**Webology**, Volume 18, Number 5, 2021
**ISSN:** 1735-188X
**DOI:** 10.29121/WEB/V18I5/29

# Utilizing Steganography and Cryptography to Conceal Information Within BMP Images

**Devesh Pratap Singh[1], Dibyahash Bordoloi[2], Surendra Shukla[3]**

[1]Department of Computer Science & Engineering,Graphic Era Deemed to be University, Dehradun, Uttarakhand India, 248002
[2]Head of the Department, Department of Computer Science & Engineering,Graphic Era Hill University, Dehradun, Uttarakhand India, 248002
[3]Department of Computer Science & Engineering,Graphic Era Deemed to be University, Dehradun, Uttarakhand India, 248002

## ABSTRACT

Every day, more sophisticated methods will be needed to safeguard confidential data from intrusion and hacking attempts. Both cryptography and steganography are well-respected for their ability to protect confidential information during transmission via potentially unsafe channels. However, when these two approaches are combined, data transmission security is much improved. For that reason, the purpose of this study is to present a new steganography method that, when combined with a novel encryption method, offers an additional layer of protection against assaults. The new solution is based on the Least Significant Bits (LSB) methodology and works with BMP files to conceal sensitive information. The experimental outcomes in this study is done using VB6 language. Peak Signal-to-Noise Ratio and Mean Squared Error are two common metrics used to evaluate picture quality (PSNR). Varied host images have been tried with different sizes of files to be concealed. From what we can see, the new method provides much improved PSNR and lower MSE values across the board. For this reason, the suggested method provides an effective means of guarding sensitive data while transmission across unsafe networks.

**Keywords:** Steganography;Cryptography;LeastSignificant Bit;BMP Images;Network Security; PSNR.

## INTRODUCTION

Virtual Data transmission across unsafe networks may be protected by cryptography or steganography. With the use of cryptography, the text is jumbled up and rendered unintelligible. While steganography makes the textual data invisible by concealing it. But when used together, these techniques improve the safety of our communications. In general, cryptographic methods may be split into two camps: symmetric and asymmetric. With symmetric cryptography, the sender and the intended recipient use the same key to encrypt and decode the data. [1]

**Webology**, Volume 18, Number 5, 2021
**ISSN:** 1735-188X
**DOI:** 10.29121/WEB/V18I5/29

Cover media, the hidden message, and the steganography algorithm are the three main components of a steganographic operation. Better security may also be attained via the use of a secret key or password. The cover format may be any visual or textual content, as well as audio or video. The most often used kind of steganography, however, is picture steganography, which simply refers to the practise of embedding a stego-image (an image with hidden information) into a larger image. Steganography using photographs is both easy to use and widely used. There are a vast variety of picture file formats in the digital realm, but BMP images are the most common option for the steganography process due to their ease of use and widespread compatibility with Windows software. Some of the most prevalent steganographic techniques are least significant bit (LSB) encoding, transform methods, and masking and filtering. To steganographiy, LSB is one of the most widely used and effective techniques. [2] In recent years, several steganography algorithms that use the least significant bit approach have been published and studied [3]. In [4], the author suggested encrypting the secret data using the RSA and Diffie Hellman algorithms and then concealing it in the cover picture with the LSB approach. In contrast, Jamal N.[5] presented a novel LSB steganography system that combines with a novel symmetric encryption technique dubbed MJEA. There is an emphasis on medical imagery and patient data. Outcomes from experiments shown that this method achieves excellent PSNR and MSE results [6]. A great deal of progress has been made in the field of security, but there is always room for improvement and innovation. The purpose of this study is to create a steganography algorithm using the LSB technique.

## THE PROPOSED TECHNIQUE

The The suggested method relies heavily on BMP pictures and is composed of three primary algorithms: encryption, embedding, and extraction and decryption. Here are the steps of the first algorithm:

### Encryption Algorithm

In this section, we will go through the fundamental building blocks of this algorithm: First, type in the length of the secret message.

Second, for each letter you enter (key1 and key2), you will be given its corresponding ASCII code.
Key3 = key1 XOR key2 is the result of applying the XOR technique to keys 1 and 2.
Obtain the ASCII value for "Ch" by reading a character from the text in Step 4.
The fifth step is to divide the result of the fourth step by 3, yielding Ch1=Int (Ch/3).
Sixth, we subtract the number we got in step 5 from the one we got in step 4: Ch2 = Ch1 - Ch. Ch3 = Ch1 + Int(key1/2), therefore the seventh step is to figure out Ch3.
The eighth step is to compute Ch4, which is defined as Ch2 + Int(key2 / 3).
Nine, do an XOR operation on Ch3 and key3: Ch5 = Ch3XOR key3. In Step 10, we XOR Ch4 with key3, therefore Ch6 = Ch4 XOR key3. The eleventh stage is to binary-ize the Ch5 and Ch6 values.
Step 12: Repetition of steps 4-11 for all massage characters.

