ICOMITEE 2021
PROGRAM BOOK

The 2021 International Conference on Computer Science, Information Technology and Electrical Engineering (ICOMITEE)

October
27th – 28th, 2021
El Hotel Royale, Banyuwangi

Co-Host :

Sponsorship :

HALAMAN PENGESAHAN

Judul	:	*Combination of Modified LSB Steganography and Huffman Compression for Data Security*
Penulis	:	Dedi Darwis, Adhie Thyo Priandika, Ade Surahman, A. Ferico Octaviansyah Pasaribu, **Akmal Junaidi**, Wamiliana
NIP	:	19710129 199702 1 001
Instansi	:	Jurusan Ilmu Komputer, Fakultas MIPA, Universitas Lampung
Publikasi	:	2021 International Conference on Computer Science, Information Technology, and Electrical Engineering (ICOMITEE), 27-28 Oktober 2021
		ISBN : 978-1-6654-0147-0
		Page 218-224
Penerbit	:	IEEE Computer Society

Bandar Lampung, Desember 2021

Mengetahui,
Dekan FMIPA Universitas Lampung

Penulis,

Dr. Eng. Suripto Dwi Yuwono, M.T.
NIP. 19740705 200003 1 001

Dr. rer. nat. Akmal Junaidi, M.Sc.
NIP. 19710129 199702 1 001

Menyetujui,
Ketua Lembaga Penelitian dan Pengabdian kepada Masyarakat
Universitas Lampung

Dr. Ir. Lusmeilia Afriani, D.E.A.
NIP. 19650510 199303 2 008

CONFERENCE PROGRAM BOOK

2021 International Conference on Computer Science, Information Technology, and Electrical Engineering
(ICOMITEE 2021)

October 27th - 28th, 2021
Banyuwangi, Indonesia

ICOMITEE 2021 Partners and Supporters

Organizer:

Technical Co-Sponsorship:

Co-Organizers:

2021 International Conference on Computer Science, Information Technology, and Electrical Engineering (ICOMITEE) | 978-1-6654-0147-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICOMITEE53461.2021.9650124

2021 International Conference on Computer Science, Information Technology, and Electrical Engineering (ICOMITEE)

2021 International Conference on Computer Science, Information Technology, and Electrical Engineering (ICOMITEE) took place 27-28 October 2021 in Banyuwangi, Indonesia.

IEEE catalog number:	CFP21U07-ART
ISBN:	978-1-6654-0147-0

2021 International Conference on Computer Science, Information Technology, and Electrical Engineering (ICOMITEE) | 978-1-6654-0147-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICOMITEE53461.2021.9650247

PROCEEDINGS

2021 International Conference on Computer Science, Information Technology, and Electrical Engineering (ICOMITEE 2021)

ISBN : 978-1-6654-0146-3 (USB, Part Number: CFP21U07-USB)
ISBN : 978-1-6654-0147-0 (XPLORE COMPLIANT, Part Number: CFP21U07-ART)

Additional copies may be ordered to:
Faculty of Computer Science
University of Jember
Jl. Kalimantan no.37, Kampus Bumi Tegalboto, Sumbersari, Jember, 68121
+62331 - 326935

Foreword from Conference Chair of ICOMITEE 2021

In the name of Allah, the Most Beneficent and the Most Merciful.

On behalf of the organizing committees, I would like to welcome all of you to Banyuwangi, Indonesia for the 2021 International Conference on Computer Science, Information Technology and Electrical Engineering (ICOMITEE).

2021 has been a very challenging year due to the COVID-19 pandemic. With the safety and well-being of our participants as our top priority, ICOMITEE, originally planned to be hold in Banyuwangi, Indonesia, has been converted to a hybrid conference. Nevertheless, while we may all be physically distant, we hope we can still connect intellectually. I would like to express my hearty gratitude to all participants for sharing and presenting your experiences in this hybrid conference. Only high-quality selected papers are accepted to be presented in this event, so we are also thankful to all the international reviewers and steering committee for their valuable works. I would like to give a compliment to all partners in publications and sponsorships for their valuable supports.

ICOMITEE 2021 is the international conference hosted by University of Jember (UNEJ), co- hosted by Nahdlatul Ulama University of Surabaya (UNUSA), Teknokrat Indonesia University and Banyuwangi State Polytechnic. ICOMITEE 2021 is officially approved by IEEE Indonesia Section and IEEE

Indonesia Computer Society Chapter for technical co-sponsored.

This event is intended to provide technical forum and research discussion related to advance engineering on electrical & electronics, computer science and informatics. The Conference is aimed to bring researchers, academicians, scientists, students, engineers and practitioners together to participate and present their latest research finding, developments and applications related to the various aspects of Information System Management, Data Analytics & Big Data, IT Infrastructure and Security, Electrical and Telecommunication

Allow me to express my deepest gratitude to those who have made this conference possible. My thanks go to the Rector of the University of Jember. I would also like to thank the invited speakers: Prof. Md Saidur Rahman from Bangladesh University of Engineering and Technologi, Prof. Anton Satria Probuwono from King Abdulaziz University and Assoc. Prof. Dr. Ford Lumban Gaol from IEEE Indonesia Computer Society Chapter for accepting our invitation in the conference.

