
Implementation of the Least Significant Bit Method for Hiding Text in Digital Images

Harmoko Lubis¹, Jontinus Manullang²

¹²AMIK Medicom, Jl. Darat No.74, Medan, Indonesia
Email : harmoko_lubiz@gmail.com

ABSTRACT

To speed up the process of sending secret messages, we need a medium for small messages that can still guarantee the confidentiality of the messages they contain. GIF (Graphics Interchange Format) is an image format that is one of the most commonly used formats on the web because of its small size and for encrypting the text that is sent. Encryption is carried out at the time of delivery by converting the original data into confidential data, while decryption is carried out at the time of receipt by converting the confidential data into original data. The most common way to hide messages is to use the Least Significant Bit (LSB). This research has succeeded in implementing the LSB algorithm to solve steganography on digital images in GIF format optimally.

Keywords: *Least Significant Bit, Digital Image, Secret, Steganograph.*

1. Introduction

To speed up the process of sending secret messages, we need a medium for small messages that can still guarantee the confidentiality of the messages they contain. GIF (Graphics Interchange Format) is an image format introduced by CompuServe in 1987 and is one of the most commonly used formats on the web because of its small size and for encrypting text that is sent. To fulfill this, an encoding process (encryption and decryption) is carried out on the data to be sent. Encryption is carried out at the time of delivery by converting the original data into confidential data, while decryption is carried out at the time of receipt by converting the confidential data into original data. So the data sent during the delivery process is confidential data, so that the original data cannot be known by unauthorized parties. The GIF format only accommodates a maximum of 256 colors in an image file because it uses 8-bits for each pixel. Unlike the JPEG format which can accommodate millions of colors (using 24-bit for each pixel). (Vaughan, 2006).

The GIF image format has two versions, namely GIF87a and GIF89a. GIF87a is the first version of the GIF format which is a static image. CompuServe then introduced an advanced version, namely GIF89a. GIF89a can display dynamic images (animations) and transparent backgrounds.

The most common way to hide messages is to use the Least Significant Bit (LSB). Although there are many shortcomings in this method, the ease of implementation makes this method still used today. This method requires conditions, namely, if compression is performed on the watermarked image, a lossless compression format must be used, because this method uses several bits per pixel in the image. If a

lossy compression format is used, hidden secret messages can be lost. If a 24-bit color image is used as the cover, a bit of each of the Red, Green and Blue components can be used so that 3 bits can be stored in each pixel. An 800 x 600 pixel image can be used to store 1,440,000 bits (180,000 bytes) of confidential data.

2. Methodology

The research method used in the preparation of this research is a literature study method by searching and collecting data by looking for references, literature or materials needed from various sources of discourse related to research. Literature study in the preparation of this final project, namely by: (a) Collecting data through the internet, looking for books that discuss programming Microsoft Visual Basic 6.0 to design programs and some other materials related to writing. (b) Designing the form and layout of the program using the Visual Basic 6.0 programming language

3. Results and Discussion

a. Main course

The main menu is the initial form that appears when the application is run. The Main Menu Form Display Form can be seen in the image below.



Figure 1. Main Menu

b. Image Select Form

Select image form is a form for displaying images to be inserted. Display Form Select images can be seen in the image below:

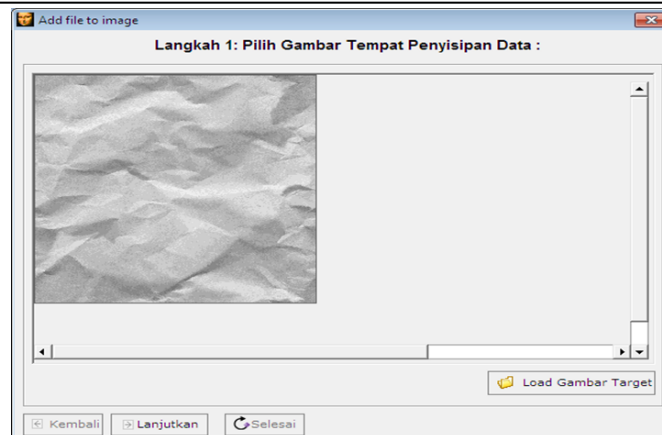


Figure 2. Select Image Form

c. Form Select text file

Select a text file form is a form to display the text that will be inserted. Form Display Form select a text file can be seen in the image below.

