Dual Security Method for Digital Image using HBV Encryption and Least Significant Bit Steganography

Ajib Susanto¹, De Rosal Ignatius Moses Setiadi¹, Eko Hari Rachmawanto¹, Christy Atika Sari¹, Rabei Raad Ali², and Ibnu Utomo Wahyu Mulyono¹

¹ Department of Informatics Engineering, Dian Nuswantoro University, 207 Imam Bonjol Street, Semarang 50131, Indonesia
² Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, 86400 Parit Raja, Johor, Malaysia

Abstract. This study proposes a combination of two security techniques, namely steganography and cryptography. The proposed steganography technique is LSB because it has advantages in data embedding capacity and message imperceptibility. The LSB technique is very simple and predictable, so to improve message security HBV encryption techniques are applied. HBV encryption is applied to the message before pinning it. HBV encryption is a combination of the Beaufort algorithm and Vigenere cipher so that the message security will be stronger. By combining HBV and LSB encryption, the message can be hidden properly, and its awake. Based on the experimental results, the encryption and embedding process can run well and produce good quality encryption and stego images. Similarly, the extraction and decryption process can run perfectly.

1. Introduction
Steganography is one of the hiding data techniques that is widely used to secure data sent over the internet network. Digital imagery is an object that is widely used in current research [1] [2]. Watermarking is also one of the data hiding techniques that are similar to steganography. The difference between these two techniques is their function. Watermarking is useful for protecting the image copyright of a host by permanently attaching a watermark so that the watermark is not lost when the host image is manipulated [3]. Watermarking does not emphasize large payloads, the most important thing is the strength of embedded watermark attachments must be strong against various attacks, besides that the image quality of hosts that have been given a watermark should also have good quality. Good image quality can be measured by PSNR with a minimum value of 40dB or more [4]. While steganography serves to protect secret messages so that they cannot be extracted or read by others. In the science of host image steganography only used as a message embedding media, the most important thing and must be protected is the security of embedded secret messages. Two other important things are imperceptibility, which means that the message embedded in the host image cannot be perceived by the human senses so it does not arouse suspicion. The payload is also an important thing in the science of steganography, with a large payload that will make the efficiency of sending messages better.

This study focuses on how to secure messages on steganography techniques, especially in digital images. One method that until now continues to be developed in the science of steganography is Least Significant Bits (LSB). LSB method works by replacing the smallest bit with the message bit so that with this technique the host image cannot be returned to its initial state. But this doesn't really matter, because the most important thing is the embedded message security. LSB method is a method in the
spatial domain of steganography which is very simple but produces an impercept stego image and has a relatively large payload [1]. By default, the LSB method can embed one message bit on one-pixel image or has a one-eighth the capacity of the cover image size. The LSB technique is a very predictable technique because generally message embedding is done from left to right and from top to bottom. Some techniques are used to embed messages by being spread either randomly or using random generators such as PN Generators. This method of deployment serves to secure messages and can also increase imperceptibility [5]. Another way is to combine cryptographic techniques with steganography [6] [7] [8].

Cryptography is a science used to secure data by encoding data with certain algorithms. This method is effective for protecting against attackers [9]. When combined with steganography, cryptography is usually done on messages before pinning, after an encrypted message is embedded in the host's image. There are many cryptographic methods. One of the popular classical symmetrical cryptography is Vigenere cipher. The Vigenere algorithm is also a substitution cryptographic algorithm. Substitution cryptography is a technique that changes plain text with ciphertext based on key [10] [11]. There are several derivatives of Vigenere cipher, one of which is Beaufort cipher [12] [13]. This cryptographic technique has the power that depends on the key. Encryption will be stronger if the key used is really random, with the same size as plain text, and only used once [5] [14] [15]. So, the idea proposed in this study is to apply the Beaufort Vigenere cipher hybrid algorithm with multiple keys so that the results of encryption are increasingly difficult to decrypt by unauthorized parties, then the results of encryption are embedded with the LSB method on the host image.

2. Previous Research
Several studies have proposed a combination of steganography and cryptographic techniques, as in the study proposed by Kusuma et al. [8]. In his research, LSB was used to hide images. LSB is used because of its superiority in message storage capacity and good stego image quality. The simple weakness of LSB closed with the implementation of DES cryptography methods and the prioritized storage of messages on the edge of the image. Inserting messages in the edge area of the image serves to improve the quality of the stego image produced.