At this conference, the committee received total 77 full manuscripts from various cities in Indonesia and abroad such as China, Malaysia, Ireland, Australia, Poland, Srilanka, Kazakhstan, and India. But, after the review process, 38 full manuscripts were accepted.

I also want to thank and appreciate to all committee members, all TPC Sponsors and Financial Sponsors, all TPC members, and 393 high reputable reviewers from various countries, for all your dedications to the ICOMITEE 2021.

I look forward to having a successful conference, and we hope that all the attendees enjoy and get benefits from this conference.

Prof. Saiful Bukhori ST., M.Kom.
Conference Chair of ICOMITEE 2021

Foreword from IEEE Indonesia Section

Dear distinguished guests, keynote speakers, colleagues, researchers, professionals, ladies and gentlemen, good morning, a prosperous, warm, and spirited greeting.

On behalf of IEEE Indonesia Section, we would like to extend our warmest welcome to all keynote speakers, presenters, and participants to the 2021 International Conference on Computer Science, Information Technology and Electrical Engineering (ICOMITEE). The conference aims to bring together researchers and experts in information systems to share their ideas, experiences and insights. The conference is organized by Universitas Jember (UNEJ) and technically co-sponsored by IEEE Indonesia Section.

IEEE Indonesia Section has conducted many activities over 33 years in Indonesia. IEEE Indonesia has more than 2,600 members and more than 50 senior members from industry professionals, academia and government. In terms of collaboration, IEEE Indonesia section has a good and mutual relationship with ICT organizations, Industries, Government, Universities as well as the Community in Indonesia. IEEE Indonesia also sponsors more than 50 high quality international conferences indexed by Scopus every year held by various universities in Indonesia. Since its formation in 1988, IEEE Indonesia has sponsored the publication of more than 20,000 publications of IEEE international conferences and more than 260 publications of IEEE international journals by Indonesian authors.

The ICOMITEE shows its sustainability due to the hard work of the conference organizers, well organized conference and high quality papers. We do hope in the near future some high quality conferences will be continued and strengthened, so the result will give more benefit and positive impact to the human being, especially to Indonesian people.

In this occasion, I would also like to say welcome to Banyuwangi, which serves beautiful heritages, culture, with warm, polite and friendly people, a vibrant culture and lifestyle.

Finally, we do hope all of you will have enjoyable and valuable experience during this event. You may share your best knowledge in your area of research and professional activities.

Thank you.

Dr. Ing. Wahyudi Hasbi
Chairman, IEEE Indonesia Section

Foreword from IEEE Computer Society Chapter

Greetings!

It is our great pleasure and honor to welcome you to The 2021 International Conference on Computer Science, Information Technology, and Electrical Engineering (ICOMITEE) that will be held in El Royal Hotel Banyuwangi, 27-28 Oktober 2021.

In this event we will have the opportunities to exchange knowledge and information on latest researches and strengthening relationships amongs us, while enjoying the relaxing yet entertaining environment of Banyuwangi.

ICOMITEE is the international conference that will be held on the Faculty of Computer Science, University of Jember that collaborate with IEEE (Institute of Electrical and Electronics Engineers) Indonesia Section & IEEE Computer Society Indonesia Chapter.

The accepted papers will be published and presented Paper on the IEEE Xplore that will be indexed in SCOPUS.

Previously, ICOMITEE already held on October 2019 with the number of articiles with 84 papers from 4 countries, that already held with Blind-Review by more than 300 reviewers

Thank you

Dr Ford Lumban Gaol
IEEE Computer Society Chapter - Chair
Bina Nusantara University, Indonesia

Foreword from Rector of University of Jember

In the name of Allah, the Most Gracious and the Most Merciful.

First of all, I would like to welcome you all to the University of Jember, Indonesia. I am delighted to have you here to participate and attend the 2021 International Conference on Computer Science, Information Technology, and Electrical Engineering (ICOMITEE 2021). Thank you for joining and participating in the present conference that held in Banyuwangi during 27-28 October 2021

As almost occurring in every country, the COVID-19 outbreak resulted in a hard impact on some human development aspects, including human health, education, research, and social-economic. This situation has forced us to find an innovative and creative way in adapting the running situation, including how we carry out the international conference without interfering the participants health and safety. Therefore, this conference has been changed into hybrid method in order to harmonize between the continuation of conference agenda and the currently COVID-19 pandemic situation worldwide.

The conference is aimed to provide a forum for presentation and discussion among academics, researchers, and policymakers in this region relating to the current progresses in some topics like telecommunication, electrical, data analytics & big data, IT infrastructure & security, also management information system. I expect that all scientific papers resulted in and shared during this conference will

inspire us to be more productive in this field and also enable further improvement of our work.

