translated along the plaintext letters.

The column transposition method is also a classic cryptography. Classical cryptography is divided into two types, namely substitution cryptography and transposition cryptography, column transposition codes are included in transposition cryptography. Encryption techniques in transposition cryptography by changing the location of the message text to be encoded. Then to re-read the method by returning the location of the original message based on the agreed key and letter transposition algorithm. Column transposition encodings are written inline as usual with a predefined key length. Then the keys that have been determined are numbered in alphabetical order, if the letter is a then the number sequence is 1 and then so on. The next process is to write Plaintext along the key and number the columns according to the number on the key. The results are written according to the column number with a space to mark the column displacement. Another name for this method is permutation or scrambling because transposing each character or letter in the text is the same as permuting these characters.

## 2.3. Evaluations Method

To find out the advantages and disadvantages of a study, a method test was carried out. An image is tested to find out how good the image quality is with MSE (Mean Square Error) and

PSNR (Peak Signal Noise Ratio) measuring instruments. Mean Square Error is a measurement tool to test the quality of the image by measuring the average squared cumulative error between the stego and the original image [1], [22]. Error indicates distortion or deviation in the image, calculated by the formula:

$$MSE = \left(\frac{1}{mn}\right)^2 \sum_{i=1}^M \sum_{j=1}^N (X_{ij} - Y_{ij})^2$$

Information :

MSE = Mean Square Error

M = Row matrix

N = Column matrix

X<sub>ij</sub> = The value of the pixels in the cover image

Y<sub>ij</sub> = The value of the pixels in the stego image

Peak Signal to Noise Ratio is the ratio of the maximum value of the measured signal to the noise that affects the signal, PSNR is used to determine the ratio of the maximum value of the measured signal to the amount of noise that affects the signal [23]. PSNR is used to express image quality, it can be calculated by the formula:

$$PSNR = 10 \log \frac{255^2}{MSE}$$

Information :

PSNR = Peak Signal to Noise Ratio

dB = deciBell

MSE = Mean Square Error

Entropy is a random concept where there are states of uncertain probability. The definition of entropy related to information theory is a measure that expresses the amount of information in a message [24]. Expressed in bits. Useful for encoding message elements, can be calculated by the formula:

$$H_c = - \sum_{k=0}^n P(k) \log_2 (P(k))$$

Information :

H<sub>e</sub> = Entropy

n = Number of distinct symbols in the message, on

image n is the gray value of the image

P<sub>k</sub> = Probability of occurrence of symbol k

#### 2.4. Proposed Method

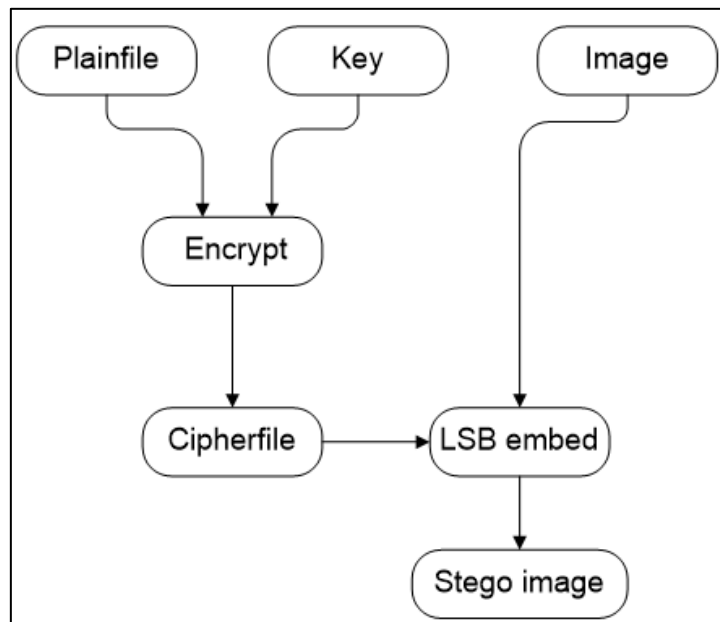


Figure 3. Propose encrypt-embed beaufort cipher-column transposition and LSB

Based on Figure 3, the following are the steps for the encryption and embedding process:

1. Enter the plaintext and key to be hidden.
2. After entering the plaintext and key, the encryption process will be carried out with the beaufort cipher.
3. After being encrypted, it will generate ciphertext to be included in the image.
4. The embedding process will be carried out using the LSB algorithm and generate a stego image.

