Requirement Specification

31 October 2003

Team ISE

Image Selective Encryption

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

Shinya Daigaku
Geoffrey Griffith
Joe Jarchow
Joseph Kadhim
Andrew Pouzeshi

Sponsored by:
Tom Lookabaugh
Assistant Professor of Computer Science

Project Proposal

A constant amount of traffic flows between computers connected to the Internet. A large volume of information may take a long time traveling from destination to destination. The resulting speed reduction makes it desirable to compress the file as much as possible in order to send the smallest amount of data. Compression of data has allowed for the high-speed data transfers that have made Internet communication and business very workable.

In addition to sending the smallest amount of information possible, users also attempt to maintain a certain level of security upon their information. Due to the fact that common encryption methods generally manipulate an entire file, most encryption algorithms tend to make the transfer of information more costly in terms of time and bandwidth. Thus, users pay a price for security relative to their desired level of security. One possible solution would be a system of encryption that works cooperatively with the standard compression schemes. *Selective Encryption* of only a small percentage of the file's bits will facilitate this solution. Because most encryption schemes will make the file larger, selective encryption seeks only to encrypt portions of the file that will make it unusable. In other words, if a user does not have the proper decryption device, the file should not be usable. Selective encryption will minimize the necessary increase in file size due to encryption while maintaining a maximum level of uselessness, or damage, to the product.

An image could be encrypted with any of the sufficiently secure encryption algorithms available to the open source community, but this will usually result in a dramatic increase in file size that will severely increase transfer time over the Internet. However, selecting key parts of a file for encryption and only encoding those bits can actually render an image unusable. The initial statistical analysis done by the team will consist of specifically breaking down the standard JPEG compression scheme into its usable parts and evaluate which of these, if encrypted, will cause a potential user to pay for rights to the image or force subscription to the provider service.

Team ISE (Image Selective Encryption) will deliver a package for selectively encrypting JPEG (Joint Photographic Experts Group) still image files. The package will provide the tools necessary to encrypt the critical information of a JPEG file in cooperation with existing standard compression tools. This package will handle JPEG files in such a way that only a small percentage of the total file will be encrypted. Selective Encryption security will not extend to the level of military secrecy, but rather a level that would deter all but brute force attacks, allowing users to securely protect private JPEG images.

An additional aspect of the encryption analysis will be the determination of the specific targets in the file for encryption. For example in an MPEG file there are headers that contain a small portion of the overall number of bits but which are extremely vital to the reproduction of the movie by the user. So, if certain headers were to be encrypted the percentage of the file being manipulated would be less than ten percent of the total number of bits in the file. Although only a small portion will be encrypted, the resulting damage experienced by an unauthorized user would be sufficient to cause the user to pay for the decryption package. However, there are other targets that, while they can be encrypted and will do sufficient damage, can be guessed by an attacker. The attacker could, with some degree off effort, render the file useful without use of the decryption software. For example, if the frame rate of an MPEG file was encrypted, an attacker could try all three of most common frame rates and one of these is certain to produce the correct rate for the particular video. In the case of JPEG Selective Encryption, Team ISE will have to balance the targets for encryption against ease of simple attacks.

A permanent website will be constructed by the team to make the software package available to anyone interested in the software process. As it is vital to the world of cryptography to let the community view the approach, the first form of the working prototype will be made available on the website. From this, feedback can be received not only from the team itself, but also from the cryptography community at large.

So, following the guidelines of the ongoing MPEG research (also being guided by the sponsor), the team will study the JPEG process and earlier attempts at encryption. With the sponsor's assistance, Team ISE will devise a workable approach to handling individual JPEG images following the concept of selective encryption.

It is possible that the team will complete the JPEG process early enough in the year that they will able to apply the same approach to other types of compressed files (text, audio, etc.) However, this initial specifications document applies only to the envisioned JPEG project.

Table of Contents

1. INTRODUCTION

Team ISE is being sponsored by Assistant Professor of Computer Science, Tom Lookabaugh, at the University of Colorado: http://itd.colorado.edu/lookabaugh/. Tom Lookabaugh is currently involved in selective encryption research on standard MPEG (Moving Picture Experts Group) files and is interested in researching the application of Selective Encryption for other multimedia formats.

The goal of selective encryption is to minimize the amount of encryption applied to a file while maximizing the damage done to the image being viewed by a user not in possession of the authorized decryption package. Complete encryption is not a requirement of the process, nor is rendering the file useless to the level of complete military secrecy. It is acceptable for an attacker to be able to view portions of the file; however, the file should be distorted enough that an attacker would not wish to use the encrypted file, but would rather purchase or subscribe to the decryption method for access to the original files.

