**TEXT AND IMAGE ENCRYPTION DECRYPTION USING AES ALGORITHM**

**ABSTRACT**

Fast evaluation of digital data exchange occurs in recent years. Due to that security of information is much important in data storage and transmission process. Security of internet banking account passwords, email accounts password etc. requires text protection in digital media. In the same way image transmission and storage during industrial and research processes requires image protection. Images have large data size and also has real time constrain problem hence similar method cannot be used to protect images as well as text from unauthorized access. However with few variations in method AES can be used to protect image as well as text. In this application I have implemented encryption and decryption for text and image using AES. These In today’s world data security is the major problem which is to be face. In order to secure data during communication, data storage and transmission we use Advance encryption standard (AES). AES is a symmetric block cipher intended to replace DES for commercial applications.it uses 128-bit block size and a key size of 128, 192, or 256 bits. The AES algorithmis use to secure data from unauthorized user. The available AES algorithm is used for text data as well as for image data. In this paper an image is given as input to AES encryption algorithm which gives encrypted output. This encrypted output is given as input to AES decryption algorithm and original image is regained as output.

**KEYWORDS:** Advanced Encryption Standards, data storage, Security, Encryption and decryption.

**EXISTING SYSTEM**

It was publish by National Institute of Standard and Technology (NIST) in 2001 developed by Joan Daemen and Vincent Rijmen, an algorithm called Rijdael [2]. Tages over 3DES such as high computational efficiency, 128-bit block size and cryptanalysis resistance is strong against differential truncated differential, linear, interpolation and square attacks [1][9]

**Drawbacks**

* Low accuracy.
* Does not performs well in different conditions what these are trained on.
* Low scalability

**PROPOSED SYSTEM**

* AES algorithm is of three types i.e. AES-128, AES-192 and AES-256. This classification is done on the bases of the key used in the algorithm for encryption and decryption process.
* The numbers represent the size of key in bits. This key size determines the security level as the size of key increases the level of security increases.
* The AES algorithm uses a round function that is composed of four different byte-oriented transformations. For encryption purpose four rounds consist of:
  + - Substitute byte
    - Shift row
    - Mix columns
    - Add round key