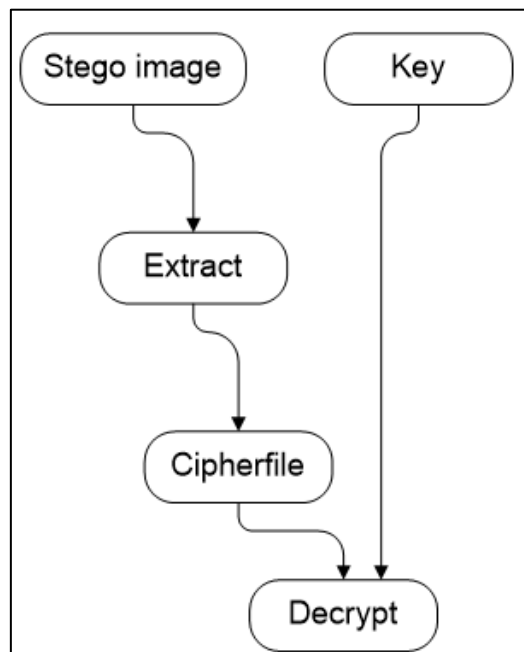


Figure 4. Proposed decrypt-extract beaufort cipher-column transposition and LSB











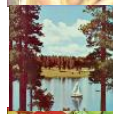
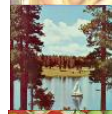


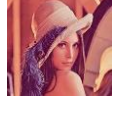
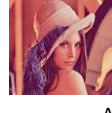
The following are the steps for the extract and decrypt process:

1. Enter the stego image to carry out the extraction process.
2. After the extract is complete it will generate ciphertext.
3. The decrypt process will be carried out by entering the key.
4. After the decrypt process is complete, it will generate plaintext using the beaufort cipher.

### 3. RESULTS AND DISCUSSION

The results of tests carried out on RGB, CMYK, CMY and YUV images produced images according to Table 1. The results of the avalanche effect test that the researcher did with the plain text "udinus" and "polkee" are shown in Table 2. Based on Table 1, it had been seen that the best PSNR value is in an image that has a YUV color space when the four images are tested by inserting a message of 6142 characters out of the maximum 6144 characters that can be accommodated by an image. Based on Table 2, the PSNR value will be smaller because the more messages are inserted, the more bits are changed in the cover image. In an image measuring 512 x 512 which can accommodate messages of 98112 characters, when inserting messages of 240 characters the average PSNR obtained is 77.1968 dB, when inserting messages of 480 characters the average PSNR is 74.2214 dB and 71.3807 for the average PSNR which is obtained when inserted 960 characters. From these results, the PSNR value remains above 40 dB, which means that the quality of the stego image created is very good as shown in Table 4.

Table 1. MSE, PSNR and Entropy using 128x128 pixels and 512x512 pixels

Name file	Cover	Stego file	Image size (in pixels)	Maximum inserted (in bit)	Message (in character)	MSE	PSNR (in dB)	Entropy
a			128x128	6144	6142	0,4922	51,2091	7,0547
b						0,4916	51,2141	7,2053
c						0,5037	51,1084	7,0662
d						0,4871	51,2546	7,0812
		Average				0,4937	51,1966	7,1018
e			512x512	98112	240	0,0024	74,2930	6,4288
f						0,0026	74,0511	6,6640
g						0,0024	74,2794	7,7639
h						0,0024	74,3760	7,6710
		Average				0,0025	74,1076	5,7058










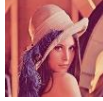










j						0,0024	74,2930	6,4288
k						0,0026	74,0511	6,6640
l			512x512	98112	480	0,0024	74,2794	7,7639
m						0,0024	74,3760	7,6710
n						0,0025	74,1076	5,7058
	Average					0,0025	74,2214	6,8467
o						0,0048	72,2486	6,4288
p						0,0050	71,1280	6,6639
q			512x512	98112	960	0,0049	71,2148	7,7638
r						0,0048	71,2725	7,6709
s						0,0051	71,0398	5,7246
	Average					0,0049	71,3807	6,8504