The hard work and valuable contributions of both the organizing and scientific conference committee members have made this conference organization possible. I thank everybody who in one way or other has contributed to make this international conference a success. Additional thanks is also delivered to our sponsors (IEEE Indonesian Section and IEEE Computer Society Indonesian Chapter) for providing support and assist us for this conference.

Dr. Ir. Iwan Taruna, M.Eng, IPM.
Rector of University of Jember,
Indonesia

2021 International Conference on Computer Science, Information Technology, and Electrical Engineering (ICOMITEE) | 978-1-6654-0147-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICOMITEE53461.2021.9650337

Table of Contents

Combination of Modified LSB Steganography and Huffman Compression for Data Security

Dedi Darwis
Faculty of Engineering and Computer Science
Universitas Teknokrat Indonesia
Bandar Lampung, Indonesia
darwisdedi@teknokrat.ac.id

Adhie Thyo Priandika
Faculty of Engineering and Computer Science
Universitas Teknokrat Indonesia
Bandar Lampung, Indonesia
adhie_thyo@teknokrat.ac.id

Ade Surahman
Faculty of Engineering and Computer Science
Universitas Teknokrat Indonesia
Bandar Lampung, Indonesia
adesurahman@teknokrat.ac.id

A. Ferico Octaviansyah Pasaribu
Faculty of Engineering and Computer Science
Universitas Teknokrat Indonesia
Bandar Lampung, Indonesia
fericopasaribu@teknokrat.ac.id

Akmal Junaidi
Department of Computer Science
Universitas Lampung
Bandar Lampung, Indonesia
akmal.junaidi@fmipa.unila.ac.id

Wamiliana
Department of Mathematics
Universitas Lampung
Bandar Lampung, Indonesia
wamiliana.1963@fmipa.unila.ac.id

***Abstract*— This paper was carried out on the basis of the need for data security on digital media in the form of methods that can help secure confidential data so that confidential data can only be read by the desired person and to anticipate that the data is not read by unauthorized persons. This paper suggests the use of steganography techniques in securing messages, where confidential messages will be inserted into the cover image. The method in this paper uses a combination of two methods, namely the Huffman method for data compression and the Least Significant Bit (LSB) method as a method in Steganography. The Huffman method is used to compress the data before it is inserted into the cover image so that it can reduce the size of the data to be inserted, and the resulting stego image does not change significantly. The results of the experiments carried out, message insertion without using Huffman compression, resulted in an average MSE value of 1.25 and an average PSNR value of 42.35 . Meanwhile, the results of the combination of LSB and Huffman compression methods can produce an average MSE value of 0.37 and an average PSNR value of 53.96.**

Keywords*— Compression, Huffman, LSB, MSE, PSNR, Steganography

I. INTRODUCTION

In today's digital era, the issue of data security and confidentiality is one of the important aspects of information[1],[2]. With the development of illegal wiretapping techniques, many parties try to access information that is not their right[3]. For example, important information in the fields of education, health, business and government agencies can be a threat to information security, especially on data communication media that are very popular today, such as chat applications, e-mail, social media and other applications[4],[5]. The exchange of information through the internet has many advantages, one of which is the speed in delivery, but on the other hand, delivery via the internet has disadvantages, namely cybercrime such as wiretapping, data changes and others[6],[7]. So, it is necessary to secure information using one of the techniques that have been widely used, namely Steganography.

Steganography is the science or art of hiding messages involving a medium. First, a message is needed that is hidden in a certain medium. The media can be in the form of images, sounds, text and others, which are commonly called Steganographic Covers. Second, it is related to sending a cover where a message has been inserted to the recipient without raising suspicion, and the recipient can retrieve the message. The application of Steganography can be used in digital technology such as audio, images, video and any files stored in bits[8],[9],[10]. In this paper, we use the Least Significant Bit (LSB) method, which is a method that is not too complex but can accommodate messages on a cover image with fairly large size. The basis of this method is binary-based numbers, namely the numbers 0 and 1, because digital data is an array of numbers 0 and 1, so the process of application is easy. This method relates to the size of 1 bit and the size of 1 byte, i.e., every 1 byte of data consists of 8 data bits and the bit in the rightmost position, or the last bit is called LSB[11]. The LSB method is proven to produce a fairly good stego-image quality with an average of >= 40db, and the LSB method can also overcome some robustness problems in Steganography [12].

In this paper, the focus of the work carried out is how to increase the message storage capacity of the LSB. Thus, if the message that is inserted into the cover image is large, the large message can be compressed before being embedded in the cover image. The number of message characters or information that can be accommodated on the cover image will be related to the pixel size of the cover image, and if the message size is too large, the cover image will undergo changes that are too significant, making other parties' suspicious Secret messages also cannot be accommodated if the message size is too large. Overcoming this problem can be solved by compressing the message size before the embedded message process using one of the Huffman data compression techniques, namely the process of compressing large messages so that they become smaller[13],[14]. Data compression aims to compress data so that its size becomes smaller so that the data to be inserted is getting smaller. In the process, the Huffman method in compressing data using a statistical approach and the results of the compression carried out is large enough to produce a relatively smaller file size [15],[16].

