Implementation of a Prototype for Secure Online Payment System Using Discrete Cosine Transformation and Permutative Straddling

GRADUATE PROJECT REPORT

Submitted to the Faculty of
The School of Engineering & Computing Sciences
Texas A&M University-Corpus Christi
Corpus Christi, TX

in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Computer Science

by

Ranjith Kumar Bodla
Fall 2014

Committee Members

Dr. Mario Garcia
Committee Chairperson

Dr. David Thomas
Committee Member
ABSTRACT

E-commerce is the current trending topic in the online shopping market. With ever increasing popularity, the payment methods used are more prone to fraudulent attacks with misuse of credit/debit cards or personal information. Such attacks are more in the case of CNP (card not present) type of transactions based on recent report from FICO Analytic Software Company which looks after FICO score, a measure of consumer credit risk. This project presents an approach with less information needed from consumer standpoint for online e-commerce transactions. This approach uses discrete cosine transformation (DCT) and permutative straddling method with its high capacity and more efficiency in embedding data.
# TABLE OF CONTENTS

Abstract .................................................................................................................................................................. ii

Table of Contents .............................................................................................................................................. iii

List of Figures ................................................................................................................................................... vi

List of Tables .................................................................................................................................................... viii

1. Background and Rationale .......................................................................................................................... 1

   1.1 Hiding Data ............................................................................................................................................... 2

   1.2 Steganography ......................................................................................................................................... 2

   1.3 Visual Cryptography .............................................................................................................................. 4

   1.4 Cryptography vs. Steganography .......................................................................................................... 4

   1.5 F5 Steganographic Algorithm .............................................................................................................. 4

   1.6 Type of Attacks on steganogram ........................................................................................................... 6

      1.6.1 Visual Attacks .................................................................................................................................. 7

      1.6.2 Statistical Attacks ............................................................................................................................ 7

2. Previous Research, Motivation .................................................................................................................... 8

   2.1 Previous Research .................................................................................................................................. 8

   2.2 Motivation .............................................................................................................................................. 10

   2.3 My Contribution .................................................................................................................................... 12

3. Architecture .................................................................................................................................................. 13

   3.1 JPEG File Exchange Format ................................................................................................................. 14

      3.1.1 Discrete Cosine Transformation ...................................................................................................... 14

      3.1.2 Quantization ................................................................................................................................... 15

      3.1.3 Huffman Coding .............................................................................................................................. 15
3.1.4 Huffman Decoding.................................................................16
3.2 Permutative Straddling..............................................................17
3.3 Matrix Encoding.................................................................17
3.4 Flow of Execution..............................................................18
3.5 Step-by-step process of project development .........................21

4. Functionality of the Application...............................................22
4.1 Applications........................................................................22
  4.1.1 E-commerce Application.............................................22
  4.1.2 Central Authority Application .......................................22
4.2 E-commerce User ............................................................23
  4.2.1 Login..........................................................................23
  4.2.2 Home Page............................................................24
  4.2.3 Available Products.....................................................25
  4.2.4 Add items to cart.......................................................25
  4.2.5 View Items in the cart...............................................26
  4.2.6 Payment screen.......................................................27
  4.2.7 Order Confirmation...................................................27
  4.2.8 XML file generation at E-commerce Site .......................28
  4.2.9 Encoding xml file data into input image .......................29
4.3 Merchant Login....................................................................31
  4.3.1 Merchant Home Page...............................................31
  4.3.2 Merchant Product View.............................................31
  4.3.3 Add New Item........................................................32
4.3.4 Product Update.................................................................33
4.3.5 Delete a Product.................................................................33
4.4 Central Authority.................................................................34
4.3.1 Login.................................................................................34
4.3.2 User Credit Card Details.....................................................35
5. Testing and Evaluation ..........................................................37
5.1 Test Cases.............................................................................38
6. Conclusion and Future Work..................................................47
Bibliography and References......................................................48
LIST OF FIGURES

