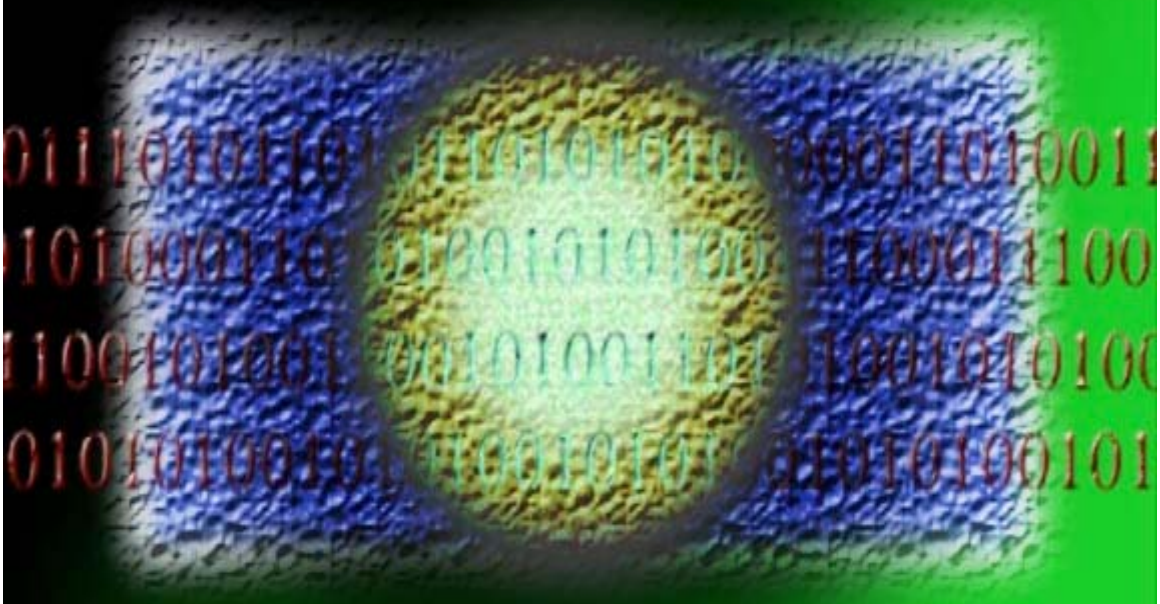
System Architecture
September 30th, 2003



Team ISE

Image Selective Encryption

CSCI 4308-4318, Software Engineering Project
Department of Computer Science
University of Colorado at Boulder

Shinya Daigaku
Geoffery Griffith
Joe Jarchow
Joseph Kadhim
Andrew Pouzeshi

Sponsored by:
Tom Lookabaugh
Assistant Professor of Computer Science

Project Proposal

The selective encryption project (Team ISE) is being sponsored by Assistant Professor of Computer Science, Tom Lookabaugh. Dr. Lookabaugh teaches and researches in the technology and practice of video communication, high technology businesses, and the intersection of policy, innovation, and management. His website contains a great deal of information on his research projects and responsibilities: http://itd.colorado.edu/lookabaugh/.

While many compression techniques have allowed an increase in the flow of traffic across the lines of the Internet, the files they produce are largely unprotected by efficient security measures. They are generally unencrypted and susceptible to unauthorized viewing. Team ISE will be working to incorporate encryption into common compression schemes starting with the JPEG image standard. While the final product is not required to provide more than the classes that would define the encryption and decryption methods, the initial portion of the project is oriented around the research and analysis of the most workable methods for securing compressed files. For this we will be developing a preview and testing suite with a simple graphical interface providing the ability to attack different portions of the compression standard.

The immediate efforts of the team will focus on developing selective encryption for the JPEG standard. If that portion of the project is able to be finished in a reasonable period of time, the team will venture into developing schemes for audio and text compression standards (MP3, zip, etc.)

Therefore the design of the test suite will first be for JPEG development. The test suite will utilize a pattern or process that can easily be extended to other desired formats.

Finally, the team will construct a permanent website which will allow anyone to download the team's previews, products, code and documentation. The site will be constructed on a computer and operating system provided by the Sponsor.

Table of Contents

1. INTRODUCTION

Team ISE is being sponsored by Assistant Professor of Computer Science, Tom Lookabaugh: http://itd.colorado.edu/lookabaugh/.

