TEAM ISE DEVELOPER'S REFERENCE

Team ISE has deemed it necessary to supply those who will follow in our footsteps with answers to questions that will inevitably arise. Therefore, we have created a document broken down into three sections, one for each of the main products that we produced over the last year. The sections cover questions over the ISE Manipulator, Production Code, and Website. We also recommend viewing all of the documentation on our website. You can view to each section by clicking on one of the following links:

ISE Manipulator
ISE Production Code
ISE Website

Also, Dr. Tom Lookabaugh at the University of Colorado at Boulder is responsible for maintaining all of the code and research produced by Team ISE. If you have questions or comments about any of the code, documentation or other items created by Team ISE, please contact Dr. Lookabaugh using the contact information given on the ISE Website. We hope you have as much fun and learn as much as we did – Good Luck!!!

Sincerely,

Team ISE
CSCI 4308 – 4318: Senior Project
University of Colorado at Boulder

ISE Manipulator

What is the ISE JPEG Manipulator?
The ISE JPEG Manipulator is a Windows application written in the C# (pronounced "Cee-Sharp") programming language and is design to allow the user to analyze and create JPEG images, based on the data from pre-existing JPEG images. The JPEG Manipulator was designed to help Team ISE with research during the course of the project. The Manipulator is extremely useful in determining how data (random or chosen) will react when integrated into a JPEG image. It is also a nice tool for analyzing the file structure of a JPEG image.
back

What does each of the code files do?
There are a total of four necessary code files included with the JPEG Manipulator. First, the most used code file is the frmMain.cs. This is the Main Form of the JPEG Manipulator and contains the frmMain form class and all of the code necessary to implement the base functionality of the Manipulator. The frmMain form class is directly inherited from the System.Windows.Forms class and provides the additional functionality as a series of methods in the class. Second, frmLoad.cs is the code file for the frmLoad form class inherited directly from the System.Windows.Forms class. This code was developed to provide a loading form to be displayed when a new image is loaded into the Manipulator. All of the functionality for this class is contained within the frmLoad.cs file and can be used as a separate .NET component. Third, the frmAbout.cs contains all of the code necessary to implement the frmAbout form class in the Manipulator. This class is also inherited directly form the System.Windows.Forms class. The fourth file is the frmSplash.cs code file. This file contains all of the necessary code to implement the frmSplash form class and is directly inherited from the System.Windows.Forms class. Please note that the latter 3 files are quite small, only a couple hundred of lines of code each, and only implement the functionality for the form's purpose.
back

Where can I find an in-depth design of the Manipulator?
There are several documents produced by Team ISE that explain the design for the ISE Manipulator. The ISE System Architecture document provides a nice high-level design of the ISE Manipulator. In addition, the ISE Design Specification provides an in-depth, high-level design as well as a description of each of the Methods necessary to fully develop the frmMain form. Also, for the convenience of future developers, the ISE Manipulator code, object and DLL files contain XML comments for each of the Methods

in the frmMain class, so that Visual Studio's Intellisense will display those comments (along with parameter details and return value information) in the comment viewer and in the Visual Studio Object Brower. This documentation is available at the [website](#).
[back](#)

What do I need to compile the Manipulator code?

Although it is not required, Team ISE highly recommends working with Visual Studio .NET when creating and compiling this code. We have included a Visual Studio Solution file that contains all of the necessary file data to create, manage and build these codes very easily. This Solution file contains two Project files, one for the Manipulator itself and one for the Manipulator Installer package. But, since this is a .NET application, the only software truly necessary to build this program is the .NET framework. If the development machine does not have Visual Studio available, the developer always has the option of building the executable from calls to the command line compiler built into the .NET framework. For more information about using the command line compiler, please see www.microsoft.com/msdn. Again, Team ISE recommends using Visual Studio to manage and build these code files using the Solution file provided with the final distribution package.
[back](#)

What version of .NET was used for the Manipulator?