Figure 1.1 Example of Steganography .................................................................3
Figure 1.2 F5 Encoding Process ...........................................................................5
Figure 1.3 F5 Steganography Example ...............................................................6
Figure 2.1 Transaction in Online Shopping .......................................................9
Figure 2.2 Example of Rise in Users on E-commerce Accounts in 2009-2013 ....11
Figure 2.3 Data Provided by IC3 for Internet Related Frauds from 2000-2013 ...12
Figure 3.1 Proposed System Architecture .........................................................13
Figure 3.2 Flow of Information in JPEG Compressor ........................................14
Figure 3.3 Example of Discrete Cosine Transformation Coefficients for a Higher Frequency Region .................................................................16
Figure 3.4 Permutative Straddling Scatters the Changes (x) ............................17
Figure 3.5 Flow Chart Diagram for the Proposed System .................................19
Figure 3.6 Input Output Flow of Proposed System ...........................................20
Figure 3.7 F5 Steganography on the Input Image ..............................................20
Figure 3.8 Huffman Decoding of image at CA Site .........................................21
Figure 4.1 Login Page of the E-commerce Application .....................................24
Figure 4.2 User Home Page in the E-commerce Application after Logging In ....24
Figure 4.3 Available Products in the Category of Notebooks ............................25
Figure 4.4 Adding Items to Cart .................................................................26
Figure 4.5 Items in the User Cart .................................................................26
Figure 4.6 Payment Screen .................................................................27
Figure 4.7 Order Confirmation .................................................................28
Figure 4.8 XML File with Input Payment Details .......................................................28
Figure 4.9 Input Image to be Encoded .................................................................29
Figure 4.10 Encoded Image with Payment Information ........................................30
Figure 4.11 XML File Generated at CA Application .............................................30
Figure 4.12 Merchant Home Page on E-commerce Site ......................................31
Figure 4.13 View of the Existing Products in Electronics Category ....................32
Figure 4.14 Adding a New Item in the Selected Category .....................................32
Figure 4.15 Updating Existing Items .................................................................33
Figure 4.16 Delete a Product ..............................................................................34
Figure 4.17 Central Authority Application Login Page ......................................35
Figure 4.18 Credit Card Details of the Users ......................................................35
Figure 5.1 Login Validation ..............................................................................39
Figure 5.2 Username and Password Validation at Shopping Site ......................40
Figure 5.3 Input Credit Card Information ..........................................................41
Figure 5.4 XML File Generation ......................................................................41
Figure 5.5 Validating at Central Authority user username and password ..........42
Figure 5.6 Embedded Image Size after Compression ........................................43
Figure 5.7 Contents of XML File at Shopping Site .............................................44
Figure 5.8 Contents of XML File at Central Authority Site ...............................44
Figure 5.9 Embedding Efficiency of the jpg Image with Payment Details ........45
Figure 5.10 Encoding Content in Image of Less Size .......................................46
LIST OF TABLES

Table 4.1 Dimensions and Size of Input and Output Image..............................................36
1. BACKGROUND AND RATIONALE

Online shopping in E-commerce is the purchase of products via internet. An electronic purchase order request is issued, by entering and validating credit or debit card information. The product is shipped through mail or by courier. Common dangers in this process can be identity theft, merchant collusion and phishing attacks. Identity theft is the process of stealing someone’s personal information and making use of it illegitimately. Merchant collusion is the process of stealing the consumer information by the employees of the merchant organization or E-commerce web sites.

The objective of this project is to implement a prototype for secured online payment system using Discrete Cosine Transformation (DCT) and Permutative Straddling. This makes use of F5 steganography which consists of DCT and Permutative Straddling. With such a system it has the capability to overcome a recent fraud which happened with a user on Xoom.com – money transferring website on April 24 2014 in St. Louis, Missouri, where his card details were hacked by the intruder from the payment screen and misused for personal benefits. Nomorerack is other example of online data breach in shopping site between Nov 1 2013, and Jan 15, 2014 where they were forced to go with forensics audit after receiving complaints from banks, which resulted in not meeting Payment Card Industry (PCI) standards where user details was stored in the database.

Importance of the project

The major advantages of this project are:

- With F5, this system achieves a high embedding capacity of data in the image with the help of Huffman Encoding.
• As there is less customer information sent to the merchant, there is no chance of merchant related frauds or merchant collusion.

