Abstract

Data transmission is frequently face intrusions issues. Different data hiding methods are there to address this problem. Steganography being one; intends on writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. Moreover, cryptography is a tool used in protecting information using cipher text. However, these methods are subjected to suspicion and prone to visual and statistical attacks. While trying to overcome such problems, researchers need to compromise with imperceptibility and hiding capacity. Any basic algorithms including traditional Least Significant Bit algorithm are simpler and faster processing although they are highly vulnerable to these visual and statistical attacks. Once the algorithm is known extracting the hidden information is fairly simple using steganalysis tools. Thus, these are having relatively low data hiding capacity, security compared to the algorithms with enhancements. These enhancements use complex mathematical functions with existing algorithms using cryptography as a method of improving security. The employing cryptography involves complex mathematical calculations requiring advanced processing capabilities leading to slow performance. As a result; it’s difficult to work in low
This research focuses on developing a system that adapts to the enhanced security without using complex mathematical functions with ways in which to improve data hiding capacity. Having less complexity internally provides the user with lower processing environment. The system uses an indexing technique in hiding data inside the cover image providing high security. The proposed system will have an additional step residing outside the traditional Least Significant Bit algorithm which provides hiding data with less vulnerability to intrusion. The requirement of an indexing image will provide the user with high security because the extraction process will totally depend on the bit patterns of the indexing image. This enhancement will be an attempt to overcome threats and weaknesses in the traditional Least Significant Bit algorithm and enhance the security of data hiding.

References

2.  N. Provos and P. Honeyman, “Detecting Steganographic Content on the Internet”, Center for Information Technology Integration, University of Michigan, August 2001
7.  J. J. Roque and J. M. Minguet, “SLSB: Improving the Steganographic Algorithm LSB”, Universidad Nacional de Educación a Distancia (Spain)


15. A. D. Ker, “Improved Detection of LSB Steganography in Grayscale Images” Oxford University Computing Laboratory, Parks Road, Oxford OX1 3QD, England, 2004