Multimedia files prove to be a good subject for selective encryption, as these files tend to be very large and employ compression algorithms that concentrate critical information in small portions of their bit stream. If the critical data in certain multimedia standards is encrypted properly, the remaining information becomes useless to those without the appropriate decrypter. There are many types of compression algorithms that fit this description, such as MPEG 1, 2 and 4 video, G.723 and G.729 video, AAC audio, MP3 audio, JPEG and JPEG2000 image formats. Applying a Selective Encryption security solution to selected multimedia formats will greatly increase the protection level of important information.

The focus of the ISE project is to research and develop an algorithm for selectively encrypting the JPEG *baseline* compression image standard. The product of the research and development will be a package that will encrypt a file so that the amount of the file being encrypted is relatively small (on the order of 1-2% of the total file). The product will be delivered in a package that will include an encrypter and a decrypter for JPEG files, a website to facilitate the delivery of the product and documentation about the process. The encrypter and decrypter will encrypt and decrypted selected targets contained within JPEG files. The ISE project will employ the AES (Advanced Encryption Standard) for our Selective Encryption algorithm. This package will be made available in a purely open source form on our final website.

In addition to the package containing the decrypter and encrypter, Team ISE will also provide a test suite available to prospective users. The test suite will be used to aid in the research, development and testing of the team's final product. The test suite will provide the functions necessary to completing this project. First, it will allow the user to preview a standard JPEG image. Second, the test suite break down the various portions of a JPEG image and provide the ability to manipulate the data of all of the pieces the particular file. Third, after altering the data in any particular file, the test suite will provide the capability to preview the encryption attempt without the benefit of compatible decryption. Forth, the suite will have the ability to decrypt an encrypted file. 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, however, the delivered test suite will only employ the AES encryption scheme chosen by the team. The test suite will be available to download from the team website.

The final website will be deployed on a sponsor provided Apache web servers. The machine facilitating the web server will use the Linux Red Hat 9.0 operating system platform. The team will acquire a fixed IP address from the proper University of Colorado authorities and will develop a simple website capable of delivering information to viewers about the benefits and application of Selective Encryption technology. The site will provide users the option to download and use the final software package. The site will also provide links to important information and will remain in place as long as the sponsor deems necessary.

The envisioned software package will accomplish the complex task of selectively encrypting a JPEG baseline standard image, while providing a simple user interface to users. Team ISE has identified three specific types of users: high-end art users, typical Internet image users, and small, low-end image users. The research and software will be tailored to these users' needs. Figure 1.1 is a flow chart showing the general logic design of the team's final product.

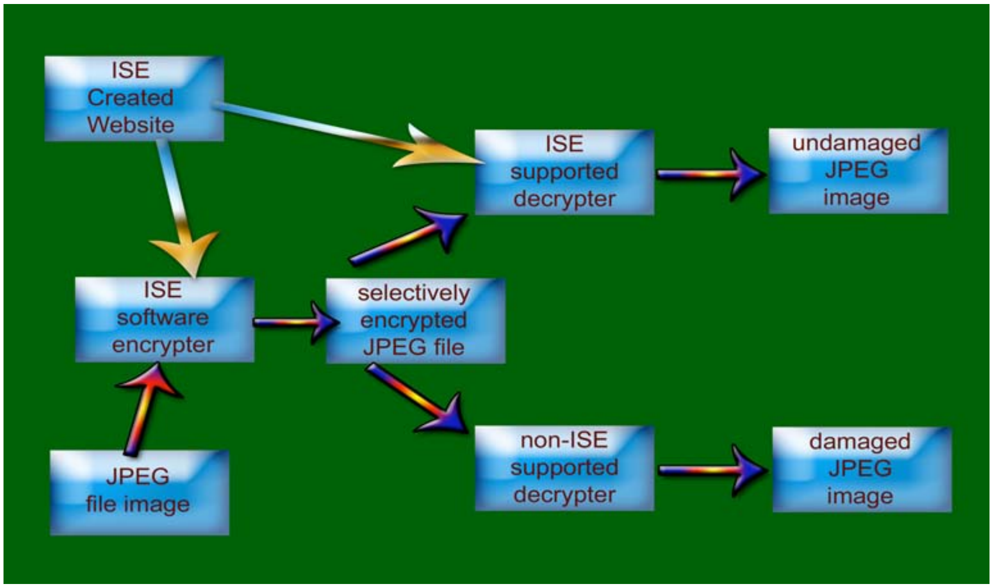


Figure 1.1: Conceptual Overview of ISE Software

Information regarding the research required by the sponsor is further outlined in the next section. Details regarding the requirements of Team ISE's Selective Encryption project are then presented, followed by short discussions of possible requirements alternatives and future enhancements. These details are concluded with a summary followed by a glossary of important terms and a list of related readings.

