

PAPER • OPEN ACCESS

## Securing and Hiding Secret Message in Image using XOR Transposition Encryption and LSB Method

To cite this article: Andik Setyono and De Rosal Ignatius Moses Setiadi 2019 *J. Phys.: Conf. Ser.* **1196** 012039

View the [article online](#) for updates and enhancements.



**IOP | ebooks™**

Bringing you innovative digital publishing with leading voices to create your essential collection of books in STEM research.

Start exploring the collection - download the first chapter of every title for free.

# Securing and Hiding Secret Message in Image using XOR Transposition Encryption and LSB Method

**Andik Setyono, De Rosal Ignatius Moses Setiadi**

Department of Informatics Engineering, Dian Nuswantoro University, Semarang, Indonesia

Email: andik.setyono@dsn.dinus.ac.id

**Abstract.** The popular LSB technique is used in steganography techniques on spatial domains. This technique has many advantages in terms of imperceptibility and payload. Except in the case of security, the LSB technique is very weak because it is very simple and predictable. This study combines LSB steganography techniques and transposition XOR encryption techniques with the aim of increasing the security of embedded messages. Before the embedded message is encrypted with a transposition encryption algorithm and embedded with an XOR operation based on the key on the largest bit of the Host image. In the process of testing text messages with a size of 1 kB, 2 kB, and 4 kB pinned. The test results indicate that the security of the message is getting stronger without reducing the advantages of LSB techniques, namely imperceptibility and payload. All messages can also be extracted and decrypted perfectly, as evidenced by the CER value = 0.

## 1. Introduction

Security is very important when sending confidential data via the internet. Various security techniques such as watermarking, digital signatures, steganography and cryptography have been widely implemented in many studies [1] [2] [3] [4]. Each of these methods has its own function with advantages and disadvantages. Watermarking is widely used for copyright protection [5], digital signatures are widely used for the protection of digital signatures [3], while steganography and cryptography are widely used to secure digital messages [6]. Steganography and cryptography are often applied jointly in one method to improve security, as in research [7] [4] [8].

Steganography is a data hiding technique that continues to be developed today. In steganography science there are several important things such as imperceptibility, security, and payload [9]. These three things are always researched by researchers to continue to be improved. As in the research [10] proposed methods to increase data payload, research [11] [12] improve data security, in research [8] improve data imperceptibility.

One of the popular methods that are still being developed to date is the LSB method. LSB is a steganographic technique that is included in the spatial domain, where messages are embedded directly in the image on the least significant bit [13]. The advantage of the LSB method is that it is relatively easy to implement, has good imperceptibility and a large payload. These LSB advantages make many researchers focus on improving message security in LSB technique. To improve message security many researchers usually use cryptographic techniques to encrypt messages before messages are embedded [4] [14] [15]. Some cryptographic methods that are widely combined with steganography techniques are Chaotic Map, RC4 and OTP. In the study [16], the three methods have been tested and compared with various measurement methods such as MSE, PSNR, Entropy, UACI, NPCR, histogram analysis, and



computational speed, where it has been concluded that OTP is better in terms of security and computational speed. The main operation on the OTP algorithm that makes robust encryption, is XOR operation. Research [16] also concluded that Chaotic Map has the slowest computing, especially when using a lot of iterations. But the chaotic map method has a strong property in terms of diffusion and confuse. Chaotic map techniques are also often called scramble techniques that only perform randomization without changing the contents of the data. One of the simpler and faster scramble techniques is the transposition technique.

This research proposes encryption techniques by combining transposition techniques and XOR operations on the OTP method to produce super encryption techniques. Super encryption technique is a combination of two or more methods in a cryptographic algorithm [17]. With the advantages of the XOR operation in the OTP method and the transposition technique as one of the scramble methods like chaotic maps, then it can produce a super encryption method against various attacks with a fast computing process. The proposed super encryption method is combined with the LSB method to obtain more secure steganography techniques.

## 2. Related Research

Irawan et al. [7] proposed LSB steganography techniques combined with OTP encryption. LSB was chosen because it has many advantages which are simple, relatively good in terms of imperceptibility and payload. OTP is used to close down the weaknesses of LSB techniques that are easy to guess. To get good security the keys that are used randomly and extensively are the same as the embedded messages. The disadvantage of this method is that if the message is pinned large then the key made is also large, it requires more shipping bandwidth. To increase imperceptibility, embedding is done on the edge area of the image. Based on the test this technique is able to get a satisfying PSNR value and an identical histogram with the host image.

Arun and Murugab [14] proposed combined LSB steganography techniques with XOR substitution operations on RGB images. This method is very simple LSB which is secured by XOR operation with an 8-bit random key. Embedding is divided into each color channel R, G and B. Thus the security of the message is increased before being pinned.