Version 1.1 of the .NET framework was used to develop the ISE Manipulator, but we believe it could be compiled with ANY version of the .NET framework (including the older 1.0 version). We have included the .NET framework re-distributable package for Windows with the final distribution package. Also, the .NET framework and can be attained by downloading it from [Microsoft](#), if unavailable otherwise.
[back](#)

[Back to top](#)

ISE Production Code

What is the ISE Class?
The ISE Class is a C++ super-class, specifically designed to serve as a base for any selective encryption/decryption class targeted for compressed media. It contains all of the necessary methods and data members needed to construct an object for selective encryption, except for the actual encrypt and decrypt methods. Because the algorithms for selective encryption and decryption are uniquely tailored to a specific file type, these methods must be implemented in an inheriting class, such as the JPEG_ISE Class. When the JPEG_ISE class was implemented the code was written only to deal with standard baseline JPEG images.
back

How can I extend the ISE Class?
There are a number of steps required to inherit the ISE super class. First, one must design an algorithm to selectively encrypt a specified file type. These algorithms are then implemented within the inheriting class by defining the two virtual methods: encrypt_file() and decrypt_file(). All other protected methods within the super class are accessible by the inheriting class as needed.
back

Do I need to make my own constructor?
No, the ISE super class implements an overloaded constructor that should be used to construct any object inherited from ISE. **Note:** that the default constructor is declared protected and forces the class user to call the overloaded constructor. Also note that there are many ways to use the overloaded constructor. The only necessary parameter is the encryption/decryption key, but the user may also specify an input and output file.
back

Why are there only two files associated with an ISE object?
An ISE object can be used for either encryption or decryption. In each case, the only necessary data members are the input and an output file names. Setting these data members is dependent on the direction (encrypt or decrypt) of the object.
back

What methods does my inherited class have available to it?
There are a number of methods implemented in the super class. An inheriting class may use all of these methods.   The methods available are:

> ise constructor
> set_key
> set_input_file_name
> set_output_file_name
> get_input_file_name
> get_output_file_name
> make_ise_file_name
> make_output_file_name
> get_ise_file_type

These functions allow for the manipulation of all the ISE object data members. A full description of each of these methods can be found at the associated link to the production code reference.
back

What methods will my inherited class need to implement?
There are only two methods an inheriting class needs to implement: encrypt file() and decrypt_file(). Both of these methods do not take any parameters and should use the data members of the object to selectively encrypt or decrypt a file. The algorithm for the encryption must be discovered through researching a given file type.
back

What changes to the ISE class should I make to implement my selective encryption class?
Aside from implementing the encrypt_file() and decrypt_file() functionality, there are minor changes that must be made to the super class. Every ISE file type must have a unique ID to be appended to the front of an ISE encrypted file in order to determine the original file type. JPEG ISE files have a '1' as the ID. Also, the IDs '2' and '3' are reserved for mp3 and zip respectively, though their corresponding classes are yet to be defined. These changes need to be made in the ise get_ise_file_type() method and should be considered when creating the encrypt and decrypt functionality.
back

How do I design a selective encryption algorithm for my media file type?

There are a number of steps needed to design a new selective encryption algorithm. First, decide on which compressed media you would like encrypted and study its compression standard. Next, identify what portions of the file make good/bad targets for encryption. These targets should be evaluated for properties conducive to selective encryption. The factors to consider might be the portion of the file dedicated to the target, amount of damage to the file when the target is encrypted and how hard the encryption would be to break. The third step to designing a selective encryption algorithm is choosing the encryption. Team ISE used AES encryption, though other encryption algorithms may be used. The last step is to inherit the ISE super class and implement the encrypt_file() and decrypt_file() methods.
back

What encryption should I use in my algorithm?

Team ISE decided to use Rijndael AES encryption in the JPEG_ISE class because it does not increase the file size and the block cipher allows the randomization of number of bytes encrypted at the end of a section. Also, it came highly recommended by Professor Black of the University of Colorado at Boulder. However, if an encryption other than AES is well suited for your purpose, it can be used and will have no problems inheriting from the ISE Class.
back

Is there an example of a class inherited from the ISE Class?

Yes, Team ISE produced an inheriting class with the ISE production code. The JPEG_ISE Class is designed to implement selective encryption of standard baseline JPEG images. The class is freely available with the ISE super class.
back

Is there an example of how to use the JPEG_ISE Class?