2. RESEARCH PATH

➢ 2.1. Research and Analysis Requirements

The research and analysis will be the initial part of this project. The final product of the research will allow the team to determine a specific approach to this form of Selective Encryption. The sponsor considers the research done by the team equally as important as the delivery of the final product. The research portion of this project will include:

- A proportional analysis of a large quantity of JPEG images to define what might be acceptable targets within the JPEG file structure for encryption.
- An analysis of earlier methods of encryption for performance and effectiveness.
- The analysis of potential encryption methods and targets in the JPEG image file for percentage of file encryption vs. image corruption.
- The analysis of different encryption methods and targets in the JPEG image file for the encryption target's susceptibility to potential attack.
- The final stage of the research analysis will conclude with approval from the sponsor on the useful approaches and corresponding performance issues.

➢ 2.2. Research Related Products

Following significant discoveries throughout the project the Sponsor requires that the team will produce research documentation to be presented at applicable security and compression conferences.

3. REQUIREMENTS

The requirements have been divided into several sections based upon the category of the requirement. These categories consist of the Supporting Environment, Functional, Performance, Documentation and Release Requirements. Each of the requirements is defined below.

➢ 3.1. Supporting Environment

The supporting environment includes specification of both the expected environments that the package should be able to perform in and the form in which the package will be written. There is also a specification of the minimum hardware environment the package will require to be run on. The package referred to in the requirements consists of the encryption and decryption package. The test suite is not a portion of this package, and has its own runtime and language requirements.

- **3.1.1. Software**

  The supporting software environment includes the runtime environment as well as the development requirements.
  - **3.1.1.1. Runtime Environment**
    - ❖ Package to be operational in Linux Red Hat 9.0, Windows XP and Mac OS X.
    - ❖ The test suite is to be operational in a .NET environment.
    - ❖ Web page is to be viewable on Internet Explorer 6.0 and Safari 1.0.

  - **3.1.1.2. Development Environment**
    - ❖ Package to be written in ANSI C/C++ specification.
    - ❖ Package should not change IJG's claim of wide portability (see http://www.ijg.org for specific environments).
    - ❖ CVS will be used for software versioning.
    - ❖ Test suite to be written in the C# (C-sharp) programming language.
    - ❖ The web page will be built on a server utilizing Linux Red Hat 9.0 operating system, supplied by the sponsor.
      - ✓ Web page will use HTML version 4.01.

- **3.1.2. Hardware**
  - Package should be able to be run on any computer system supporting color graphics.
  - Generic color monitor and JPEG image viewing system outlined above.
  - Keyboard as part of the user interface.
  - Hardware supports the software environment outlined above.

3.2. Functional Requirements

The functional requirements specify all of the functionality Team ISE's product is required to provide. These requirements will include the interface to our production code and outline the functionality that must be supported. The requirements of the test suite and web page will also be listed in this section.

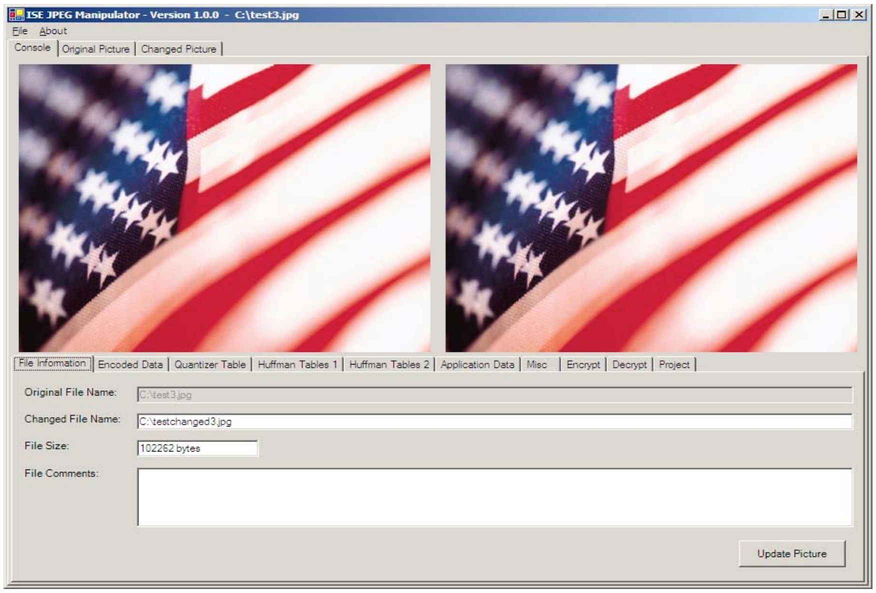
- **3.2.1. Required Operations**
  - Encrypt a selected portion of a JPEG baseline standard image compression format.
  - Decrypted files must maintain compliance to the JPEG compression standard.
  - Level of encryption is not "secretive/military" but level to provide sufficient protect against all but brute force attacks.