Hussein et. Al. [15] proposed a mapping technique to break text messages before embedded using LSB techniques. Each character message along the 8-bit section is broken down into 2-bits each using ASCII table mapping. before being pinned. Thus indirectly the message is encrypted with the spread technique. Budiman et al. [17] proposed a super-encryption technique with a combination of Trithemius and double transposition algorithms. The double transposition technique is a message randomization technique based on rows and columns. While the Trithemius algorithm is a classic encryption technique using tabula recta. With the combination of these two methods, the result of encryption is stronger than just one method.

Based on the related research above, this method proposes a combination of XOR encryption and transposition of columns in text messages before embedded in the image using the LSB method. The biggest bit in the host image will be used as an XOR encryption key, this is used to reduce shipping bandwidth. While the message is transposition encryption before it is pinned.

## 3. Proposed Method

In the proposed method in this study required input data in the form of the host image, text message, and key transposition in the embedding process to produce stego image and secondary key. Whereas the message extraction process requires stego image and transposition key and secondary key.

### 3.1. Embedding Process

Here is the detail of the message embedding process:

1. Read the test message in the form of a .txt file
2. Calculate the length of the message character contained in the message and save it on the variable ( $lm$ ).
3. Input the transposition encryption key ( $kt$ ).
4. Calculate the key length and save it as a column variable ( $c$ ).

5. Get row variable row ( $r$ ) with formula (1)


$$r = \text{ceil}(lm/c) \tag{1}$$

6. Get a secondary key ( $sk$ ) with formula (2), then save it to be proposed for the decryption process.

$$sk = c * r \tag{2}$$

7. Sort the transposition key before starting the encryption process.
8. Encrypt with the column transposition method, the result of this process will change the message in the form of an array to change into a matrix and be converted into an array for the embedding process ( $E_m$ ). The following is the encryption process for column algorithm transposition with an example message: UNIVERSITAS DIAN NUSWANTORO SEMARANG IS JEMPOL DAN OKE, and the key to transposition is: POLKE.

KEY:	P	O	L	K	E
	1	2	3	4	5
1	U	N	I	V	E
2	R	S	I	T	A
3	S		D	I	A
4	N		N	U	S
5	W	A	N	T	O
6	R	O		S	E
7	M	A	R	A	N
8	G		M	E	M
9	A	N	G		J
10	E	M	P	O	L
11	D	A	N		O
12	K	E	null	null	null
SORT KEY:	5	4	3	2	1



In accordance with the order of the alphabet POLKE will change to EKLOP, and the empty/null cell table will be changed to character \*.

From the table above, the message is changed according to the order of the transposition key, where:

- Column 1: EAASOENMJLO\*
- Column 2: VTIUTSAE O \*
- Column 3: IIDNN RMGPN\*
- Column 4: NS AOA NMAE
- Column 5: URSNWRMGAEDK

So, the encrypted message becomes EAASOENMJLO\*VTIUTSAE O \* IIDNN RMGPN\* NS AOA NMAEURSNWRMGAEDK

9. Convert the encrypted message to a binary form and paste it into the host image using the XOR operation. The XOR operation key used is the largest bit of the pixel of the host image that will be observed by the message bit. The XOR operating formula used is (3).

$$LSB(x, y) = MSB(x, y) \text{ XOR } E_m(i) \tag{3}$$

### 3.2. Extraction Process

The following is a detailed message extras process:

1. Read stego image.
2. Input secondary key ( $sk$ ).
3. Extraction of messages ( $sk$ ) pixels on stego images with XOR operations, with formula (4). Then convert into ASCII character.

$$E_m(i) = MSB(x, y) \text{ XOR } LSB(x, y) \tag{4}$$

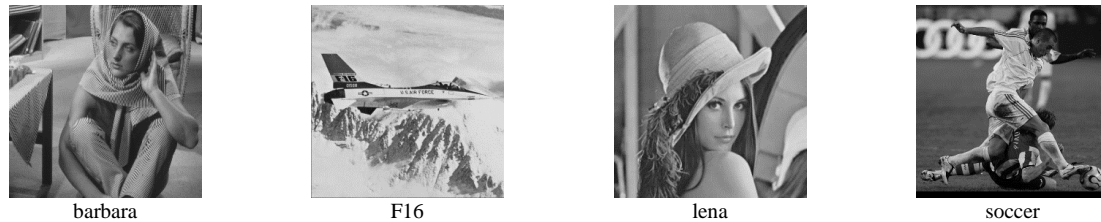
4. Input the transposition encryption key ( $kt$ ), according to the embedding process.
5. Change the extraction of the message ( $E_m$ ) into a matrix with the line length ( $r$ ) and column ( $c$ ). Where the column is obtained from the length ( $kt$ ) and row is obtained by formula (5).

$$r = \text{ceil}(E_m/c) \tag{5}$$

6. Read the matrix message according to the sequence of the transposition key, then delete all symbols \*. So that a secret message is obtained.