Team ISE has included a main program using the functionality of the JPEG_ISE class. It was created to be an example of how the class could be used to selectively encrypt a JPEG image.
back

Where can I find more information about Team ISE and the ISE Production Code?

We have created a companion website that includes every research document we have created. This Website also contains links to many useful resources and even a bulletin board for discussions.
back

Back to top

ISE Website

How are the passwords obtained?
Where is the computer running the web page located?
What server is used?
What OS is the server running on?
What is the path to the directory with the web pages on the server?
Where are the images, documents, etc. located?
What is the IP address of the website?
Was an editor used to code the pages?
What version of HTML is used?
Are the pages written in valid HTML?
What character set are the pages coded in?
Do the pages make use of a CSS?
Do the pages follow a particular format?
What language was used to create the menu bar?
How can the menu bar be modified?
How is the menu bar included in the HTML pages?
Where was the message board obtained?
What is the message board coded in?
What type of database does the message board use?
Can the database be modified?
How can the database be copied?
How are the message board administrator options accessed?
How are new categories added?
How are categories deleted or edited?
How are new forums added?
How are forums edited?
How are forums deleted?
Can threads be automatically deleted?
Can the administrator manage the user accounts?
How are E-mail addresses banned?
How are E-mail addresses un-banned?
How are IP addresses banned?
How are IP addresses un-banned?
How are ranks set?
How are ranks deleted?

How are the passwords obtained?

Passwords are needed to log onto the computer the website is located on. Passwords are also needed to access the administrative options of the message board, and to log to the MySQL database used by the message board. These passwords were only provided to Dr. Tom Lookabaugh. In order to obtain these passwords, you must contact Dr. Lookabaugh.

back

Where is the computer running the web page located?

The web page is run off of a machine in Dr. Lookabaugh's Pervasive Computing Lab in the Discovery Learning Center at the University of Colorado at Boulder. To access this lab, you must obtain keys from Dr. Lookabaugh and the University of Colorado.

back

What server is used?

Apache/2.0.48 (Fedora) Server is used to serve this web page. This server comes with the Fedora Core Operating System, or can be downloaded from http://www.apache.org/. The particular version used to serve the web page was included in the Fedora Core release. The Apache server is configured to serve pages from a specific folder. The folder on the sponsor's computer is the "html" folder, which can be reached by following path from the root directory:

..\var\www\html

All pages that are to be served must be located in this folder.

back

What OS is the server running on?

The Operating System used by the server is the Red Hat Fedora Core Release. For more information on this operating system, please visit http://fedora.redhat.com/.

back

What is the path to the directory with the web pages on the server?

To reach the directory with the web pages, you must first log onto the computer where the server is located. You must log on as the root user. Obtain all passwords and usernames from Dr. Lookabaugh. Once logged on, the path to the directory with the pages is:

..\var\www\html

All of the pages are located in the "html" directory.

back

Where are the images, documents, etc. located?

The images, documents, and code accessible to the pages are located in subdirectories of the html directory. These subdirectories were created to organize all of the data used by the web pages.

All of the images are located in the "images" subdirectory. All images should be placed into this directory. Images can then be displayed on the web pages using the following HTML code:

> <img src="images/*ImageName*">

ImageName refers to the actual name of the image plus its extension.

All of the documents are located in the "documents" subdirectory. All documents should be placed into this directory. Documents can then be called using the following HTML code:

> *LinkName*

DocumentName refers to the actual name of the document plus its extension. *LinkName* refers to the name of the desired link. It is recommended that all documents be in PDF format due to its portability.

All of the code is located in the "code" subdirectory. All downloadable code should be placed into this directory. Links to download the code can be created using the following HTML code:

> *LinkName*

CodeName refers to the actual name of the code download plus its extension. *LinkName* refers to the name of the desired link.

All of the message board code is located in the "board" subdirectory.
The following path will lead to the menu bar code from the "html" directory:

> **images\menu**

The images and JavaScript files used to create the menu bar are located in this directory.
back↩

What is the IP address of the website?