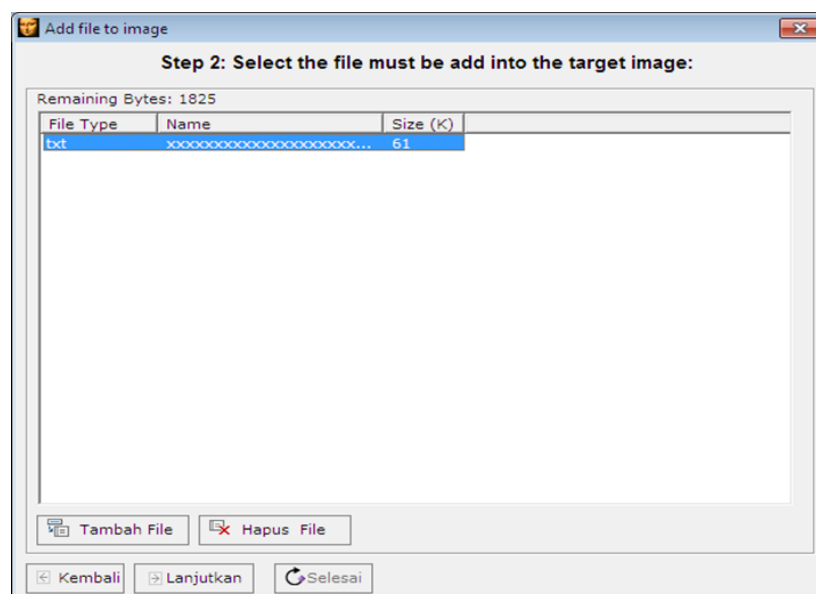


Figure 3. Form Select Text File

d. Form Insertion Process

The insertion process form is a form to display the process when an insertion occurs. Display Form The insertion process form can be seen in the image below.

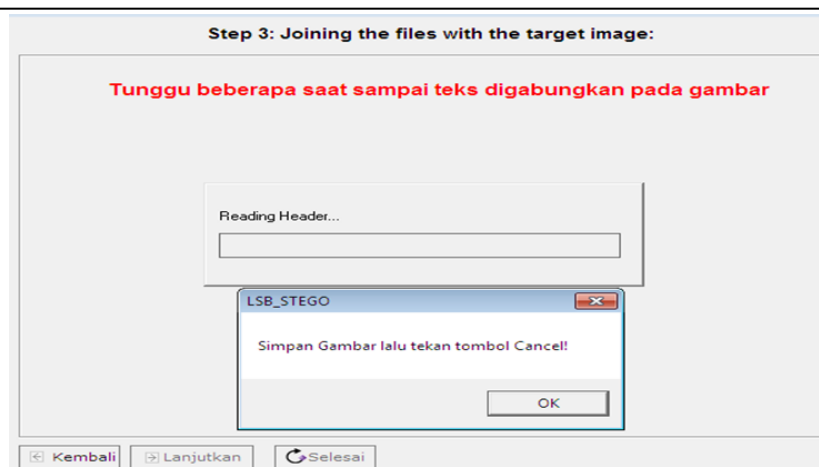


Figure 4. Insertion Process Form

4. Conclusion

This research has succeeded in implementing the LSB algorithm to solve steganography on digital images in GIF format optimally. The software that was built succeeded in inserting messages with the most optimum size according to the method. This algorithm is good for securing digital data in the form of text messages in an image file. Because after the image is inserted a message, it causes a difference in the original image because it inserts text at the last bit in the image. And the encoded text can be numeric, character or a mix of both.

References

- [1] Al Fattah, hanif. 2007. Analisis & Perancangan Sistem Informasi. Yogyakarta: Andi.
- [2] Nurdiana, Dian, and Andri Suryadi. "Perancangan Game Budayaku Indonesiaku Menggunakan Metode MDLC." Jurnal Petik 3.2 (2017): 39-44.
- [3] Suryadi, Andri. "Perancangan Aplikasi Game Edukasi Menggunakan Model Waterfall." Jurnal Petik 3.1 (2017): 8-13.
- [4] Sutabri, Tata. 2012. Analisa Sistem Informasi. Yogyakarta: Andi.
- [5] Andi, 2010. Microsoft Visual Basic 6.0 & Crystal Report 2008. Yogyakarta : Madcoms.
- [6] Andi, 2011. Tutorial 5 Hari Mahir Menggunakan Pinnacle Studio 14, Semarang : Wahana Komputer.
- [7] Andi Offset, 2010. Pengolahan Citra Digital Oleh Darma putra Enterprise Jubilee, 2013. Visual Basic 2013 Untuk Pemula. Jakarta : PT.Elex Media Komputindo, 2013.