978-1-6654-0147-0/21/$31.00 ©2021 IEEE

The purpose of this research is to combine LSB steganography technique with Huffman compression. With the combination of these two methods, it is expected that there will be more messages inserted into the cover image, even though the cover image is of a small size. In addition, it is hoped that this combination of methods can improve image quality from the fidelity aspect. So, it can be a recommendation in securing information that is relatively large in size but still produces a good quality stego-image.

II. RELATED WORK

In [17] author, the confidential data is compressed using the Lempel Ziv Welch (LZW) technique before the message is inserted into the cover image. In the compression and decompression process, a key that has been encrypted using RSA is inserted to make the compressed message more secure. The process of inserting a message using is done by taking the input matrix and then detecting the edges of the image to insert the message. Each pixel in an RGB image has a size of 24 bits, namely 8 bits for red, 8 bits for green, and 8 bits for blue. The message is inserted at the edge of the image so that it is not easily detected by the Human Visual System (HVS). The image quality produced from the combination of compression and Steganography produces a PSNR value of >= 43db. In [18] author, to solve the problem of the size of the message to be inserted, it is proposed to use LZW compression with a color code-based approach. The proposed technique uses a forward-mail platform to hide confidential data. The workings of the proposed method are to compress the secret message, and then the message is inserted into the e-mail cover. The secret data bit is embedded into the message or cover text by creating a color using a color code table. The experimental results show that the proposed method not only produces a high insertion capacity but also reduces the complexity of the computational process.

In [19] author, two different techniques are proposed. First, using LSB without encryption and without compression. Second, using LSB with a combination of encryption and compression. In addition, in this paper, it is also combined with the Discrete Cosine Transform (DCT) method to convert the image into the frequency domain. The results of the experiments carried out prove that the use of a combination of methods can increase the message embedding capacity on the cover image compared to without using a combination. The image quality of the proposed technique has been evaluated based on the MSE and PSNR parameters. Based on the evaluation results, the MSE value generated in the combination of methods is an average of 1.1 dB, and the average PSNR value is >= 48 dB. In [20] author proposed a combination of AES for cryptography, and DWT for Steganography. However, because the DWT algorithm has a weakness in the relatively lower storage capacity. So, to overcome this problem, Huffman Coding is proposed to reduce the number of message bits in order to increase storage capacity. The test is done by encrypting the secret message using AES, then the compression result is compressed using Huffman, then the compression result is inserted into a digital image as a process of Steganography. After conducting several experiments using, a message image of 128x128 pixels and a cover image of 512x512 pixels, the average MSE was 1.5676 and the average PSNR result was above 40 dB, which was 46.1878.

III. PROPOSED WORK

A. *Huffman Compression Process*

Huffman algorithm is a compression algorithm that uses a statistical approach. The sequence of steps in the encoding process for this algorithm is as follows:

1. Sort the grayscale values by the frequency with which they occur.
2. Merge the two trees that have the lowest frequency of occurrence and reorder them.
3. Repeat step 2 until one binary tree remains.
4. Label the binary tree by labelling the left side of the tree as 0 and the right side of the tree as labelled 1.
5. Trace the binary tree from root to leaf. The row of side labels from root to leaf is the Huffman code.

For example, by using ASCII code, the string "ABBABACAACDDD" is then converted into binary code as follows:

A	B	B	A	B
01000001	01000010	01000010	01000001	01000010
A	B	A	C	A
01000001	01000010	01000001	01000011	01000001
A	C	D	D	D
01000001	01000011	01000100	01000100	01000100

Then change it to Huffman code, with the following steps:

1. Make a list of the frequency of occurrence of each character and sort it from smallest to largest as in Table 1.

TABLE 1. CHARACTER OCCURRENCE FREQUENCY

Character	*Frequency*
A	6
B	4
C	2
D	3

2. Merge the two trees that have the smallest occurrence frequency and reorder them as shown in Fig 1.

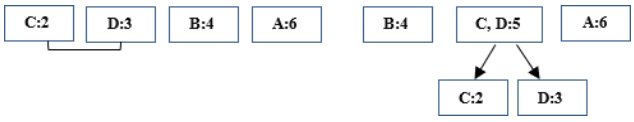

Fig 1. Huffman Process 1

3. Merge the two trees that have the smallest occurrence frequency and reorder them as shown in Fig 2.

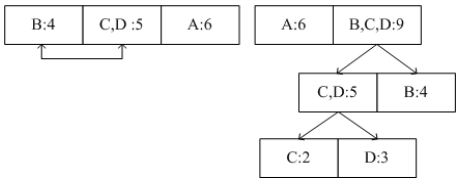

Fig 2. Huffman Process 2

4. Recombine the two trees that have the smallest occurrence frequency and rearrange them as shown in Fig 3.

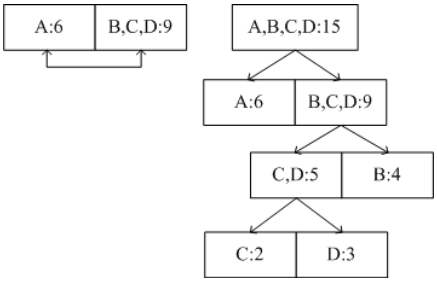

Fig 3. Huffman Process 3

5. Add labels from root to leaf, left = 0, right = 1 as shown in Fig 4.

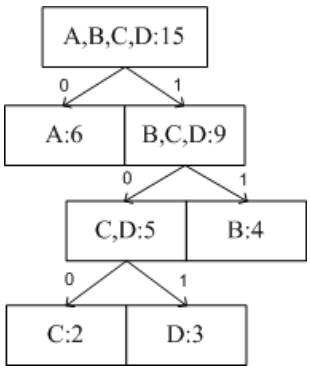

Fig 4. Huffman Process 4

Tracing from root to leaf (from top to bottom) yields the Huffman code as follows:

A=0 B=11 C=100 D=101

The final result of the Huffman code can be seen in Table 2.

TABLE 2. HUFFMAN CODE RESULTS

Character	*Frequency*	*Huffman Code*
A	6	0 = 1 bit
B	4	11 = 2 bit
C	2	100 = 3 bit
D	3	101 = 4 bit

Thus, the resulting string "ABBABABACAACDDD" can be written as follows:

0 11 11 0 11 0 11 0 100 0 0 100 101 101 101 101

Based on the Huffman process that has been described, it appears that the code of a symbol/character should not be the prefix of another symbol code in order to avoid ambiguity in the decompression or decoding process. The size of the string before compression (in ASCII code) is: 15 x 8 = 120 bits.

The size of the string after compression (in Huffman code) is:

=6 x 1 bit + 4 x 2 bit + 3 x 3 bit + 2 x 3 bit
=29 bit
Then the compression ratio becomes

$$= 100\% - \frac{29}{120} x\ 100\ \% = 75{,}8\ \%$$

B. *The Process of Inserting Text Messages into the Cover Image*

After the message in the form of text is compressed, the next process is the insertion of the message into the cover image. The insertion process is the second process after data compression. Data insertion begins by inserting a cover image into the application, after that the LSB algorithm will read the RGB binary code on the cover image and the Huffman tree code. The user enters a key that serves to secure the data contained in the Steganography. The algorithm will read the binary from the key entered to get the binary value for each character, if the binary code generated is 0 then the secret message will be inserted into the cover image in the seventh binary, while if the binary code is 1 then the secret message will be inserted into the binary code. cover image on the eighth binary. The flow of the message insertion process can be seen in Fig 5.

Fig 5. Message Insertion Process

C. *Message Extraction Process*

The message extraction process is the process of releasing the secret message contained in Steganography. The extraction process begins by entering the stego-image into the steganography program, after which the algorithm will read the inserted stego-image. Next, enter the key and the algorithm will read the binary of each key character that will be used to perform the message extraction process. The flow of the message extraction process can be seen in Fig 6.

Fig 6. Message Extraction Process

IV. RESULT AND DISCUSSION

A. *Huffman Compression Test Results*

Huffman compression test is done to find out how much data compression is generated. This Huffman compression test uses a number of characters that are arranged randomly and have various character occurrence values. From the tests that have been carried out, the results of the Huffman compression are presented in Table 3.

TABLE 3. HUFFMAN COMPRESSION TEST RESULTS

No	*Number of Characters*	*Original size (byte)*	*Size of Compression (byte)*	*Ratio*
1	10 Characters	10	20	-100%
2	50 Characters	50	56	-12%
3	100 Characters	100	166	-66%
4	500 Characters	500	70	86%
5	1000 Characters	999	120	87.99%
6	5000 Characters	49997.12	122	97.56%
7	10.000 Characters	10024.96	135	98.65%
8	20.000 Characters	19968	171	99.14%
9	50.000 Characters	49971.2	179	99.64%
10	100.000 Characters	103424	75	99.93%

The results obtained from the Huffman compression test in Table 3 are the ratio values obtained from these tests are very diverse. This is due to the frequency of characters that are compressed. The greater the frequency of occurrence of characters from a message, then the compression value will be greater and if the smaller the frequency of occurrence of characters from a message, the smaller the value of the compression ratio.

B. LSB Steganography Testing

The test at this stage is to find out whether the compressed data can be inserted into the cover image. At this stage the combination of the Huffman compression method and the LSB steganography method will be tested for its capabilities. The test is carried out by inserting one of the messages in Table 3. The test will be carried out in two ways, namely inserting a message without Huffman compression, and the second is inserting a message that has been compressed by Huffman so that the comparison can be seen.

The cover image used in this study represents the color representation, namely R (Red), G (Green) and B (Blue), this is intended to test whether the data can be inserted into the cover image based on the color representation being tested. Message insertion is carried out on the cover image by paying attention to the key given before carrying out the message insertion process. The key entered by the user will be read by the algorithm and converted into binary code. If the binary value is 0 then the data will be inserted in the sixth bit, if the binary value is 1 then the data will be inserted in the seventh bit. The key binary code will continue to be repeated until the data in the cover image is read. The Cover Image used for the trial can be seen in Fig 7.