- **3.2.2. Package Functionality**
  - Must be able to read in .jpg or files for encryption.
    - Encryption software must gracefully terminate upon receipt of other file types.
  - Must output a file ending with an .ise extension. The .ise extension denotes a Team ISE selectively encrypted file.
  - Decrypt module will input and process .ise file types.
    - Decryption software must gracefully terminate upon receipt of other file types.
  - Decrypt will output a standard .jpg file.
  - Final product will be a software package that provides simple interface methods.

- **3.2.3. ISE Function Interfaces**

  This section illustrates the pseudo code form that the Team ISE Selective Encryption package interface methods must have.
  - int selectiveEncryption(ifstream &input_file_stream, ofstream &output_file_stream, char* key_material, char* encrypt_flags, int num_flags, int quality);
  - int selectiveDecryption(ifstream &input_file_stream, ofstream &output_file_stream, char* key_material, char* decrypt_flags, int num_flags, int quality);

- **3.2.4. Test Suite Requirements**
  - **3.2.4.1 Test Suite Display**
    - ❖ The test suite must have a standard windows display.
    - ❖ The test suite must include buttons and tabs to display different portions of the JPEG image file data.
    - ❖ Figure 3.2.4.1 displays a screenshot of the test suite.



Original File Name: C:\test3.jpg

Changed File Name: C:\testchanged3.jpg

File Size: 102262 bytes

File Comments:

Figure 3.2.4.1 Test Suite Screen Shot.

  - **3.2.4.2 Test Suite Functionality**
    - ❖ The test suite must be able to parse compressed JPEG files.
    - ❖ The test suite must divide up and display the hexadecimal values of the different pieces of a JPEG file.
    - ❖ Display the manipulated image of the file alongside the original image. The image size will be altered to fill the display windows.
    - ❖ The test suite must allow the user to make changes to the data contained in each of the pieces of a JPEG file.
      - ✓ These changes must be incorporated into the encoding of the file, and the image displayed must be updated to be the image produced by the changes in the encoding.
    - ❖ Include tabs to display the image without altering its size.
    - ❖ Incorporate the encryption and decryption software methods provided in the final software product.
      - ✓ The test suite will provide a graphical user interface for the final Team ISE product package.

- ❖ Provide options for the user to save all of the information and changes to the current image.

- **3.2.5 Supporting Web Page**
  - To be deployed on machine provided by the sponsor.
  - Contain links explaining the purpose of the software package provided by Team ISE.
  - Contain links to downloadable version of the software package.
  - Contain links to downloadable version of the test suit package.
  - Contain links to the software documentation as well as providing the user with the ability to download the documentation.
  - Contain open source files of the software package.
  - Contain links to other sources of related information.
  - Contain information about the sponsor.
  - Contain information about Team ISE.

3.3. Documentation and Release Requirements

The following requirements specify the documentation that is to be provided, along with issues related to the release and delivery of the final product.

- **3.3.1. Documentation Requirements**
  - Man Page - A standard UNIX man page.
  - User Tutorial - A presentation of system for first-time user.
  - Research paper(s) written in a style specified by the sponsor.
  - A website to include all code and documentation and supporting links.
  - Documents will be made available in Adobe PDF file format.

- **3.3.2. Release Requirements**
  - Product will be delivered as series of ZIP files for Unix, Windows and Mac users.
  - Files will include installation programs for automatic generation and installation of executable and preview/evaluation programs.
  - Documentation will be provided on the website for download.