Table 2. Evalache Effect

No	Key	Plain Text	Cipher Text	Changing bit	AE
1	23,14	udinus polkee	xgdiqoutazie	14	14,58%
2	13,14 15,16 17,16	udinus polkee	dgviwoftpzee jmvigyhvjtyc pmviqyjvdtgc	14	14,58%
3	23,14 23,35	udinus polkee	xgdiqoutazie xxdlquulafug	19	18,27%
4	01,13 12,13	udinus polkee	ddnsvswofkpeq adivewrffpmq	16	16,67%
5	01,19 12,49	udinus polkee	dvnsaolkxao aditeirefema	29	30,21%
6	71,10 74,53	udinus polkee	nuricuppjlge wfebeyfnnhsg	29	30,21%
7	23,14 74,53	udinus polkee	xgdiqoutazie wfebeyfnnhsg	30	31,25%
8	23,35 71,10	udinus polkee	xxdlquulafug nuricuppjlge	26	27,08%



Table 3. MSE, PSNR, Entropy using 16x16 pixels images



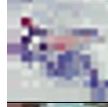
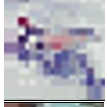
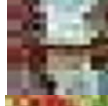
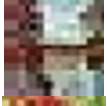
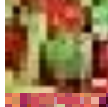



File name	Cover	Stego file	Max = 90, Message = 25 character			Max = 90, Message = 48 character			Max = 90, Message = 88 character		
			MSE	PSNR	Entropy	MSE	PSNR	Entropy	MSE	PSNR	Entropy
			a			0,1276	57,0220	6,5723	0,2656	53,8881	6,6149
b			0,1484	56,4154	6,6800	0,2591	53,9959	6,6788	0,4804	51,3142	6,6608
c			0,1367	56,7725	7,4858	0,2382	54,3599	7,4869	0,4661	51,4456	7,4787
d			0,1549	56,2289	7,5549	0,2813	53,6399	7,6399	0,5065	51,0849	7,5189
e			0,1367	56,7725	7,4824	0,2852	53,5800	7,4941	0,4804	51,3142	7,5128
Average			0,1409	56,6423	7,1551	0,2659	53,8928	7,1829	0,4822	51,2993	7,1567

Table 4. PSNR standard value [13], [23], [25]

PSNR (dB)	Image Quality
60	Very good (no noise)
50	Good (there is some noise but the image quality is still good.)
40	Fairly good (there is fine grain or snow in the image)
30	Not good (there is a lot of noise)
20	Not good (unusable)

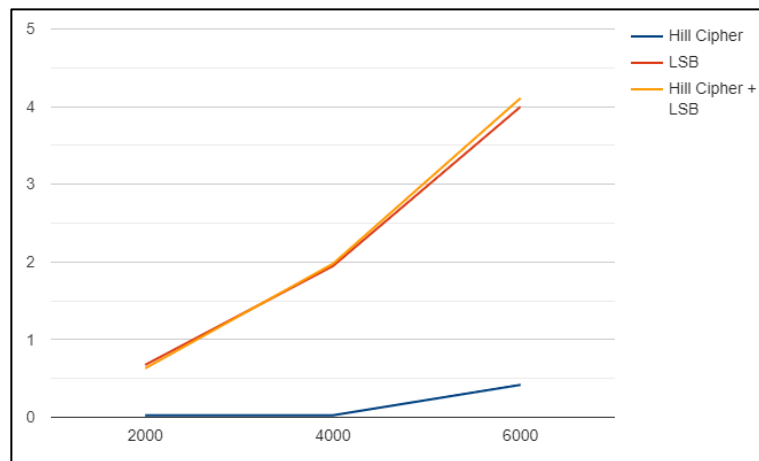


Figure 5. Graphic Time Execution

Based on Table 5, the computation time testing using the tic toc function uses a lenna.png image measuring 128 x 128 which can accommodate 6096 message characters and is tested with message strings of 2000, 4000 and 6000 characters. There are 3 methods tested computationally, namely the Beaufort Cipher, Column Transposition, and LSB. Test results in units of seconds (seconds) as shown in Table 5 and Figure 5.

