ABSTRACT

Around the world, the internet has developed into one of the media data communication that is very popular. There have been many developing various techniques of information retrieval illegally, and many people trying to access information which is not right.

A variety of techniques to protect information that is kept secret from the person who is not entitled to has been much done in an attempt to secure an important data. Steganography is a technique to hide message files in order for lay people are not aware of the existence of the message files that are hidden. This technique is often used to avoid suspicions of people and avoid the desire to know the contents of the message file. The Digital image is one of the most common media is known by the public. This final project aims at analysing and designing steganography as one of engineering safeguards message files in the GIF image. On the technique of steganography is used the method of LSB (Least Significan Bit) and method of Spread Spectrum.

After successful implementation of the system, several tests were carried out on stego image. From the results of several tests that have been carried out, especially testing based on the MSE and PSNR values, the LSB and Spread Spectrum methods both have a poor value, because the image with the GIF format has only 256 color palettes.

Keywords : Steganography, Least Significant Bit (LSB), Spread Spectrum, GIF