"Multistage Information Hiding using Novel Visual Cryptography"

(Sponsored by KSCST, Bangalore. Ref No. 35S0775)

A project report submitted in partial fulfillment of the requirements for the degree of

BACHELOR OF ENGINEERING

in

INFORMATION SCIENCE & ENGINEERING

by

Ms. AHALYA
(4AI08IS002)

Mr. AKSHAY R S
(4AI08IS003)

Ms. ASHWINI D
(4AI08IS006)

Ms. DIVYA J
(4AI08IS016)

Under the guidance of

Mrs. DEEPASHRI. K. S. B.E., M.Tech
Assistant Professor, Dept of IS & E
Chikmagalur-577102

DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING
ADICHUNCHANAGIRI INSTITUTE OF TECHNOLOGY
(Affiliated to Visvesvaraya Technological University, Belgaum)
Chikmagalur -577 102

ABSTRACT

With the ever increasing amount and variety of data to be stored and transmitted in various mediums, the specification of security which has to be established at various levels of medium access and the accompanying issues of authentication and authorization has become a critical factor. Various Steganographic, watermarking and data-embedding algorithms have usually manipulated the actual data in order to either hide any coveted information or to provide some level of access control over the medium. The mediums are usually images, video, audio etc., wherein specific portions or the overall space is usually 'corrupted' with 'significant' data.

In this proposed system, "Multistage Information Hiding using Novel Visual Cryptography", describes an approach to hide valuable secret information inside the different file formats without losing it by using Steganographic and Cryptographic techniques. The main objective is to never leave anyone to know that information is already hidden in the file. Scalability is also one of the major factors that we are considering. Here we are considering different formats of files (text, image, audio and video). The data (text, image, audio and video) that has to be transferred is embedded in a file (image, audio and video) and encrypted. Encrypted file is further divided into *'n'* shares and each of these *'n'* shares is transferred through different network channels, so that only someone with all *'n'* shares could decrypt the encrypted file, while any *'n-1'* shares revealed no information about the original data. In the next step, encrypted file is decrypted to get embedded file, later this file is decoded to obtain the secrete information.