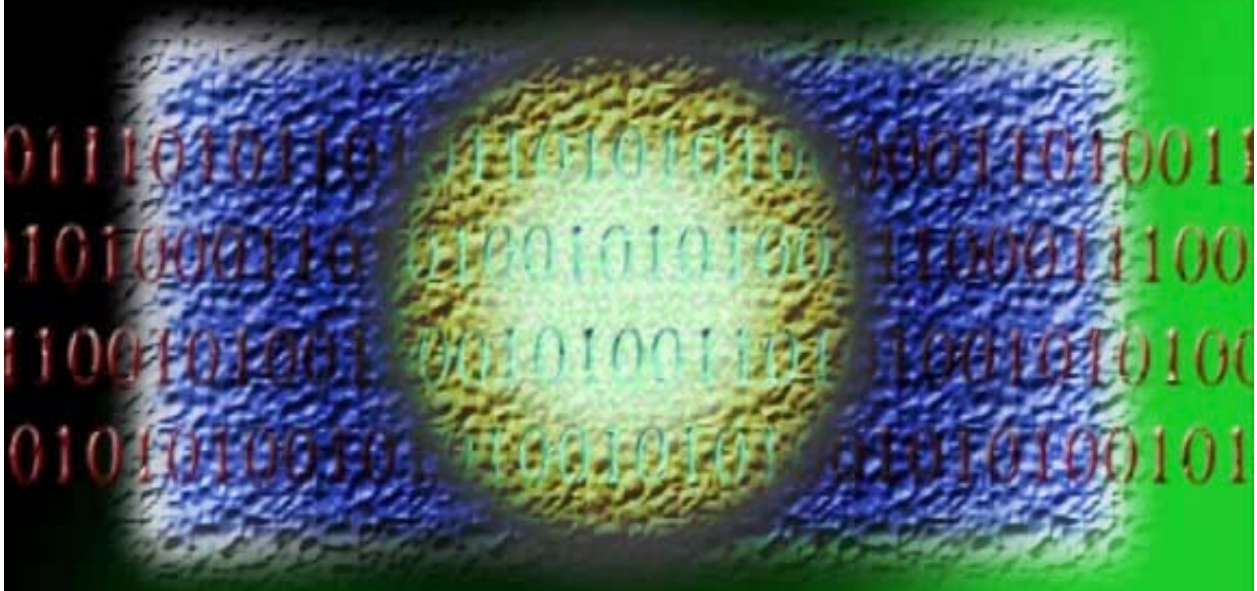
Initial Requirements
September 19th, 2003



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
Associate 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. 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 seek to balance the necessary increase in file size, or bandwidth, 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 prohibit transfer 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 evaluating which of these, if encrypted, will cause a potential user to pay for or subscribe to the decryption service.

Team ISE (Image Selective Encryption) will deliver a package for selectively encrypting JPEG 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. The level of encryption will not reach to the height of military secrecy, but rather a level that would thwart most simple attacks while causing potential users to pay for viewing the image.

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 10% 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 at by an attacker. The attacker could, with some degree off effort, render the file useful without use of the decryption software. For example if one encrypted the frame rate of an MPEG file, an attacker could just guess at the 3 most common frame rates, and one is certain to produce a correct copy of the video. Again, 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

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 to 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. This is due to the fact that the multimedia files tend to be very large and their compression algorithms concentrate critical information in small portions of this bit stream. If the critical information is encrypted, the remaining information becomes useless to those without the proper decoder. There are many types of compression algorithms that fit this description. Examples of such are MPEG 1, 2 and 4 video, AAC audio, G.723 and G.729 video, and JPEG and JPEG2000 image.

The focus of this project is to research and develop an algorithm for selective encryption of a standard baseline compressed JPEG image file. This process must encrypt a file in such a way that the amount of the file being encrypted is relatively small, yet the damage done to the file is on a scale that would render the file useless without a proper decryption device. This process will be delivered in a package that will include an encrypter for JPEG files and a decrypter that will reverse the operation. This package will be made available in a fully open source form on the website that will be constructed by the team.