B. EmbeddedAlgorithmAt this point, the cover picture has been encrypted using the LSB approach, concealing the secret key (key1 and key2) and the duration of the massage inside it. The secret message will be encoded on the cover photo using just the colours red "R" and green "G." aircraft. Main phases of this algorithm are as follows:

**Webology**, Volume 18, Number 5, 2021
**ISSN:** 1735-188X
**DOI:** 10.29121/WEB/V18I5/29

The first action is to bring up the cover picture and determine its dimensions.
In the second step, compare the dimensions of the cover picture with the hidden message.
Step 3: Apply the following to the cover picture in order to conceal the secret keys "key1 andkey2"
First, determine the binary sequence of keys 1 and 2.
Second, beginning with the pixel in column 13, row 2, take the pixel and separate it into its R, G, and B components.
3. Cover the least significant bit of "key1" with the least significant bit of byte "R."
4.Conceal the least significant bit of "key2" in the least significant bit of byte "G"
Using steps 5 through 7, separate the preceding pixel into its R, G, and B components.
Sixth, until all parts are hidden, repeat steps 3 through 5.
Fourth, use the following techniques onto the cover picture to conceal the massage's duration:
First, we may retrieve the binary representation of each value in the massage length "msg len" by dividing it into the three blocks "B1, B2, and B3."
Integer ((msg len/1000)/1000) = B1. B2 = Int(msg len/1000) mod 1000
What does B3=msg lenmod 1000 mean?
To do this, find the pixel in column 13, row 3, and then pick it up; from this point on, you'll be dividing pixels into their R, G, and B components.
3. cover the "B1" bit in the lowest "R" byte.
4.Conceal the "B2" bit in the least significant byte (G).
5. Cover the "B3" bit with the least significant bit of byte "B."
(6) Take the preceding pixel and separate it into its R, G, and B components.
Step 7.Repeat steps 3-6 until all portions are hidden.
5. Conceal the binarysequence of an encrypted message by using:
Take the pixel in the first column of row 4 and separate it into its R, G, and B components.
2. Cover up the "Ch5" bit in the lowest byte "R."
Thrive in the worst of byte "G," hiding the "Ch6" bit.
A four-step process: 4. Leap two pixels.
Take the pixel and separate it into its R, G, and B colours, step 5.
Repeat from step 2 through step 5 until all bits are hidden, and then go on to step 6. Sixth, save the steganographic picture.
Algorithm C for Data Extraction and Decryption
The fundamental operations of this algorithm are as follows: First, open the steganographic picture.
The second step entails deducing the secret "key1 and key2" key:
Taking the pixel in the second row, column 13 first, select the pixel and split it into the R, G, and B channels.
Key1=0, thus take the least significant bit of byte "R" and put it in key2.
3. Pick up the least bit of byte “G”and save in key2, where key2= 0.
4. Pick up the preceding pixel and divide it into R, G and B components.
Five, return to the previous step to get the next byte.
Key1 and Key2 values may be retrieved by retrieving bits and converting each group of 8 into a decimal number.
Here's a calculation for key3: key3 = key1 XOR key2.
Third, use the following to get the length of the message, "msg len":

1) Pick a pixel in column 13, row 3, then split it into its R, G, and B components.

**Webology**, Volume 18, Number 5, 2021
**ISSN:** 1735-188X
**DOI:** 10.29121/WEB/V18I5/29

2) To save the least significant bit of byte "R" at location B1, where B1=0, 2.
3) 3. Take the least significant bit from byte "G" and put it in B2, where B2=0.