Table 5. Comparison result between Beaufort, Column Transposition, LSB and it combination

Mwthod	Image Size	Max	Message	Time Execution (in second)
	-	-	2000	0.025148
Beaufort Cipher +	-	-	4000	0.025587
Column	-	-	6000	0.041636
Transposition	128x128	6096	2000	0.673335
LSB	128x128	6096	4000	1.947807
	128x128	6096	6000	3.996231
	128x128	6096	2000	0.628808
Beaufort Cipher +	128x128	6096	4000	1.975124
Column Transposition	128x128	6096	6000	4.10699
+ LSB				

#### 4. CONCLUSION

Based on experiment result, it can be concluded that the file encryption application uses super encryption which was developed to add to the personal security system, can encode with two methods at once. The process of encoding files with the super encryption method has been carried out with a combination of LSB to obtain high imperceptibility. The impercept value is described through MSE and PSNR, which in this study obtained a value of more than 50 dB, while the entropy value of all data was close to 8. In future research, additional media files can be used with larger sizes so that they are more diverse in applying the super encryption method based on LSB. Another option that can be done is to increase the number of encoded files in one task at once in order to shorten the time, making it easier to remember the key, the encryption key can be stored in text form. Pada penelitian yang akan datang, dengan tujuan untuk memperbaiki hasil maka dapat dilakukan eksperimen dengan dataset citra berukuran lebih besar dari 1024 atau 2048 piksel.

#### REFERENCES

- [1] K. R. Ilaga and C. A. Sari, "Analysis of Secure Image Crypto-Stegano Based on Electronic Code Book and Least Significant Bit," *Journal of Applied Intelligent System*, vol. 3, no. 1, pp. 28–38, 2018.
- [2] A. K. Sadasivuni, A. Chandrasekhar, D. Chaya, K. 2#, and S. A. Kumar, "SYMMETRIC KEY CRYPTOSYSTEM FOR MULTIPLE ENCRYPTIONS," *International Journal of Mathematics Trends and Technology*, [Online]. Available: <http://www.ijmtjournal.org>
- [3] J. P. Sermeno, K. A. S. Secugal, and N. E. Mistio, "Modified Vigenere cryptosystem: An integrated data encryption module for learning management system," *International Journal of Applied Science and Engineering*, vol. 18, no. 4(Special Issue), pp. 1–10, 2021, doi: 10.6703/IJASE.202106\_18(4).003.
- [4] O. F. AbdelWahab, A. I. Hussein, H. F. A. Hamed, H. M. Kelash, and A. A. M. Khalaf, "Efficient Combination of RSA Cryptography, Lossy, and Lossless Compression Steganography Techniques to Hide Data," *Procedia Comput Sci*, vol. 182, pp. 5–12, 2021, doi: 10.1016/j.procs.2021.02.002.
- [5] G. Swain and A. K. Sahu, "Data hiding using adaptive LSB and PVD technique resisting PDH and RS analysis," *International Journal of Electronic Security and Digital Forensics*, vol. 11, no. 4, p. 458, 2019, doi: 10.1504/IJESDF.2019.10021739.
- [6] D. Suprihant *et al.*, "Combination Vigenere Cipher and One Time Pad for Data Security," *International Journal of Engineering & Technology*, vol. 7, no. 2, pp. 92–94, 2018.
- [7] R. Verma, A. Kumari, A. Anand, and V. S. S. Yadavalli, "Revisiting Shift Cipher Technique for Amplified Data Security", doi: 10.47852/bonviewJCCE2202261.