• With Certified Authority, customer satisfaction is improved and more number of parties can be involved in the process.

• CA can send cover text to bank through mail, which cannot be cracked though intruder tracks because of the private key encryption.

• A security breach in a single database can easily be contended since customer data is distributed over 3 parties.

• Resistant to both Visual and Statistical Attacks.

1.1 Hiding Data

Data to any organization is highly important. They must be protected and secured from intrusion. Data should be visible only to the sender and receiver of transmitted data. Hiding data is nothing more than protecting the data in some medium or encrypting the data. There are many techniques that use the concept of hiding data; cryptography and steganography are among them.

1.2 Steganography

Steganography is the process of hiding a secret message to be transmitted in a cover media which can be text, image, video, audio etc. In text steganography, message is hidden by shifting the characters in a word, converting it into ASCII values and formatting it to a new sentence etc. Among all the steganography, text steganography requires considerably smaller memory and simpler communication [4].
Figure 1.1 shows an example of steganography with the image of a mansion as the cover media where the actual secret image is stored.

![Figure 1.1 Example of Steganography](image)

**Uses of steganography**

There are many uses of steganography when used to hide confidential information in a cover media like image, video, and text file. A few of the uses are:

1. Used to combine explanatory information with an image (like doctor's notes accompanying an X-ray).
2. Embedding corrective audio or image data in case corrosion occurs from a poor connection or transmission.
3. Peer-to-peer private communications.
4. Posting secret communications on the web to avoid transmission.
5. Maintaining anonymity.
6. Hiding data on the network in case of a breach.
1.3 Visual Cryptography

Visual cryptography is the art of hiding or a cryptographic technique relying on visual mode of sharing by use of image encryption. With the concept of image encryption, considering k image shares out of n image shares (k, n) visual secret scheme, the secret image is divided into meaningless images that are transmitted over an untrusted communication channel [4]. A combination of all the k shares of images can give the original secret image.

1.4 Cryptography vs. Steganography

Steganography and cryptography are closely related, with the main difference being their goals. Cryptography encrypts the data, which makes it unreadable, but the encrypted data cannot be hidden from unauthorized users as the presence of hidden data is known. In contrast, steganography prohibits unauthorized users from even having any knowledge of the existence of the hidden data.

1.5 F5 Steganographic Algorithm

The F5 steganographic algorithm was introduced by German researchers Pfitzmann and Westfield in 2001. Main purpose of their work was to propose a secured approach to develop concepts and a practical embedding method for only JPEG images (because it uses JPEG Compressor) that would provide high steganographic capacity without sacrificing security. Influenced by this attack, they challenged the paradigm of replacing bits of information in the cover-image with the secret message while proposing a different paradigm of incrementing image components to embed message bits. F5 steganographic algorithm consists of DCT and Permutative Straddling. They decreased
the absolute value of the coefficient by one, instead of replacing the LSBs of quantized DCT coefficients with the message bits.

This type of embedding cannot be detected using $\chi^2$ statistical attack. Chi-squared statistic is measured with the $\chi^2$ (chi-square) attack which is a fit between two discrete distributions. This attack can be automated using statistical techniques. As the embedded data is pseudorandom and the natural image data is not, a test for randomness should let us differentiate between a natural image and one with pseudorandom data embedded in it. Figure 1.2 shows the stages involved in F5 Encoding process [14].

![Figure 1.2 F5 Encoding Process [14]](image)

Figure 1.3 shows a sample of F5 Steganography. The input to the F5 Encrypt/Decrypt program is a carrier image (JPEG or BMP) and secret message which is to be encrypted in the carrier image. The output is an encrypted image (resultant steganogram) which looks similar to carrier image [14].
1.6 Type of Attacks on steganogram

Attacking steganographic algorithms is very similar to attacking cryptographic algorithms. Some possible attacks are:

File only - The attacker has access to the file and must determine if there is a message hidden inside.