Remove the least significant bit from byte "B" and place it in B3, where B3=0.
Using steps 5 through 7, separate the preceding pixel into its R, G, and B components.
Repeat 6 to get the following byte.
The values of B1, B2, and B3 may be obtained by retrieving bits and converting each group of 8 bits into a decimal number.
8. Determine the length of the message, "msg len," using the formula msg len=B1+B2+B3. The fourth step is to get the text by using these rules:
First, grab the pixel in row 4, column 1, and separate it into its R, G, and B components.
Second, extract the lowest bit from byte "R" and put it in Ch5, where Ch5= 0.
3. Take the least significant bit from byte"G" and put it in Ch6, where Ch6= 0.
A four-step process: 4. Leap two pixels.
Take the pixel and separate it into its R, G, and B colours, step 5.
Repeat 6 to get the following byte.
To acquire Ch1 and Ch2's values, all you have to do is retrieve bits and convert each group of 8 into a decimal number.
Ch3 = Ch5 XOR key3 is the eighth operation; key3 is XORed with Ch5 to form Ch3.
Ch4 = Ch6 XOR key3 is an XOR operation, hence the answer to the question is Ch6.
Ten. Determine Ch1 by using the formula Ch1 = Ch3 - Int (key 1/2).
Ch2 = Ch4 - Int (key2 / 3) is the formula for determining Ch2.
To get to Ch;Ch, add Ch1 and Ch2 together, since Ch;Ch = Ch1 + Ch2.
Thirteen, interpret the ASCII code as a letter or symbol.
Fourteenth, do the same thing with every other character.
The fifth step is to save or print the hidden message or picture.

## EXPERIMENT RESULTS

These findings are the product of experimental work done in VB6 on an Intel® CoreTMi52.30 GHZ processor. In this evaluation, we utilise two 24-bit BMP pictures. (24 x 300 x 300) "AhmedAl Bashir" is the first photograph. The second picture is titled "duck" and has the dimensions (24 x 348 x 249). Cover pictures before the concealing procedure was performed using the suggested technique are shown in Figures 1 and 3. Although stego-images hidden with this method are shown in figures 2 and 4, respectively. The aforementioned photographs demonstrate unmistakably that stego-images may be mistaken for cover images, and that the binary data buried inside can be effectively retrieved.

Steganography quality is measured in this study using PSNR (PeakSignal-to-Noise Ratio) and MSE (Mean Square Error) to assess the level of picture distortion.

All four trials utilised covers with one of four distinct coloured graphics. The average root-mean-square error (MSE) and peak-to-average noise ratio (PSNR) for each tested picture.

**Webology**, Volume 18, Number 5, 2021
**ISSN:** 1735-188X
**DOI:** 10.29121/WEB/V18I5/29

## CONCLUSION

Together, steganography and encryption techniques are proposed in this paper as a novel security method to provide protection against intrusion.

Experiment findings offers a good PSNR values in all tested circumstances and concealed text files were retrieved effectively without loosing any data.

This algorithm is highly safe and can effectively process Arabic and English texts.

It is hoped that further development would allow for the concealment of additional forms of multimedia content inside a variety of cover art formats.

## REFERENCES

1. Diffie, W., & Hellman, M. E. (2019). New directions in cryptography. In Secure communications and asymmetric cryptosystems (pp. 143-180). Routledge.
2. Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. arXiv preprint arXiv:1804.00200.
3. Abood, O. G., & Guirguis, S. K. (2018). A survey on cryptography algorithms. International Journal of Scientific and Research Publications, 8(7), 495-516.
4. Evans, T. M. (2019). Cryptokitties, cryptography, and copyright. AIPLA QJ, 47, 219.
5. Dutta, I. K., Ghosh, B., & Bayoumi, M. (2019, January). Lightweight cryptography for internet of insecure things: A survey. In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0475-0481). IEEE.
6. Raikwar, M., Gligoroski, D., & Kralevska, K. (2019). SoK of used cryptography in blockchain. IEEE Access, 7, 148550-148575.
7. Alqad, Z., Oraiqat, M., Almujafet, H., Al-Saleh, S., Al Husban, H., & Al-Rimawi, S. (2019). A New Approach for Data Cryptography. *International Journal of Computer Science and Mobile Computing*, *8*(9), 30-48.
8. Pittalia, P. P. (2019). A comparative study of hash algorithms in cryptography. *International Journal of Computer Science and Mobile Computing*, *8*(6), 147-152.
9. Watt, C., Renner, J., Popescu, N., Cauligi, S., & Stefan, D. (2019). Ct-wasm: type-driven secure cryptography for the web ecosystem. *Proceedings of the ACM on Programming Languages*, *3*(POPL), 1-29.
10. Namasudra, S., & Deka, G. C. (2018). Introduction of DNA computing in cryptography. In *Advances of DNA computing in cryptography* (pp. 1-18). Chapman and Hall/CRC.