The website is to be constructed on a server being purchased by the Sponsor in an environment that will match the other computers in the working lab. The team will acquire a fixed IP address from the proper University authorities and will set up a simple website capable of informing viewers about the possibilities of the technology of Selective Encryption and to provide them with a package they can download and test. The site will provide links to important information and will remain up permanently even once the project is complete.

The envisioned software package will accomplish a seemingly simple result while being extremely effective and usable to the appropriate users. Below is a flow chart showing the general picture of the package's operations. (Figure 1.1.)

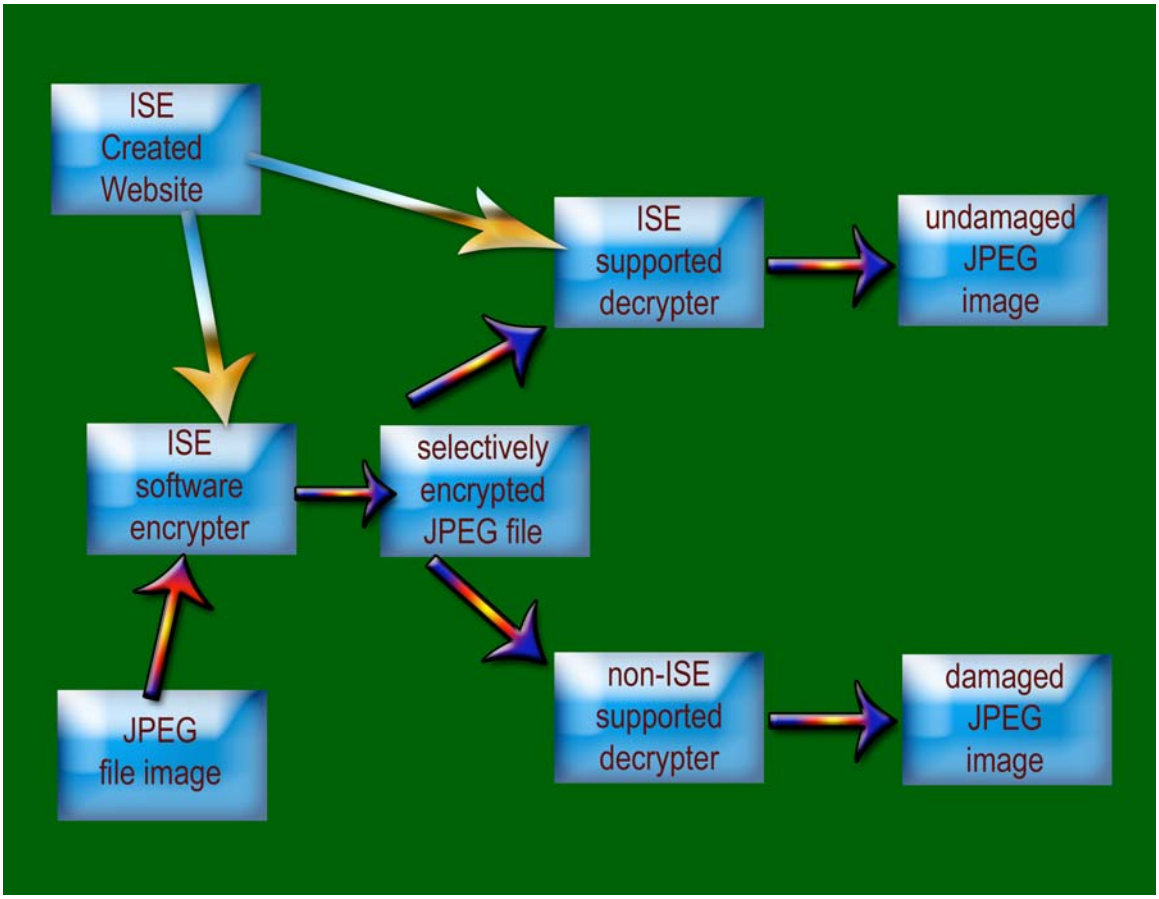


Figure 1.1: Conceptual Overview of ISE Software

The ISE website displayed in the flow chart will be used to distribute the ISE software and will also contain information on the product as well as the research behind it.