Selective encryption is intended to utilize the standard formatting of commonly used compression schemes. Targeting small portions of a file that has been or will be divided into pieces defined by the standard algorithm can allow encryption of only a tiny portion of the file. If the target is chosen with care, the encryption can have the effect of damaging the usability of the file for the user who does not have the compatible decryption package.

Team ISE will first be developing a selective encryption scheme for the JPEG image standard. A standard encryption algorithm will be used to encrypt target portions of the file. However, because it is not the goal of Team ISE's project, the team will not be developing or implementing the encryption algorithm. However, the team will include a freely available encryption implementation with the software package. Current encryption candidates are the RC4 stream cipher algorithm and the AES block cipher. However, the team is not limited to these options.

The final product that the team will be providing to the open source community will be methods or classes that will provide the ability to encrypt and decrypt a file created by or used with a standard compression method. These methods or classes will be written in ANSI C/C++. See Figure 1.1 for an overview of the usage of the team's final product. Given a reasonable amount of time the team will also attempt to create selective encryption schemes for other compression standards, such as audio and text.

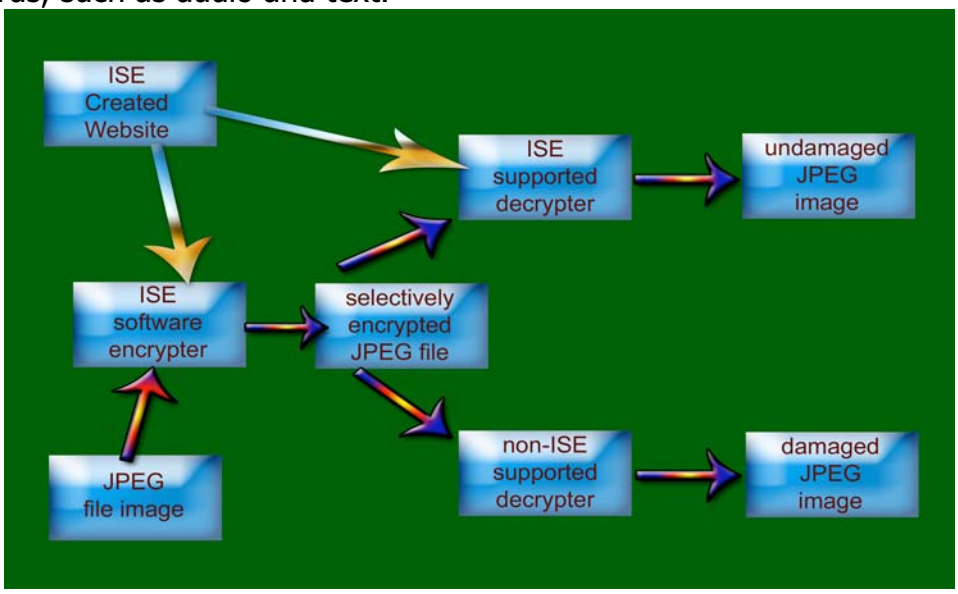


Figure 1.1: Conceptual Overview of ISE Software

To develop this and possibly other products, the team will be creating a test suite for use in establishing a workable encryption scheme. Again, there will be no work by the team to create an encryption algorithm; the target is only the development of a scheme for selective encryption. The intention of selective encryption is that it be such a system that it is possible to use any standard encryption algorithm. The test suite will effectively simulate an end user product. It will utilize a standard encryption algorithm but the end user would not be required to use any algorithm chosen by the team.

There are several necessary functions that the test suite must have. It will first be able to preview a standard file. Each compressed file is divided into separate pieces of information as per the compression standard. Therefore, the test suite will provide the ability to manipulate the various portions of the compression standard in each compressed file. Having manipulated the file, the test suite will be able to preview the encryption attempt without the benefit of compatible decryption. It will also have the ability to preview a standard file that has been both encrypted and decrypted. The decryption options will allow the user try to defeat the encryption methods (let the user put on a black hat.) Any selective encryption scheme could be developed using a package that implemented these features.

The test suite will be developed with Visual Studio C#.

The test suite will use the encryption and decryption classes or methods that the team is developing. The methods will be developed in standard ANSI C/C++, as per the specifications document, and will be able to be called by the test suite.

The website that will be constructed by the team will be on a computer and operating system provided by the Sponsor. It will have a simple home page with links to previews, final product code and to documentation.

This document will primarily define the high-level design architecture for the final product, the test suite, and for the website to be used and developed by the team. For each element of the project, this document will outline the design of invocation, user interface, high-level modular decomposition and file description.