Irawan et al. [14] also applied text message hiding techniques to the cover image using the LSB method. In addition, canny edge detection is also applied to determine the image edge area, this edge area is stored for message embedding and message extraction. Before the message is pinned, the message is encrypted with the OTP method. The PSNR measurement results produce a value of around 69dB for message embedding of 8192 bits in grayscale type 512 * 512 pixels images.

Danuputri et al [16] also applied the LSB steganography method combined with the Vigenere cryptographic technique. This time the combination of methods was applied to the Android programming language. Before the message is encrypted with the Vigenere algorithm, the message is compressed with the Arithmetic coding compression algorithm. To add to the security of the key Vigenere is encrypted with the 256 SHA algorithm. In this study, the cover media used is digital images, while the messages used are in the form of pdf, documents, and sheets files.

Dewangga et al [17] also proposed LSB steganography techniques with two kinds of cryptographic techniques, namely Vigenere and Caesar. Caesar's algorithm is applied first to text messages, then followed by the Vigenere algorithm. The text cipher generated by the two cryptographic algorithms is then pinned to the smallest bit of the RGB type stego image. Tests are performed on RGB images with sizes 8 * 8 pixels up to 12 * 12 pixels with the maximum message size that can be pinned. The message encryption results produce an avalanche effect of 100%, and the PSNR value is between 59dB and 63dB.

From some of the above studies, it is proven that the LSB method is still widely applied in various recent steganographic studies. This is because the LSB method is still relatively good in terms of message storage capacity and imperceptibility. Its weakness is only in simple embedding techniques so that message extraction is predictable. To improve security this technique is combined with cryptography. So, in this study, a Hybrid method of Beaufort and Vigenere algorithms was proposed with two random keys to increase message security.
3. Hybrid Beaufort Vigenere (HBV) Cipher Algorithm
The HBV cryptographic algorithm is a combination of the Beaufort algorithm and Vigenere cipher. Vigenere cipher is a substitution cryptographic technique that was popular in its time. Vigenere cipher is also often called Vernam cipher or one-time pad cipher. The type of key used in the encryption and decryption process is a symmetrical key. The encryption quality of this algorithm depends on the key. The encryption results will be very strong if the key size is the same as plaintext, the key is only used once, and is completely random [15]. However, this has a negative impact on the plain text that has a large and long size because the key size used must also be large. Vigenere cipher uses XOR or modulo operations in performing encryption and decryption operations. The Vigenere cipher formula for the encryption and decryption process can be calculated with formula (1) for encryption and formula (2) for decryption.

\[
Ct = (Pt + Rk) \mod 256 \tag{1}
\]

\[
Pt = (Ct - Rk) \mod 256 \tag{2}
\]

Where \(Ct\) is a cipher text, \(Pt\) is plain text, \(Rk\) is a random key with a range of 0 to 255, 256 is used as a dividing constant because the range used is 8 bits.

Beaufort cipher is a derivative substitution cryptography method from Vigenere cipher that uses subtraction techniques [12] [13]. The formula used in Beaufort cipher is very synonymous with Vigenere cipher. The similarity of the two techniques is the use of the modulo function or the remainder of the results for or the type of key used. The difference between the two methods is the key role, in Vigenere key ciphers are used as plain text enhancers and text cipher subtractors. Whereas in the formula used by Beaufort cipher, the key is used to be deducted from plain text and text ciphers. To be more clear, we can note the Beaufort cipher encryption and decryption formula in formula (3) for encryption and formula (4) for decryption.

\[
Ct = (Rk - Pt) \mod 256 \tag{3}
\]

\[
Pt = (Rk - Ct) \mod 256 \tag{4}
\]

From the two algorithms, HBV cipher method is made which is more powerful using multiple random keys, where the first random key \(Rk1\) contains a value with a range of 8 bits and the second random number contains a value with a binary range \(Rk2\). For more details, see formula (5) for HBV cipher encryption and formula (6) for HBV cipher decryption.

\[
Ct = \begin{cases} 
(Pt + Rk1) \mod 256, & Rk2 = 0 \\
(Rk1 - Pt) \mod 256, & Rk2 = 1 
\end{cases} \tag{5}
\]

\[
Pt = \begin{cases} 
((Ct - Rk1) \mod 256, Rk2 = 0 \\
(Rk1 - Ct) \mod 256, Rk2 = 1 
\end{cases} \tag{6}
\]

4. Proposed Method
Based on the things that have been stated in the introduction section, that the steganography technique using LSB has many advantages, except in terms of security, in this study HBV cipher algorithm is proposed to be applied to secret messages before being embedded in the cover image with the LSB algorithm. In this section it will be divided into two main processes, the first process is the process of encryption and embedding, while the second process is the process of extraction and decryption.