- [8] R. Verma, A. Kumari, A. Anand, and V. S. S. Yadavalli, "Revisiting Shift Cipher Technique for Amplified Data Security," *Journal of Computational and Cognitive Engineering*, 2022, doi: 10.47852/bonviewJCCE2202261.
- [9] E. Irfan Riaz Shohab Sandhu *et al.*, "An Enhanced Vigenere Cipher For Data Security," *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, vol. 5, no. 03, 2016, [Online]. Available: [www.ijstr.org](http://www.ijstr.org)
- [10] E. W. Abood *et al.*, "Audio steganography with enhanced LSB method for securing encrypted text with bit cycling," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 1, pp. 185–194, Feb. 2022, doi: 10.11591/eei.v11i1.3279.
- [11] B. B. Ahamed and M. Krishnamoorthy, "SMS Encryption and Decryption Using Modified Vigenere Cipher Algorithm," *Journal of the Operations Research Society of China*, Aug. 2020, doi: 10.1007/s40305-020-00320-x.
- [12] M. Fadlan, Suprianto, Muhammad, and Y. Amaliah, "Double layered text encryption using beaufort and hill cipher techniques," in *2020 5th International Conference on Informatics and Computing, ICIC 2020*, Nov. 2020. doi: 10.1109/ICIC50835.2020.9288538.
- [13] E. J. Kusuma, O. R. Indriani, C. A. Sari, E. H. Rachmawanto, and D. R. I. M. Setiadi, "An imperceptible LSB image hiding on edge region using DES encryption," in *2017 International Conference on Innovative and Creative Information Technology (ICITech)*, Nov. 2017, pp. 1–6. doi: 10.1109/INNOCIT.2017.8319132.
- [14] C. Irawan, E. H. Rachmawanto, C. A. Sari, and C. A. Sugianto, "SUPER ENKRIPSI FILE DOKUMEN MENGGUNAKAN BEAUFORT CIPHER DAN TRANSPOSISI KOLOM," in *Semnas LPPM UMP*, 2020, pp. 556–563.
- [15] C. A. Sari, G. Ardiansyah, D. R. I. Moses Setiadi, and E. H. Rachmawanto, "An improved security and message capacity using AES and Huffman coding on image steganography," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 17, no. 5, pp. 2400–2409, 2019, doi: 10.12928/TELKOMNIKA.v17i5.9570.
- [16] E. H. Rachmawanto and C. A. Sari, "KEAMANAN FILE MENGGUNAKAN TEKNIK KRIPTOGRAFI SHIFT CIPHER," *Techno.COM*, vol. 14, no. 4, pp. 329–335, 2015.
- [17] C. A. Sari, T. S. Sukamto, D. Eko, and H. Rachmawanto, "ANALISA ROBUSTNESS CITRA DIGITAL PADA WATERMARKING DCT-DWT," in *ProsidingSNST ke-9Tahun2018*, 2018, pp. 19–22.
- [18] H. K. Ronaldo Cahyono, C. Atika Sari, D. R. Ignatius Moses Setiadi, and E. Hari Rachmawanto, "Dual Protection on Message Transmission based on Chinese Remainder Theorem and Rivest Cipher 4," in *2019 International Conference on Information and Communications Technology (ICOIACT)*, Jul. 2019, pp. 74–78. doi: 10.1109/ICOIACT46704.2019.8938568.
- [19] E. H. Rachmawanto, K. Prasetyo, C. A. Sari, I. M. S. de Rosal, and N. Rijati, "Secured PVD Video Steganography Method based on AES and Linear Congruential Generator," in *2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, Nov. 2018, pp. 163–167. doi: 10.1109/ISRITI.2018.8864466.
- [20] L. B. Handoko and A. D. Krismawan, "SUPER ENCRYPTION APPLICATION OF CRYPTOGRAPHY USING COMBINATION OF COLUMNAR TRANSPOSITION AND VIGENERE CIPHER," in *Seminar Nasional LPPM UMP*, 2020, pp. 534–539.
- [21] K. A. Darabkh, "A New Steganographic Algorithm Based on Multi Directional PVD and Modified LSB," *Information Technology And Control*, vol. 46, no. 1, pp. 16–36, Apr. 2017, doi: 10.5755/j01.itc.46.1.15253.
- [22] S. Bukhari, M. S. Arif, M. R. Anjum, and S. Dilbar, "Enhancing security of images by Steganography and Cryptography techniques," in *2016 Sixth International Conference on*

- Innovative Computing Technology (INTECH)*, Aug. 2016, pp. 531–534. doi: 10.1109/INTECH.2016.7845050.
- [23] D. Tao, S. Di, X. Liang, Z. Chen, and F. Cappello, “Fixed-PSNR Lossy Compression for Scientific Data,” May 2018, [Online]. Available: <http://arxiv.org/abs/1805.07384>
- [24] X. Zhang, L. Wang, G. Cui, and Y. Niu, “Entropy-Based Block Scrambling Image Encryption Using DES Structure and Chaotic Systems,” *Int J Opt*, vol. 2019, pp. 1–13, Aug. 2019, doi: 10.1155/2019/3594534.
- [25] D. N. Aini, D. R. I. Moses Setiadi, S. N. Putro, E. H. Rachmawanto, and C. A. Sari, “Survey of Methods in the Spatial Domain Image Steganography based Imperceptibility and Payload Capacity,” in *2019 International Seminar on Application for Technology of Information and Communication (ISEMANTIC)*, Sep. 2019, pp. 434–439. doi: 10.1109/ISEMANTIC.2019.8884333.