Study on the Image Encryption Algorithm Using AES and Visual Cryptography

SRS Document Template Structure

IEEE/ANSI 830_1998

The primary objective of image encryption is to transmit an image securely over a connected network so that no unauthorized user should be able to decrypt the image. Image encryption has applications in many fields including Banking, Telecommunication and Medical Image Processing etc. Encryption has become an important part due to the emergence of Internet, where sending and receiving data across computers need security of some standard. Various algorithms have been proposed in this field to encrypt and decrypt images. Research shows that using AES and Visual Cryptography to encrypt images is not entirely new. An encryption scheme has been proposed that splits the Image into R, G, and B components and encrypt them using AES. An encryption scheme has been proposed that uses AES and Visual Cryptography to store bio metric data in the cloud. However, these implementations do not disclose any information related to security in the private key generated using AES. Another interesting approach to encrypt image is using the chaotic theory based algorithms.

Abstract

With the current emergence of the Internet, there is a need to securely transfer images between systems. In this context, we propose a secure image encryption algorithm that uses both AES and Visual Cryptographic techniques to protect the image. The image is encrypted using AES and an encoding schema has been proposed to convert the key into shares based on Visual Secret Sharing. The cryptanalysis of the algorithm is then performed and is proved to be secure. The proposed algorithm is then implemented using python and the results are discussed along with the possible future modifications.

Purpose of the document

AES and Visual Cryptography are vulnerable to certain attacks and therefore are not suitable for Image Encryption. The algorithm proposed in this paper can not only withstand the existing attacks but is a so secure from future attacks. In order to achieve such security standard, the best parts of both the algorithms are combined to work together. The proposed algorithm is divided into two phases.

1. Encryption Phase
2. Decryption Phase

Definition

Cryptanalysis is the study of ciphers, cipher texts and cryptosystems with a goal of finding weaknesses in them that will eventually allow the recovery of the plaintext from the 2016 2nd

International Conference on Next Generation Computing Technologies (NGCT-2016) Dehradun, India 14-16 October 2016 811 cipher text, without necessarily revealing much details about the key or the algorithm used for encryption. Some of the common attacks against the existing system are explored and then how the proposed algorithm withstands to such attacks is discussed in detail.