2. INVOCATION

Throughout this document design specifications will be laid out for the final product, the test suite and the website. There will be more or less detail depending on the necessary complexity of the object being described.

2.1. Production Code:

- On invocation, the ISE encrypter will be given an image file path, a flag indicating the target portion(s) of the image for encryption, a step size value for the quality of encryption (the amount or portion of the file to be encrypted), the encryption key file path, (optional) the output file name and path.
- On invocation, the ISE decrypter will be given an encrypted image file path, a flag indicating the target portion(s) of the image for decryption, a step size value for the quality of decryption (the amount or portion fo the file to be decrypted), the decryption key file path, (optional) the output file name and path.

2.2. Test Suite:

- The Previewer will start up as a version 1.1 .NET windowed application using a default test image and an appropriate set of default parameters for the encryption and decryption modules.

2.3. Web Site:

- The web site will be accessed through a fixed IP on the University of Colorado network and will have a home page that will identify the project and provide links to previews, final product code and documentation.

3. USER INTERFACE

The general high-level design for the various user interfaces will be laid out as follows.

3.1. Production Code:

- The user interface will be strictly a command line environment where the command encryption or decryption is given along with the necessary parameters.

  Parameters:
  - int file_type_encryption (image_file_path, target_flag(s), encryption_quality, key_file_path, output_file_path)
  - int file_type_decryption (image_file_path, target_flag(s), decryption_quality, key_file_path, output_file_path)

3.2. Test Suite:

- The test suite will be constructed in Visual Studio C# (see Figure 3.1 below) and will attempt to make development of the selective encryption scheme very organized and straightforward.

- There will be a tab corresponding to each major portion of the compression standard. In the JPEG standard, the compressed file is stored in easily parsible portions and each has a clear identification and purpose (Huffman encoding tables, Quantizer tables, etc..)
- The test suite will have a modular design which will allow the team to scale it to work for other compression formats, such as MP3 and ".zip".

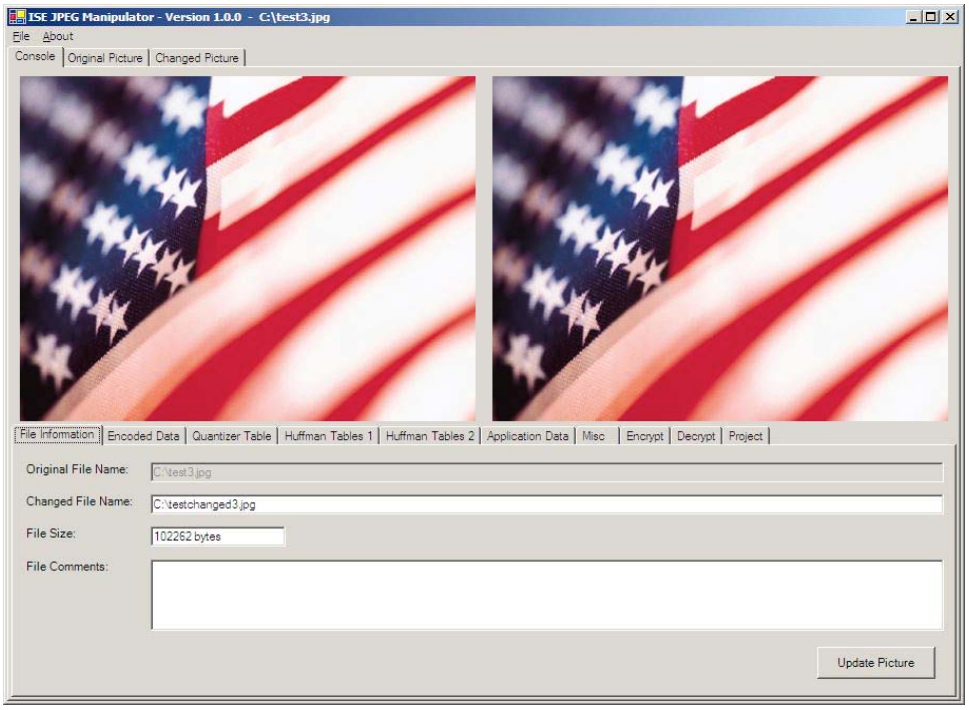


Figure 3.1: Screen Shot of ISE Testing Suite being prototyped

Graphical User interface:

(Comments will only be placed under the items not obvious.)