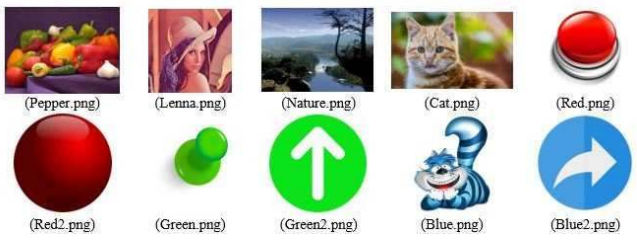

Fig 7. Cover Image

The following in Table 4 are the results of LSB steganography testing on message insertion without Huffman compression, and in Table 5 are the results of testing the combination between Huffman compression and LSB steganography.

TABLE 4. LSB STEGANOGRAPHY TEST RESULTS WITHOUT HUFFMAN COMPRESSION

No	*Cover Image*	*Cover Image Dimension*	*Cover Image Size (kb)*	*Size of Message (kb)*	*Stego Image Size (kb)*
1	Pepper.png	512 x 384	280	48	296
2	Lenna.png	512 x 512	462	48	478
3	Nature.png	400 x 300	162	48	178
4	Cat.png	600 x 352	500	48	516
5	Red.png	512 x 512	145	48	161
6	Red2.png	512 x 512	137	48	153
7	Green.png	512 x 512	190	48	206
8	Green2.png	512 x 512	121	48	137
9	Blue.png	512 x 512	266	48	282
10	Blue2.png	512 x 512	119	48	135

TABLE 5. TEST RESULTS COMBINATION OF HUFFMAN COMPRESSION AND LSB STEGANOGRAPHY

Cover Image	*Cover Image Dimension*	*Cover Image Size (kb)*	*Original Size of Message (kb)*	*Size of Message (kb)*	*Stego Image Size (kb)*
Pepper.png	512 x 384	280	48	0.17	289
Lenna.png	512 x 512	462	48	0.17	471
Nature.png	400 x 300	162	48	0.17	171
Cat.png	600 x 352	500	48	0.17	509
Red.png	512 x 512	145	48	0.17	154
Red2.png	512 x 512	137	48	0.17	146
Green.png	512 x 512	190	48	0.17	199
Green2.png	512 x 512	121	48	0.17	130
Blue.png	512 x 512	266	48	0.17	275
Blue2.png	512 x 512	119	48	0.17	128

The results of the process in Table 4 and Table 5 show that the insertion of data into the cover image has been carried out successfully. However, the test results in Table 5 show that the size of the stego-image is relatively smaller than the test results in Table 4. This is because the message is compressed before the message is inserted into the cover image.

C. Fidelity Test

Fidelity testing is carried out to measure the quality of the cover image and stego image, whether there is a significant change after the addition of a message, so that steganalysis does not know that in the stego image there is a secret message. The fidelity test is carried out by several tests,

namely by calculating the MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) values.

1) MSE Testing (Mean Square Error)

The MSE (Mean Square Error) test is carried out to calculate the average value of the square of the sum of the squares of absolute errors between the cover image and the stego image. Before determining PSNR (Peak Signal to Noise Ratio), you must first calculate the MSE value using equation (1).

$$MSE_{AVG} = \frac{MSE_R + MSE_G + MSE_B}{3} \quad (1)$$

Information:
MSE_{AVG} = The average value of MSE cover image.
MSE_R = MSE value in red.
MSE_G = MSE value in green.
MSE_B = MSE value in blue.

The results of the MSE calculations carried out in this paper can be seen in Table 6.

TABLE 6. MSE TEST RESULTS (MEAN SQUARE ERROR)

No	*Stego Image*	*MSE Value using LSB (dB)*	*MSE Value using Combination of Huffman and LSB*
1	Stego1	1.19	0.31
2	Stego2	1.21	0.52
3	Stego3	1.35	0.43
4	Stego4	1.11	0.36
5	Stego5	1.02	0.41
6	Stego6	1.05	0.38
7	Stego7	1.32	0.45
8	Stego8	1.42	0.32
9	Stego9	1.05	0.27
10	Stego10	1.83	0.29

From the results of the tests that have been carried out in Table 6, the average MSE value of LSB steganography testing without using Huffman compression is 1.25. Meanwhile, for the combination of LSB steganography and Huffman compression, the average MSE value is 0.37. This shows that the smallest mean value of the MSE is the result of a combination of LSB steganography and Huffman compression. The smaller the MSE value, the better because there is not much change in the pixel value in the stego-image. Furthermore, the results of the MSE test are made in graphical form to show the comparison results as presented in Fig 8.