The IP address of the website and the computer it is located on is 128.138.75.184. The website is served off of port 80.
back↩

Was an editor used to code the pages?

Quantum Plus 3.1 was used to edit the HTML code of the web pages. It is recommended that this editor be used to modify the HTML code. It is not necessary to use this editor. However, the code was formatted using the spacing of this editor, and will be formatted properly in this editor.

back✍

What version of HTML is used?

The web pages are coded in HTML 4.01 Transitional. This allows some backwards compatibility with old HTML features. All pages associated with the website define the version of HTML being used by including the following header:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
```

Any new pages added to this site should include this header and comply with HTML 4.01 Transitional standards.

back✍

Are the pages written in valid HTML?

The HTML used to code the pages is valid HTML 4.01 Transitional. The pages were validated using the HTML validator located at http://validator.w3.org. Any new pages should be validated using this validator. Additionally, any modifications made to the existing pages should be revalidated. To use the validator, visit the site located at the URL above and supply it with the address of the page that is to be validated. For example, if the download page is to be revalidated, type

http://128.138.75.184/DocumentIndex.html

into the address box on the validator website and click on the "Validate URI" button. The validator will return a report on any necessary fixes required to make the page valid.

back✍

What character set are the pages coded in?

The pages are coded in the ISO-8859-1 character encoding. All additional pages should include the following code within the header element to define the encoding:

```
<META http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
<META http-equiv="Content-Language" content="en-US">
```

These elements should be included inside of the <HEADER> element.

back✍

Do the pages make use of a CSS?

A cascading style sheet was not used to define the style of the web pages. The website was intended to be a very simple design that is only used to distribute code and documentation. Thus, no style sheet was defined, and the pages were constructed in a very simple manner.

back↩

Do the pages follow a particular format?

All of the pages have a header and footer. These should be included in any additional pages to ensure conformity to the rest of the website. The header and footer code can simply be cut and pasted into any additional pages. The HTML for the header is:

```
<TABLE bgcolor="#003300" align="center" width="100%">
 <tr>
    <td>
        <P>
            <FONT size="+1" color="#FFFFFF">
            <B>University of Colorado Computer Science Department</B><br>
            2003-2004<br>
            </FONT>
            <FONT size="+2" color="#FFFFFF">
            <B>ISE JPEG Selective Encryption Sponsor</B>
            </FONT>
        </P>
 </tr>
</TABLE>
<H1 align="center">
    <img src="images/ISE_icon_white.jpg" alt="Team ISE">
</H1>
```

This code should be included immediately after the <BODY> element.

The HTML for the footer is:

```
<P>
    <FONT size="2">
    This project was done by
    <a href="http://www.colorado.edu" target="_blank">University of Colorado</a>
    students under the supervision of the
    <a href="http://www.cs.colorado.edu" target="_blank">Computer Science Department</a>.
    </FONT>
</P>
<P>
    <FONT size="2">
    This Website is located on a sever at the University of Colorado at Boulder. Questions: Contact
    <a href="http://www.cs.colorado.edu/people/tom_lookabaugh.html" target="_blank">Tom
        Lookabaugh</a>
    or
    <a href="mailto:TeamISE@hotmail.com">TeamISE@hotmail.com</a>.
    </FONT>
</P>
```

```
<TABLE bgcolor="#003300" align="center" width="100%">
 <tr>
    <td>
        <P align="center">
            <FONT color="#FFFFFF">
                <B>Team Image Selective Encryption Sponsored by Tom Lookabaugh</B><br>
                <B>Department of Computer Science</B><br>
                <B>University of Colorado at Boulder</B><br>
                <B>Boulder, CO 80309-0430</B><br>
                <B>HTML 4.01 Transitional</B><br>
                <B>Copyright &copy 2003-2004</B>
            </FONT>
        </P>
 </tr>
</TABLE>
```

This code should be inserted immediately before the </BODY> element.
[back]

What language was used to create the menu bar?
The menu bar was created using the Xara Menu Maker tool. This tool generated the JavaScript used by the menu bar.
[back]

How can the menu bar be modified?
The JavaScript file is located using the following path from the "html" directory:

images\menu\isemenu.js

Xara Menu Maker is not required to modify this file. The file can be opened in an editor and modified to add additional menu or submenu items. There are two .js files in this directory. Only the isemenu.js file needs to be modified in order to add new menu items. The menu.js file should not be modified.
[back]

How is the menu bar included in the HTML pages?
The menu bar is included in the HTML pages using the following HTML code:

```
<SCRIPT src="images/menu/menu.js" type="text/JavaScript"></SCRIPT>
<SCRIPT src="images/menu/isemenu.js" type="text/JavaScript"></SCRIPT>
```

This code should be included immediately after the header.
[back]

Where was the message board obtained?

The message board was obtained from http://www.chipmunk-scripts.com/. This is a free software download that Team ISE made use of rather than creating their own message board.
back

What is the message board coded in?

The message board is coded in PHP with embedded MySQL queries. Because Team ISE did not develop this code, it should not be modified.
back

What type of database does the message board use?

The message board makes use of an underlying MySQL database. The installation script provided by the message board created all of the necessary tables utilized by the message board. This database software comes with the Red Hat Fedora Core release.
back

Can the database be modified?

The database can be modified by logging in as the root user and running the MySQL database. Refer to the password section to learn how to obtain the proper username and passwords. However, the database should not be modified to ensure the proper working of the message board. Additions to the message board can be made using the administrator options provided by the message board. This code will create the proper relations in the database needed for any changes. All modification to the database should be done indirectly through the administrator options.
back

How can the database be copied?

If the website is to be moved to another machine, the database tables must be copied from the MySQL server the database is currently in to the MySQL server on the new machine. If the new machine does not have a MySQL server, a server must be downloaded and installed by visiting the MySQL link. After the server is downloaded and installed, the database from the old server must be imported to the database on the new server. Refer to the MySQL online documentation for instructions on coping databases to another machine.
back

How are the message board administrator options accessed?

First, the administrator login name and password must be acquired. Refer to the section on passwords for information on how to obtain these items. Once these items are known, click on the "Login" link in the upper right corner of the message board page directly under the header. Provide the text boxes with the correct administrator username and password. The message board will then redirect you to the forum page. Centered at the bottom of the forum page is a link called "Admin CP". Clicking on this link will open a

window in which all of the administrator options can be accessed by clicking on the links. Click on one of the options under the "Admin Options" table to use the option.
back✍

How are new categories added?

After logging in as the administrator and clicking on the "Admin CP" link, click on the "Add category" link. Provide a name for the category and its rank. The category's rank determines the order in which the category is listed in relation to the other categories. The lowest number category is listed first. After entering this information click on the "submit" button. The message board now contains a new category.
back✍

How are categories deleted or edited?

After logging in as the administrator and clicking on the "Admin CP" link, click on the "Delete/Edit Category" link. All existing categories will now be listed in a table. The category name will be listed in the left column, a "Delete?" link in the middle column, and an "Edit?" link in the right column of the table. To delete a category, click on the "Delete?" link found in the middle column of the table. The board will ask you if you are sure you want to delete the category. Click on the "Main" link on the "Admin Options" table to cancel the delete. To edit the category, click on the "Edit?" link in the right column of the table. You will be redirected to the add category window. However, the category name and rank are already filled in. Make desired changes to the name and rank and click submit. The edited changes will now be applied.
back✍

How are new forums added?

After logging in as the administrator and clicking on the "Admin CP" link, click on the "Add Forum(s)" link. This will redirect you to the add forum window. Once in this window, you can create a forum by filling in a name in the "name of forum" text box. Next, choose which category to associate the forum with by clicking on the pull down menu. The menu will be populated with all of the categories on the message board. Select the category and then set the permission level to read, post, and reply in the forum you are creating. Selecting one of the permissions from the pull down menu for each read, post, and reply can set the respective permission level. In the last text box, type a definition of the forum. After all text boxes are filled and all permissions set, click on the "Create Forum" button to create a new forum with the information you inserted.
back✍

How are forums edited?