- Menu Bar
  - File
    - Open project
    - Save project
    - Save project as
    - Exit
  - Help
    - Help
    - About (Will include versioning information.)
- Image Display section
  - Console tab
    - Original image preview
      - Displays the original unmanipulated image.
    - Final output image preview

- Displays the final image after encrypt and decrypt.

- File information tab
  - Will include the original file name and a button to allow opening another file.
  - Will display the output file name and will include a browse button so that the output name can be changed without overwriting any existing files.
  - Will display file size.
  - Will include a section for adding comments to the output file.
- Huffman Encoded Scan Data tab
  - Will display the Scan header.
  - Will display the encoded data (start of scan).
  - If the file is manipulated, this tab will display the original header and the original encoded data for comparison.
- Quantizer Table tab
  - Will display up to 5 quantizer tables and if any are modified will also display the unmanipulated table.
- Huffman Table tab
  - Will display up to 5 Huffman tables and, if any are modified, will also display the unmanipulated tables.
- Application Data tab
  - Fields for up to 10 of the available application data flags.
- Miscellaneous data tab

  Fields for:
  - Restart Interval
  - Number of Lines
  - Expand Image
  - Restart modulo 8 occurred at byte index
  - Hierarchicial Progression
  - Program Errors
- Encryption tab
  - Will have check boxes for all possible flags.
  - Will have radio buttons for any implemented encryption methods.
  - Will display the path to the encryption key and will allow this path to be set or browsed.

        - Will have a field to define the step size for the quality of encryption.
        - Will call the encrypt function outlined in section 3.1.
    - Decryption tab
        - Will have check boxes for all possible flags.
        - Will have radio buttons for any implemented decryption methods.
        - Will display the path to the decryption key and will allow this path to be set or browsed.
        - Will have a field to define the step size for the quality of the decryption.
        - Will call the decrypt function outlined in section 3.1.
    - Project comments tab
        - Will have a field for project comments to be entered and saved with the project.
- Original picture tab
    - Will display the original picture without the size alterations made in the display window.
- Final Image tab
    - Will display the encrypted image without the size alterations made in the display window.

3.3. Web Site:

- The web site will be a very simple construction with a home page directing users to previews, final product code, documentation and test suite.

Figure 3.3.1: Screenshot of ISE Web Page

4. HIGH-LEVEL MODULAR DECOMPOSITION

A high-level modular decomposition of Team ISE's software project is presented in Figure 1.1. The project consists of four main modules:

- ISE Website
- ISE Encryptor
- ISE Decryptor
- Test Suite

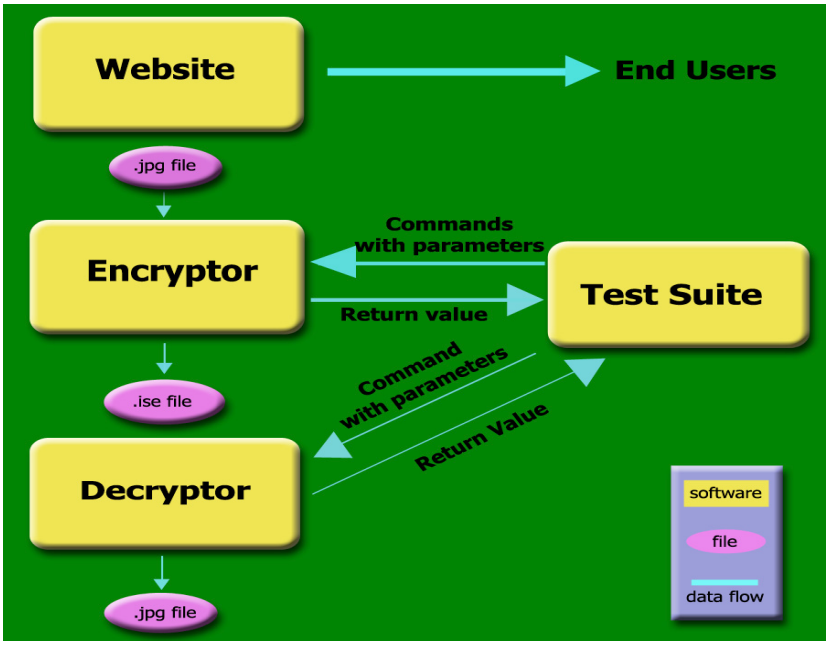


Figure 4.1 High level modular decomposition of ISE

Any comments in Sections 4.2 through 4.4 that seem to apply only to JPEG images can and will be adopted to any other compression standards that the team may attempt during the project.