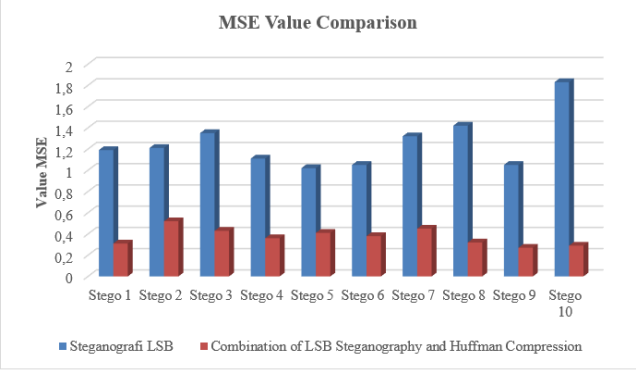

Fig 8. Graph of MSE Value Comparison Results

2) PSNR Testing (Peak Signal to Noise Ratio)

PSNR (Peak Signal to Noise Ratio) test is used to measure the quality of the resulting image [21]. The PSNR method is a measure of the comparison between the pixel value of the cover image and the pixel value in the stego image generated by using equation (2).

$$PSNR = 10_{log10}\left(\frac{255^2}{MSE}\right) \quad (2)$$

The results of the PSNR calculations carried out in this paper can be seen in Table 7.

TABLE 7. PSNR TEST RESULTS

No	*Stego Image*	*PSNR Value using LSB (dB)*	*PSNR Value using Combination of Huffman and LSB*
1	Stego1	41.34	50.45
2	Stego2	42.45	50.78
3	Stego3	41.56	54.78
4	Stego4	43.58	53.78
5	Stego5	44.67	54.67
6	Stego6	43.98	55.32
7	Stego7	43.67	56.65
8	Stego8	41.28	56.45
9	Stego9	40.32	54.32
10	Stego10	40.67	52.40

Based on the test results presented in Table 7, it shows that the average result of calculating the PSNR value for LSB steganography is 42.35. While the average value of PSNR combination of LSB Steganography and Huffman compression is 53.96. The higher the PSNR value, the better the image quality of the developed algorithm will be. To visualize the comparison results of the PSNR test, it is presented in graphical form in Fig 9.

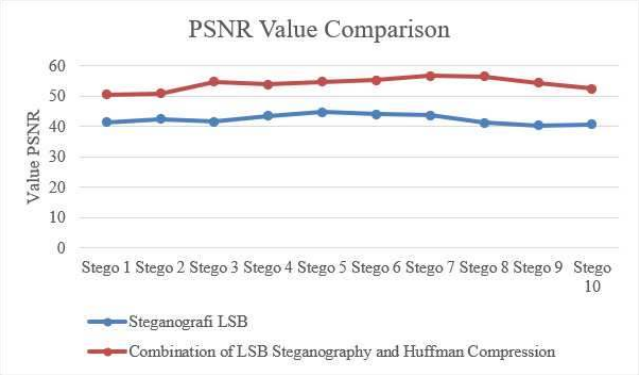

Fig 9. Graph of PSNR Value Comparison Results

Based on the test by calculating MSE and PNSR, it was found that the MSE value resulting from the combination of LSB steganography and Huffman Compression was <= 1 dB and PNSR >= 50 dB, meaning that the change in colour quality between the cover image and the stego image did not change significantly, so the presence of hidden messages are not easily detected by the human senses of sight. The result of this combination produces a better image quality than the previous paper, which is the comparison material in this paper [11], [12]. The basic principle of Steganography is how to insert a secret message into a medium without the other party knowing that in the media, there is a message that has been inserted. So, based on the results of the tests that have been carried out, the combination of LSB steganography and Huffman compression can be recommended as a method that can be used to improve data security in steganographic techniques.

V. CONCLUSION

Based on the results of the discussion and testing that has been done, it proves that the combination of LSB steganography and Huffman compression can be applied to the process of inserting messages into image media. Huffman compression can compress messages with compression ratios up to 99.93%. The high value of the compression ratio affects the frequency of occurrence of characters in a message. The image quality produced by the combination of LSB steganography and Huffman compression can be better than without Huffman compression. This is evidenced by the low MSE value resulting from the combination, which is an average of 0.37 dB, and the PSNR value is an average of 53.96 dB.

ACKNOWLEDGEMENT

This research is funded by The Ministry of Research and Technology/The National Research and Innovation Agency, the Republic of Indonesia under the schema Doctoral Research Grant 2021.

REFERENCES

[1] Wamiliana, M. Usman, A. Hijriani, Warsito, and R. Setiawan, "The Hybrid Methods of Column Transposition with Adaptive Minimum Error Least Significant Bit Replacement(AMELSBR) Using file jpg / jpeg and png," *Int. J. Comput. Sci. Netw. Secur.*, vol. 17, no. 7, pp. 174–179, 2017.

[2] X. Zhang, F. Peng, and M. Long, "Robust Coverless Image Steganography Based on DCT and LDA Topic Classification," *IEEE Trans. Multimed.*, vol. 20, no. 12, pp. 3223–3238, 2018, doi: 10.1109/TMM.2018.2838334.