After logging in as the administrator and clicking on the "Admin CP" link, click on the "Edit Forums(s)" link. A table will be displayed listing all of the different forums for each category. Click on the "Edit" link next to the forum you desire to change. This will open the same window as when clicking on the "Add Forum(s)" link, except all of the information will be filled in. Change any desired information and click on the "submit" button to make the changes take effect.

How are forums deleted?

After logging in as the administrator and clicking on the "Admin CP" link, click on the "Delete Forums(s)" link. A table will be displayed with all of the forums available for the different categories. The name of each forum will be displayed in the left column of the table, and a "Delete this Forum" link can be found in the right column of the table. Click on the "Delete this Forum" link next to the forum you desire to delete. The board will ask you again if you want to delete the forum. Click on the "Delete this Forum" button again to delete the forum. Click on the "Main" link under the "Admin Options" table to cancel the deletion.

Can threads be automatically deleted?

Threads without responses can be automatically deleted after a certain number of days. To adjust the amount of days, first log on as the administrator, click on the "Admin CP" link and then click on the "Prune Topics" link. The administrator can then enter the amount of days before a thread is to be deleted. If the thread does not receive a response after the allotted time has passed, it will automatically be deleted.

Can the administrator manage the user accounts?

The administrator can manage user accounts. After logging in as the administrator and clicking on the "Admin CP" link, click on the "User Management" link. Type the user name into the text box and click on the "Search for User" button. If you want all of the users to be displayed, leave the text box empty and click on the "Search for User" button. After clicking the button, the username(s) will be displayed along with the user's email address. To edit a user's profile click on the "Edit" link next to the user's name. The administrator can then edit the user's profile by changing the information in the text box fields. Clicking on the "Edit User" button will make the changes permanent. The administrator can also delete a user by clicking on the "Delete" link next to the user's name. The message board will prompt the administrator again before making the deletion permanent. Clicking on the "Delete This User" button will complete the deletion. To cancel the deletion, click on the "Main" link under the "Admin Options" table.

How are E-mail addresses banned?

After logging in as the administrator and clicking on the "Admin CP" link, click on the "Ban E-mail" link. The administrator can then fill in the text box with the E-mail address that is to be banned. Click on the submit button to make the ban take effect. Any users with a banned E-mail address cannot register to use the message board. **Note:** If the text box is filled with a generic E-mail, such as "@hotmail.com" all users will an E-mail address ending with "@hotmail.com" will not be allowed to register on the message board.

How are E-mail addresses un-banned?

After logging in as the administrator and clicking on the "Admin CP" link, click on the "Unban E-mail" link. A list of banned E-mail addresses will be displayed. Click on the "Delete" button next to an E-mail address to un-ban that address. Users with that E-mail address will now be allowed to register to use the message board.

How are IP addresses banned?

After logging in as the administrator and clicking on the "Admin CP" link, click on the "Ban IP" link. The administrator can then fill in the text box with the IP address that is to be banned. Click on the submit button to make the ban take effect. Any users trying to register from a banned IP address will not be able to use the message board.

How are IP addresses un-banned?

After logging in as the administrator and clicking on the "Admin CP" link, click on the "Unban IP" link. A list of banned IP addresses will be displayed. Click on the "Delete" button next to an IP address to un-ban that address. Users working from that IP address will now be allowed to register to and use the message board.

How are ranks set?

After logging in as the administrator and clicking on the "Admin CP" link, click on the "Add Rank" link. The number of posts the user has made determines the rank of a user. To create a rank, the administrator creates a rank title by filling in the "Rank" text box with the title name. The administrator then fills in the "Number of Posts Needed to Achieve" text box with a number. Clicking the "submit" button will create this rank. A user will automatically be assigned the rank once he or she has submitted enough posts.

How are ranks deleted?

After logging in as the administrator and clicking on the "Admin CP" link, click on the "Delete Rank" link. A list of ranks will then be displayed along with the number of posts needed to achieve such a rank. Clicking on the "Delete" link next to the rank will allow the administrator to delete the rank. The message board will then prompt the administrator again about deleting the rank. Clicking on the "Delete Rank" button will delete the rank. To cancel the deletion, click on the "Main" button under the "Admin Options" table.

Back to top↩