4. Future Enhancements

Pending the early completion of the JPEG selective encryption methods and software, the following enhancements may be incorporated into the final product. These enhancements illustrate the development of selective encryption, and its spread into other areas in the future.

➢ 4.1 Selective Encryption of MP3 Files

The project may be extended to include the MP3 file format. The team will research MP3 file formats and devise ways of selectively encrypting MP3 files. Completion of this will entail expanding the encrypter/decrypter software to include MP3 files. The software will output selectively encrypted MP3 files. For security and consistency, these encrypted files will have the same ".ise" extension as the encrypted JPEG files. The test suite will also be expanded to parse MP3 files and display the encoding to the user. Documentation will be updated to include descriptions of the MP3 encoder/decoder. Research papers involving MP3 selective encryption will be produced upon the Sponsor's request. The website will be updated to include all pertinent MP3 information.

➢ 4.2 Selective Encryption of ZIP Files

Upon completion of both the JPEG and MP3 selective encryption targets, the project will be further extended to the ZIP file format. Team ISE will update the encrypter/decrypter software to perform upon ZIP file types. Again, for security and consistency, selectively encrypted ZIP files will end in the ".ise" extension. Research will be done to determine how to best perform selective encryption upon ZIP files. The test suite will again be expanded to parse ZIP files and display the encoding to the user. Documentation will be updated to include descriptions of the ZIP encoder/decoder. Research papers involving ZIP selective encryption will be produced upon the Sponsor's request. The website will be updated to include all pertinent ZIP information.

5. SUMMARY

The purpose of this document was to give an outline for the path of research and the set of requirements for the ISE software package. These requirements include the software and hardware environments the application will run on, the functional requirements of the software, test suite and website, the research and analytic requirements, and the supporting and research document's requirements that will be included along with the software package. This document includes all necessary information for designing all of the necessary aspects of the Team ISE software.

6. Glossary

AES (Advanced Encryption Standard)

An encryption method that uses block ciphering.

ANSI C/C++

The standard C and C++ programming languages as defined by the American National Standards Institute.

Black Hat

The process of testing an encryption algorithm by trying to break the encryption using several different methods.

Baseline JPEG

A subset mode of sequential JPEG where the number of tables is restricted and the sample precision must be eight bits.

C#

A modern, object-oriented language that enables programmers to quickly build a wide range of applications for the new Microsoft .NET platform.

Compression Algorithm

An algorithm designed to compress a file, that is, utilizes patterns in a file to reduce the size of the file.

CVS (Concurrent Versioning System)

A code management system. CVS provides the ability to track (and potentially revert) incremental changes to files, reporting them to a mailing list as they are made, and can be used concurrently by many developers.

Decryption

The act of rendering an encrypted file into a know format.

Encryption

To convert computer data or messages to something incomprehensible by means of a key, so that only an authorized recipient holding the matching key can recover the original.

IJG (Independent JPEG Group)

An informal group that writes and distributes a widely used free library for JPEG image compression. IJG is not affiliated with the ISO committee.
www.ijg.org/

ISO (International Organization for Standardization)

The world's largest developer of standards, particularly the development of technical standard.

JPEG (Joint Photographic Experts Group)

A compression technique for color images and photographs that balances compression against loss of detail in the image. The greater the compression, the more information is lost (this is called Lossy compression).

Military Secrecy

A level of secrecy where all information is hidden.

MP3 (MPEG-1 Audio Layer-3)

A standard technology and format for compression a sound sequence into a very small file (about one-twelfth the size of the original file) while preserving the original level of sound quality when it is played.

MPEG (Moving Picture Experts Group)

A standard for digital video and audio compression.

Selective Encryption

A method of encryption that exploits the relationship between encryption and compression to reduce encryption requirements, saving in complexity and facilitating new system functionality. Selective Encryption only encrypts a small portion of a file.

Visual Studio .NET

Microsoft's visual programming environment for creating web services based on use of the Extensible Markup Language (XML).

ZIP

A method of compressing text files.

7. Related Readings

[Lookabaugh and Sicker and Keaton and Gua and Vedula 2003]

Lookabaugh, T., and Sicker, D., and Keation, D., and Guo, W., and Vedula, I. *Security Analysis of Selectively Encrypted MPEG-e Streams*. 2003.

Tom Lookabaugh's description of the methods and results of applying selective encryption to MPEG-2 streams.

[Miano 99]

Miano, J. *Compressed Image File Formats*. Addison Wesley Longman, Inc., Reading, Massachusetts, 1999.