#### 4. Experimental Results

This study uses the host image shown in Figure 1. The image is a grayscale image with a size of 256 \* 256. The host image will be embedded with a text message of 1 kB, 2 kB and 4 kB.



**Figure 1.** Host Image used

Before the message is pinned the message is encrypted by transposing the column with the key = 'polke'. Furthermore, the embedding process is measured in quality with MSE and PSNR. MSE is calculated by the formula (6) and PSNR is calculated by the formula (7). MSE and PSNR measurement results are shown in Table 1. While the sample images of the test results are displayed in Figure 2.

$$MSE = \sum_{q=0}^{Q-1} \sum_{w=0}^{W-1} \|S_i(q, w) - H_i(q, w)\|^2 \tag{6}$$

$$PSNR_{dB} = 10 \log_{10} \left( \frac{255^2}{\sqrt{MSE}} \right) \tag{7}$$

Where,  $S$  is stego image,  $q$  and  $w$  is the size of the image,  $H$  is the host image

**Table 1.** Experiment Results from Proposed Method based on PSNR and MSE Value

Image Name	1 kB Message		2 kB Message		4 kB Message	
	PSNR (dB)	MSE	PSNR (dB)	MSE	PSNR(dB)	MSE
Barbara	63.3908	0.0298	60.0497	0.0643	57.1713	0.1247
F16	62.8165	0.0340	59.9037	0.0665	57.0116	0.1294
Lena	63.5195	0.0289	59.9187	0.0663	57.0260	0.1290
Soccer	63.2185	0.0310	60.3883	0.0595	57.3182	0.1206