4.1 ISE Website

- The website will serve as the distributor for Team ISE's software package.
- It will also include links to all documentation provided by the team about the software package and the research behind the implementation.
- The website will display the product and output. This will either be done with a screen shot or a possible test encryption service found at the site.

4.2 ISE Encryptor

- The ISE encryptor will be invoked by a command line call.
- The encryptor will take a few parameters, namely the JPEG filepath, a flag indicating the target portion of the file for encryption, a step size value to define the quality of encryption, the pathname of the location of the key used in the encryption, and an optional output file name and path.
- The encryptor will gracefully terminate if the file imported to it does not end in a ".jpg" extension.
- If the optional file name and path is not included, the encryptor will produce an encrypted file in the current directory with the same name as the orignal JPEG file, however it will contain a ".ise" extension.
- The encryptor module will allow the user to determine which portion(s) of the JPEG file they would like to be encrypted. The portions of the file that can be targeted are defined by the compression standard (these are outlined in Section 3.2 for the JPEG standard.)
- The Module will allow adjustment of the desired quality of encryption. This will vary in implementation between standards. For some formats this will be a percentage of the file to be encrypted. For other formats this might define what portions of the file are to be encrypted.

4.3 ISE Decryptor

- The ISE decryptor will also be invoked by a command line call.
- The decryptor will take the following parameters: encrypted image file path, a flag indicating the target portion of the image for decryption, a step size to define the quality of decryption, the decryption key file path, (optional) the output file name and path.
- Like the encryptor, if an output file name and path is not specified, the decryptor will produce a standard JPEG file with the same name as the encrypted file, however the ".ise" extension will revert back to a ".jpg" extension and a number will be assigned to the end of the file name string("dog.ise" will become "dog001.jpg".)
- The decryptor will gracefully terminate if it is run on a file without the ".ise" extension.
- The decryptor module will allow the user to determine which portion(s) of the file they would like to be decrypted. The portions of the file that can be targetted are defined by the compression standard (these are outlined in Section 3.2 for the JPEG standard.)
- The Module will allow adjustment of the desired quality of decryption. In most cases this would be required to match the encryption step size setting.

4.4 ISE Test Suite

- The ISE Test Suite will provide the team with valuable information about the contents of the compressed JPEG file before and after encryption.
- The Test Suite will also be available to users who wish to view the file changes that can be made to JPEG files using selective encryption.
- It will also display the original and final JPEG images side by side allowing the user to visually compare the differences in image quality. The test suite will implement and include all of the functionality described in section 3.2 for the JPEG standard.

5. FILE DESCRIPTIONS

There are several files that will be used by Team ISE's software package. They will be divided into the following categories:

- Input Files
- Output Files
- Test Suite Files
- Optional Project Extension Files

Again, any comments in the following sections that seem to apply only to the JPEG image standard will be adopted by the team and applied to any other compression standards attempted by the team during the project.

5.1 Input Files

- The encryptor will require standard JPEG files. The file will have to end in ".jpg" and will have to be a standardly recognizable JPEG image.
- The decryptor will require files that have been output by the ISE encryptor ending in the ".ise" extension.

5.2 Output Files

- The encryptor will produce encrypted JPEG files ending in a ".ise" extension
- The decryptor will produce standard JPEG files ending in a ".jpg" extension

5.3 Test Suite Files

- The test suite will require standard JPEG files. The file will have to end in ".jpg" and will have to be a standardly recognizable JPEG image.

5.4 Optional Project Extension Files

- Time permitting, Team ISE will provide encryption and decryption modules to selectively encrypt other file formats, for example MP3 or ".zip" files. In this case, the encryptor will work on files ending in the standard extensions for these compression methods, and will produce selectively encrypted files with ."ise" extensions. The decryptor module will work on files with this new extension and reproduce the original files with their standard file extensions. Again, this is potential additional work to be performed by Team ISE. The main goal of the project is the production of JPEG encryption and decryption modules.

6. SUMMARY

This has been a very high-level view of the initial thoughts on a system architecture for Team ISE's selective encryption project. The document includes information on the architecture of the final encryption and decryption modules, the team's distribution website, as well as extensive planning on important tools which will be implemented for the team's reseach, development and testing. These tools will be available to users who wish to view the inner workings of the selective encryption methods. Thought was also given to the scalability of the project, specifically the inclusion of encryption and decryption modules for compression standards other than JPEG. The design and architecture allows for the extension of the available modules to other formats. It should serve as a strong beginning from which the team can start prototyping. It will also allow the team to begin the formulation of a more detailed design of the product.