4.1. Encryption and Embedding Process
The following is a step by step of encryption and embedding:
1. Read the secret message in the form of the gray image measuring m * n, then save it on the variable Pt.
2. Create a random key matrix Rk1 consisting of 8bit integers remaining for 256, where the Rk1 matrix size is the same as the message.
3. Create another random key matrix Rk2 consisting of binary numbers of the same size as the message.
4. Encrypt the secret message using formula (5) to get the text cipher (Ct).
5. Embed the ciphertext in the cover image using the LSB algorithm.

4.2. Extraction and Decryption Process
The following is a step by step of extraction and decryption:
1. Extracting the ciphertext from the stego image using the LSB algorithm, then save it to the Ct variable.
2. Read random key Rk1 (8bit) and random key Rk2 (binary).
3. Perform a decryption operation using the two random keys in the text cipher using formula (6).
4. Get the decrypted secret message image.

5. Experiment and Results
The cover image dataset used in this study was taken from [18]. The type of image used is a standard test image with a gray type or with a depth of 8 bits. All images are 512 * 512 in size. All images used are the tif type, and no modifications or preprocessing are carried out before processing. The image was chosen so that this study would be easier to compare with prior research or subsequent research. Figure 1 shows the cover image used in this study.

![Cameraman](cameraman.tif)  ![Lena Gray 512](lena_gray_512.tif)  ![Mandrill Gray](mandril_gray.tif)  ![Woman Darkhair](woman_darkhair.tif)

**Figure 1.** Cover Image Dataset

While the message image used is 256 * 128. The message size is the maximum message size that can be embedded in the cover image with the maximum embedding of each pixel of the cover image is 1 bit. The message image used is shown in Figure 2.

![SECRET](SECRET.jpg)

**Figure 2.** Message Image

The first step is to encrypt the message image first. To encrypt a message image, two random keys are needed (RK1 and Rk2); Figure 3 displays a sample of random key images used. Based on the message image and key image encryption is done using formula (5) to produce an encrypted image message as shown in Figure 4.
5

Random key 8bit (Rk1)  
Random key biner (Rk2)

Figure 3. Sample random key used

Figure 4. Encrypted Message Image

The time needed for the encryption process is relatively very fast, based on measurements using the tic toc function on Matlab only takes about 0.007 seconds (with the specifications of the AMD A12 processor and 8 GB RAM). In addition, the results of encryption on the message are visually very different from the original message image. But the visual display does not have a definite size, so the results of encryption are measured using a correlation coefficient (cc) which can be calculated by the formula (7) [11]. CC is a measuring tool to determine the level of image correlation, where the cc measurement results between 0 to 1, where if the value is closer to 0, the results of encryption are increasingly not correlated with the original image. The cc measurement results obtained a value of 0.0029, this value is very close to zero and this indicates that the results of encryption are very good.

\[
cc = \frac{\sum_m \sum_n (O - \bar{O})(E - \bar{E})}{\sqrt{\sum_m \sum_n (O - \bar{O}) (\sum_m \sum_n E - \bar{E})}}
\]  

(7)

Where m and n are image sizes, O is the original image or plaintext, and E is image encryption or ciphertext.

The next process is the embedding process carried out by the LSB method, where each pixel of the cover image is filled with one message bit. The results of the tuning produce a stego image whose quality is measured using PSNR and SSIM. The PSNR and SSIM formulas used are the default formula of the psnr and ssim functions in Matlab R2015a. PSNR is the peak noise value of the image signal, where noise indicates a large image change [19]. The more noise generated by the insertion process, the quality of the resulting stego image will be poor. The quality of the stego image must meet good criteria, a good stego image has a PSNR value of at least 40dB or greater [4]. The second measurement of the quality of stego images is SSIM. The SSIM serves to measure the similarity of the structure of the stego image with the original image. The better the quality of the stego image the structure will be close to the original image. SSIM values are generated in the range 0 to 1. The better the quality of the stego image the SSIM value is close to 1. Table 1 shows the stego image produced following the measurement of PSNR and SSIM.