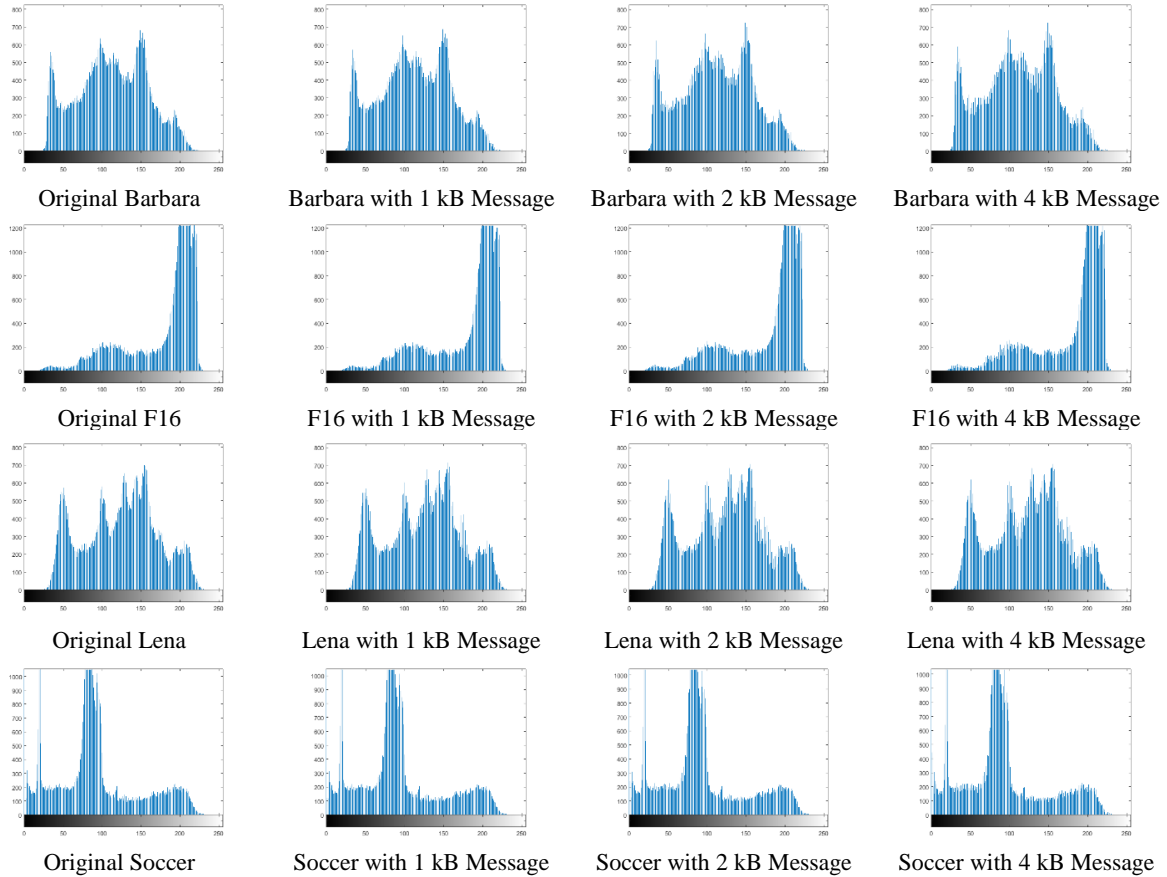


**Figure 2.** Sample Stego Image results

Table 1 shows that the results of the measurement of MSE and PSNR values, the value far exceeds the threshold of good manipulation image quality, which is 40dB [18]. The next test is to use a histogram. A histogram is the amount of intensity of the appearance of pixels. Message embedding results can change an image's histogram. This will certainly create suspicion that the data is embedded in the image. Based on the experimental results in Figure 3, histograms with different sizes of different payloads still look identical, which means the quality of the stego image is excellent [19]. Next, the extraction process must be done perfectly because steganography techniques require that messages can be conveyed properly without losing a bit [10]. Therefore, the extracted message needs to be tested by testing the Character Error Rate (CER) with the formula (8).

$$CER = \frac{nE}{lM} \tag{8}$$

Where,  $nE$  is the number of error characters and  $lM$  is the message length. Based on the results of the extraction test all messages can be extracted perfectly, in other words the  $CER$  value = 0.



**Figure 3.** Histogram of Stego Image Results

**5. Conclusion**

The LSB method is a popular method and is still widely researched. LSB has advantages in imperceptibility and data payload aspects but is weak in the security aspects of the message because of the very simple embedding method. This research proposes XOR transposition encryption to improve message security before being embedded. The experimental results prove that the proposed encryption process can improve message security and still maintain the imperceptibility and payload aspects. Text messages can also be extracted perfectly as evidenced by the  $CER$  value = 0.

**References**

- [1] Kim, C., Lee, S., Lee, J. & J.-I. Park. 2018, "Blind decoding of image steganography using entropy model," *Electronics Letters*, vol. **54**, no. 10, pp. 626 - 628.
- [2] Winarno, A., Setiadi, D. R. I. M., Arrasyid, A. A., Sari, C. A. & Rachmawanto, E. H. 2017, "Image Watermarking using Low Wavelet subband based on  $8 \times 8$  sub-block DCT," in International Seminar on Application for Technology of Information and Communication (iSemantic), Semarang.
- [3] 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 (ICON-SONICS), Yogyakarta.

- [4] Abood, M. H. 2017, "An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms," in Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), Baghdad.
- [5] Sudibyoy, U., Eranisa, F., Rachmawanto, E. H., Setiadi, D. R. I. M. & Sari, C. A.. 2017, "A secure image watermarking using Chinese remainder theorem based on haar wavelet transform," in International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), Semarang.
- [6] Setyono, A., Setiadi, D. R. I. M. & Muljono, M. 2017, "StegoCrypt method using wavelet transform and one-time pad for secret image delivery," in International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), Semarang, 2017.
- [7] 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 (ICICoS), Semarang.
- [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 (ICITech), Salatiga.
- [9] Menon, N. & Vaithyanathan. 2017, "A survey on image steganography," in International Conference on Technological Advancements in Power and Energy ( TAP Energy), Kollam.
- [10] 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.
- [11] Ulker, M. & Arslan, B. 2018, "A novel secure model: Image steganography with logistic map and secret key," in International Symposium on Digital Forensic and Security (ISDFS), Antalya.
- [12] Tambe, S., Naik, D., Parab, V. & Doiphode, S. 2017, "Image steganography using uniform split and merge technique," in International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore.
- [13] Hussain, H. S., Din, R. & Idrus, R. 2018, "Preserve Imperceptibility and Robustness Performance on Steganography Technique based on StegaSVM-Shifted LBS Model," *Journal of Physics: Conference Series*, vol. 1018.
- [14] Arun, C. & Murugan, S. 2018, "Design of image steganography using LSB XOR substitution method," in International Conference on Communication and Signal Processing (ICCSP), Chennai.
- [15] Hussein, H. L., Abbass, A. A., Naji, S. A., Al-augby S. & Lafta, J. H. 2018, "Hiding text in gray image using mapping technique," *Journal of Physics: Conference Series*, vol. 1003.
- [16] 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 (ICITACEE), Semarang.
- [17] Budiman, M. A., Rachmawati, D. & Jessica. 2018, "Implementation of Super-Encryption with Trithemius Algorithm and Double Transposition Cipher in Securing PDF Files on Android Platform," *Journal of Physics: Conference Series*, vol. 979.
- [18] 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 (ICITISEE), Yogyakarta
- [19] 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 (ICOIACT), Yogyakarta