The list of requirements for ISE follows. As there is a degree of research that must be done by the team under the Sponsor's guidance and supervision, the general path of the research is given as a precursor to the actual final product requirements. Further, as this research will to some degree determine the final necessary requirements, this document will serve as a starting point for the project, but will be refined later.

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 this process is essentially a completely determined approach.

- Proportional Analysis of a large quantity of JPEG images to define what might be acceptable targets within the JPEG file structure for encryption.
- Analysis of earlier methods of encryption for performance and effectiveness.

- Analysis of different encryption methods and targets in the JPEG image file for percentage of file encryption vs. image corruption.
- Analysis of different encryption methods and targets in the JPEG image file for the encryption target's susceptibility to attack.
- Final stage of the research analysis will evaluate and get approved by the Sponsor an acceptable performance evaluation taking into account all necessary factors that the research will review.

3. REQUIREMENTS

The requirements have been divided into several logical sections. These sections include the requirements of the Supporting Environment, Functional Requirements, Performance Requirements, and Documentation and Release Requirements.

➢ 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 basic specification of the hardware environment the package will require to be run in.

- **3.1.1. Software**
  - Package to be operational in Linux Red Hat 9.0, Windows XP and Mac OS X.
  - Package to be written in ANSI C/C++ incorporating the Independent JPEG Group (IJG) package.
  - Package should not change IJG's claim of wide portability (see http://www.ijg.org for specific environments.)
  - Web page will be built on a server and OS supplied by the Sponsor.
    - ✓ Web page to be viewable on Internet Explorer 6 and Safari 1.0.
    - ✓ 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.
  - Mouse, and Keyboard.
  - Hardware supports the software environment outlined above.

➢ 3.2. Functional Requirements

Functional Requirements specify all of the functionality that ISE is required to provide. This includes functionality interfacing to the software package, and the

commands supported by the software package. The requirements of the web page created to support the package will also be listed in this section.

- **3.2.1. Required Operations**
    - Encrypt a standard image file in cooperation with the standard JPEG encoding format.
    - Maintain compliance to the JPEG compression standard.
    - Decrypt a standard compressed JPEG image file in cooperation with the Standard JPEG decoding format.
    - Level of encryption is not "secretive/military" but only to level of damage that would force subscription to image viewing.
    - Time permitting; the package will also selectively encrypt audio files, possible mp3 or AC3, and/or text files, such as zip files. However, these are secondary options. The main goal of the project is to deliver a package that selectively encrypts JPEG files.
        - Any attempt at these secondary projects would follow the same line of research into implementation.

- **3.2.2. Interface to Package**

    - Must be able to read in either .jpg or .bmp files for encryption.
    - Research will determine what file type the encryption module will output.
    - Decrypt module will input the appropriate file type.
    - Decrypt will output a standard .jpg file.
    - Final product will be a software package with command line user interface and appropriate incorporation into the standard JPEG tools.

- **3.2.3. Commands for software package**

    - Encrypt -- take a standard .jpg or .bmp file and convert to an encrypted JPEG file.
    - Decrypt -- take an encrypted JPEG file and convert to a standard .jpg file.

- **3.2.4 Supporting Web Page**

    - To be built on server and OS provided by 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 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.

➢ 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 -- standard UNIX man page.
  - User Tutorial -- presentation of system for first-time user.
  - Research paper written up in style of the Sponsor's MPEG reference paper.
  - Web site to include all code and documentation and supporting links.

- **3.3.2. Release Requirements**

  - Delivered as zipped files for Unix, Windows and Mac users.
  - File will include entire source tree of software
  - File will include installation programs for automatic generation and installation of executable and preview/evaluation programs.
  - Documentation provided only on the website for download.

4. SUMMARY

The purpose of this document was to give an initial 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, the research and analytic requirements, and the supporting and research document's requirements that will be included along with the software package. These requirements will be modified at a later date when more information is known about completing the software package.