| Image | Description |
|-------|-------------|
| Random key 8bit (Rk1) | Sample random key used |
| Random key biner (Rk2) | |
| Encrypted Message Image | |

Table 1: Stego Image Produced Following Measurement of PSNR and SSIM
Table 1. Stego Image Results using Proposed Method.

| Image Name       | Original Image | Stego Image Results | PSNR  | SSIM  |
|------------------|----------------|---------------------|-------|-------|
| cameramen.tif    | ![cameramen.tif](image) | ![cameramen.tif](image) | 54.1541 | 0.9949 |
| lena_gray_512.tif| ![lena_gray_512.tif](image) | ![lena_gray_512.tif](image) | 54.1917 | 0.9960 |
| mandril_gray.tif | ![mandril_gray.tif](image) | ![mandril_gray.tif](image) | 54.1617 | 0.9984 |
| woman_darkhair.tif | ![woman_darkhair.tif](image) | ![woman_darkhair.tif](image) | 54.1168 | 0.9947 |

Based on the stego image shown in table 1, there is no visual difference between the original cover image and the generation stego image of the proposed method. The PSNR and SSIM values are shown in table 1 also show that the quality of the stego image is very good. The SSIM value is very close to 1, this indicates that there is almost no structural change in the stego image, in short, the structure is identical to the original cover image. The PSNR value is more than 54dB and far above the criteria requirements are very good, which is 40dB. In addition to the PSNR and SSIM values, testing is also done by observing the image histogram. A good stego image should be identical to the original image histogram. Table 2 shows the comparison of the original image histogram and stego image.
Table 2. Comparison of Original Histogram and Stego Histogram

| Image Name             | Original Histogram | Stego Histogram |
|------------------------|--------------------|-----------------|
| cameraman.tif          | ![Histogram](image) | ![Histogram](image) |
| lena_gray_512.tif      | ![Histogram](image) | ![Histogram](image) |
| mandril_gray.tif       | ![Histogram](image) | ![Histogram](image) |
| woman_darkhair.tif     | ![Histogram](image) | ![Histogram](image) |

Based on the observations in Table 2, it appears that the cover image histogram is very similar to the stego image histogram. The similarity of the histogram shows that the quality of the stego image produced from the proposed method is good. The last stage of testing the method is in the process of extraction and decryption. A secret message should be able to be extracted and decrypted perfectly so that there is no meaning of the missing message. Because the message is in the form of an image, a cc gauge is used to find out the similarity of the original message and the extracted message. The decryption process is also very fast, the time needed is almost the same as the encryption process, which is around 0.007 seconds, based on measurements with the tic toc function. Based on the measurement results of all extracted messages get the value $cc = 1$, this means the message can be extracted and decrypted perfectly. Figure 5 displays the results of the extraction and decryption of message images, and visually also proved no different.
6. Conclusion
This study successfully combined two security techniques to improve the security of message images. The HBV algorithm which is a combination of two cryptographic algorithms namely Vigenere and Beaufort can be implemented in image messages. The message image encryption algorithm is also very good, as evidenced by the cc score = 0.0029. While the decryption process runs perfectly as evidenced by the value of cc = 1. The performance of the HBV algorithm is also very fast because it only takes about 0.007 seconds for each encryption and extraction process. The results of encryption of the image message are then pinned on the cover image using the LSB algorithm. Based on the experimental results it has been proven that the stego image produced has very good quality, which is above 54dB. Likewise, with the histogram analysis that looks very identical between the histogram of the cover image and the stego image.