[3] A. K. Sahu, G. Swain, and E. Suresh Babu, "Digital image steganography using bit flipping," *Cybern. Inf. Technol.*, vol. 18, no. 1, pp. 69–80, 2018, doi: 10.2478/cait-2018-0006.

[4] O. Juarez-Sandoval, A. Fierro-Radilla, A. Espejel-Trujillo, M. Nakano-Miyatake, and H. Perez-Meana, "Cropping and noise resilient steganography algorithm using secret image sharing," *Sixth Int. Conf. Graph. Image Process. (ICGIP 2014)*, vol. 9443, no. Icgip 2014, p. 94431S, 2015, doi: 10.1117/12.2179745.

[5] D. Hu, L. Wang, W. Jiang, S. Zheng, and B. Li, "A novel image steganography method via deep convolutional generative adversarial networks," *IEEE Access*, vol. 6, no. c, pp. 38303–38314, 2018, doi: 10.1109/ACCESS.2018.2852771.

[6] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," *Neurocomputing*, vol. 335, pp. 299–326, 2019, doi: 10.1016/j.neucom.2018.06.075.

[7] M. Mishra, P. Mishra, and M. C. Adhikary, "Digital Image Data Hiding Techniques: A Comparative Study," vol. 7, no. 2, pp. 105–115, 2014, [Online]. Available: http://arxiv.org/abs/1408.3564.

[8] D. Darwis and N. B. Pamungkas, "Comparison of Least Significant Bit, Pixel Value Differencing, and Modulus Function on Steganography to Measure Image Quality, Storage Capacity, and Robustness," in *Journal of Physics: Conference Series*, 2021, vol. 1751, no. 1, p. 12039.

[9] Z. Zhou, Y. Mu, and Q. M. J. Wu, "Coverless image steganography using partial-duplicate image retrieval," *Soft Comput.*, vol. 23, no. 13, pp. 4927–4938, 2019, doi: 10.1007/s00500-018-3151-8.

[10] B. Mishra, R. Beg, and V. P. Singh, "Information Security Through Digital Image Steganography Using Multilevel and Compression Technique," *MIT Int. J. Comput. Sci. Inf. Technol.*, vol. 3, no. 1, pp. 26–29, 2013.

[11] D. Darwis, A. Junaidi, and Wamiliana, "A New Approach of Steganography Using Center Sequential Technique," *J. Phys. Conf. Ser.*, vol. 1338, no. 1, 2019, doi: 10.1088/1742-6596/1338/1/012063.

[12] D. Darwis, A. Junaidi, and D. A. Shofiana, "A New Digital Image Steganography Based on Center Embedded Pixel Positioning," *Cybernetics and Information Technologies.*, vol. 21, no. 2, pp. 89–104, 2021, doi: 10.2478/cait-2021-0021.

[13] Y. Xu, B. Chen, and Z. Hu, "Research for multi-sensor data fusion based on Huffman tree clustering algorithm in greenhouses," *Int. J. Embed. Syst.*, vol. 8, no. 1, pp. 34–38, 2016.

[14] C.-H. Wu, K.-K. Tseng, C.-K. Ng, G. T. S. Ho, F.-F. Zeng, and Y. K. Tse, "An improved Huffman coding with encryption for Radio Data System (RDS) for smart transportation," *Enterp. Inf. Syst.*, vol. 12, no. 2, pp. 137–154, 2018.

[15] Z. Yin, Y. Xiang, and X. Zhang, "Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding," *IEEE Trans. Multimed.*, vol. 22, no. 4, pp. 874–884, 2019.

[16] S. Yuan and J. Hu, "Research on image compression technology based on Huffman coding," *J. Vis. Commun. Image Represent.*, vol. 59, pp. 33–38, 2019.

[17] R. Mishra, A. Mishra, and P. Bhanodiya, "An edge based image steganography with compression and encryption," *2015 Int. Conf. Comput. Commun. Secur. ICCCS 2015*, pp. 2–5, 2016, doi: 10.1109/CCCS.2015.7374161.

[18] A. Malik, G. Sikka, and H. K. Verma, "A high capacity text steganography scheme based on LZW compression and color coding," *Eng. Sci. Technol. an Int. J.*, vol. 20, no. 1, pp. 72–79, 2017, doi: 10.1016/j.jestch.2016.06.005.

[19] O. F. AbdelWahab, A. I. Hussein, H. F. A. Hamed, H. M. Kelash, A. A. M. Khalaf, and H. M. Ali, "Hiding data in images using steganography techniques with compression algorithms," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 17, no. 3, pp. 1168–1175, 2019, doi: 10.12928/TELKOMNIKA.V17I3.12230.

[20] 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 Comput. Electron. Control.*, vol. 17, no. 5, pp. 2400–2409, 2019, doi: 10.12928/TELKOMNIKA.v17i5.9570.

[21] S. K. Kumar, P. D. K. Reddy, G. Ramesh, and V. R. Maddumala, "Image transformation technique using steganography methods using LWT technique," *Trait. du Signal*, vol. 36, no. 3, pp. 233–237, 2019, doi: 10.18280/ts.360305.