7. References
[1] Zakaria, A. A., Hussain, M., Wahab, A. W. A., Idris, M. Y. I., Abdullah, N. A. & Jung, K.-H, 2018. High-Capacity Image Steganography with Minimum Modified Bits Based on Data Mapping and LSB Substitution, Applied Sciences, vol. 8, no. 11, pp. 1-19.
[2] Setiadi, D. R. I. M., Santoso, H. A., Rachmawanto, E. H. & Sari, C. A., 2018. An improved message capacity and security using divide and modulus function in spatial domain steganography, in International Conference on Information and Communications Technology.
[3] Lei, G., Fuping, L., Shike, L., Jianping, P., Zhipeng, L. & Yukun, W., 2018. High-efficiency embedding and anti-clipping digital watermark algorithms based on the LSB, watermark separation and image interpolation, in IOP Conference Series: Materials Science and Engineering.
[4] Nasution, A. B., Efendi, S. & Suwilo, 2018. Image Steganography In Securing Sound File Using Arithmetic Coding Algorithm, Triple Data Encryption Standard (3DES) and Modified Least Significant Bit (MLSB), J. Phys.: Conf. Ser, vol. 1007.
[5] Najih, M., Setiadi, D. R. I. M., Rachmawanto, E. H., Sari, C. A. & Astuti, S., 2017. An improved secure image hiding technique using PN-sequence based on DCT-OTP, in International Conference on Informatics and Computational Sciences.
[6] Ardiansyah, G., Sari, C. A., Setiadi, D. R. I. M. & Rachmawanto, E. H., 2017. Hybrid Method using 3-DES, DWT and LSB for Secure Image Steganography Algorithm, in International conferences on Information Technology, Information Systems, and Electrical Engineering.
[7] Kusuma, E. J., Sari, C. A., Rachmawanto, E. H. & Setiadi, D. R. I. M., 2018.A Combination of Inverted LSB, RSA, and Arnold Transformation to get Secure and Imperceptible Image Steganography, Journal of ICT Research and Applications, vol. 12, no. 2, pp. 103-122.
[8] Kusuma, E. J., Indriani, O. R., Sari, C. A., Rachmawanto, E. H. & Setiadi, D. R. I. M., 2017. An Imperceptible LSB image Hiding on Edge Region using DES Encryption, in International Conference on Innovative and Creative Information Technology.
[9] T. T. Zhang, S. J. Yan, C. Y. Gu, R. Ren, and K. X. Liao, "Research on Image Encryption Based on DNA Sequence and Chaos Theory," J. Phys.: Conf. Ser, vol. 1004, pp. 1-6, 2018.
[10] Ardy, R. D., Indriani, O. R., Sari, C. A., Setiadi, D. R. I. M. & Rachmawanto, E. H., 2017. Digital image signature using triple protection cryptosystem (RSA, Vigenere, and MD5), in International Conference on Smart Cities, Automation & Intelligent Computing Systems.

[11] Setiadi, D. R. I. M., Rachmawanto, E. H, Sari, C. A., Susanto, A. & Doheir, M., 2018. A Comparative Study of Image Cryptographic Method, in International Conference on Information Technology, Computer and Electrical Engineering.

[12] Widyastuti, N., 2014. Pengembangan Metode Beaufort Cipher menggunakan Pembangkit Kunci Chaos, Jurnal Teknologi, vol. 7, no. 1, pp. 73-82.

[13] Alallayah, K., Amin, M., El-Wahed, W. A. & Alhamami, A., 2010. Attack and Construction of Simulator for Some of Cipher Systems Using Neuro-Identifier, The International Arab Journal of Information Technology, vol. 7, no. 4, pp. 365-372.

[14] Irawan, C., Setiadi, D. R. I. M., Sari, C. A. & Rachmawanto, E. H, 2017. Hiding and securing message on edge areas of image using LSB steganography and OTP encryption, in International Conference on Informatics and Computational Sciences.

[15] Shukla, R., Prakash, H. O., Bhushan, R. P., Venkataraman, S. & Varadan, G., 2013. Sampurna Suraksha: Unconditionally Secure and Authenticated One Time Pad Cryptosystem, in International Conference on Machine Intelligence and Research Advancement.

[16] Danuputri, C., Mantoro T. & Hardjianto, M. 2015. Data Security using LSB Steganography and Vigenere Chiper in an Android Environment, in International Conference on Cyber Security, Cyber Warfare, and Digital Forensic.

[17] Dewangga, I. G. A. P., Purboyo T. W., & Nugrahaeni, R. A. 2017. A New Approach of Data Hiding in BMP Image using LSB Steganography and Caesar Vigenere Cipher Cryptography, International Journal of Applied Engineering Research, vol. 12, no. 2, pp. 10626-10636.

[18] Gonzalez, R. C., Woods, R. E. & Eddins, S. L., "ImageProcessingPlace.com," [Online]. Available: http://www.imageprocessingplace.com/downloads_V3/root_downloads/image_databases/standard_test_images.zip. [Accessed 2018].

[19] Setiadi, D. R. I. M. & Jumanto, J. 2018, An Enhanced LSB-Image Steganography Using the Hybrid Canny-Sobel Edge Detection, Cybernetics and Information Technologies, vol. 18, no. 2, pp. 74-88.