File and original Copy - If the attacker have a copy of the file with the encoded message and a copy of the original, pre-encoded file, then detecting the presence of some hidden message is a trivial operation. The real question is what the attacker may try to do with the data (destroy hidden information, extract the information, replace) [22].
1.6.1 Visual Attacks

Some attacks strip away the significant parts of the image in a way that facilitates a human trying to search for visual anomalies. One common test displays the least significant bits of an image. Completely random noise often reveals the existence of a hidden message because imperfect digitalizers leave echoes of the large structure in the least significant bits [22].

The disadvantage of visual attack is that they sometimes won’t work if there are no objects on the picture with clear shapes – it causes random noise on the least significant bits of the original image. Next disadvantage is that it is hard to automatize the visual attacks.

1.6.2 Statistical Attacks

Much of the study of mathematical statistics is devoted to determining whether some phenomenon occurs at random. The simplest statistical test for detecting randomness is the $\chi^2$ (chi-squared) test. This test is based on differences between expected number of some event occurrences and number of its real occurrences [22].
2. PREVIOUS RESEARCH, MOTIVATION

2.1 Previous Research

The first noted use of steganography was estimated to be done in 440 BC when Herodotus writes two examples in his Histories. Demaratus sent a warning about a forthcoming attack to Greece by writing it directly on the wooden backing of a wax tablet before applying its beeswax surface. Wax tablets were in common use then as reusable writing surfaces, sometimes used for shorthand.


**Traditional Payment Method**

The consumer selects items from online shopping portal and then is directed to the payment page in a traditional online shopping as shown in Figure 2.1. Online merchant may have its own payment system or can make use of third party payment gateway systems such as PayPal, Wepay, payonlinesystem, WebMoney and others. In the payment portal consumer submit his or her credit or debit card details such as credit or debit card number, name on the card, expiry date of the card [4].

![Figure 2.1 Transaction in Online Shopping][4]
2.2 Motivation

There has been increase in number of e-commerce web applications, with which there is rise in consumers using these applications day by day. The consumer makes use of these applications to order items of their basic needs which will be delivered to their home. With such an increase of users registering on web applications there is also an increase in intruders trying to steal consumer information. There must be a secured approach by which user information can be securely transferred over the network from the e-commerce application to the bank or to the payment gateway. This can be achieved by hiding the information in a cover media.

Figure 2.2 [23] shows the number of users registering on a few e-commerce applications like amazon, apple, and on payment gateway company like PayPal. By referring to the trend, the number of users on amazon has highly increased in 4years with more rises in users in craigslist. EBay shows a gradual decrease in users because of other competitors.
Figure 2.2 Example of Rise in E-commerce Accounts in 2009-2013 [23].

Figure 2.3 [13] shows internet crime report provided by internet crime complaint center (IC3). In 2013, the IC3 received 262,813 consumer complaints with an adjusted dollar loss of $781,841,611, which is a 48.8 percent increase in reported losses since 2012($581,441,110).
Figure 2.3 Data Provided by IC3 for Internet Related Frauds from 2000-2013 [13].

2.3 My Contribution

My contribution towards the project includes implementing a combination of main idea from 2 papers – “F5 – a steganographic algorithm: High capacity despite better steganalysis”, “Online Payment System using Steganography and Visual Cryptography”. It includes implementing F5 steganography techniques [1] with the payment system where it uses CA [4]. Such a combinational approach is a new implementation with both the techniques hasn’t been proposed as a prototype in a single paper, or there is no source of evidence which showcases them together.
3. ARCHITECTURE

Figure 3.1 shows the proposed system architecture. First, user starts web browser on his system and opens the E-commerce application web site. User then logs in into the site with username and password given at the time of registering on the web site. Then he chooses items of his choice available on the site and adds them to the cart. At the time of check out user is prompted to enter his credit card details, billing information. Now, F5 steganography is applied on the credit card details and results in an encoded image. It is then sent to the Certified Central Authority (CA), where information is extracted from the image.
The project extends the payment process with its security feature by F5 steganography using following components of it.

3.1 JPEG File Interchange Format

JPEG saves image data in compressed form as a quantized frequency coefficient [1]. Uncompressed bitmap image is cut into parts of 8 by 8 pixels by the JPEG compressor. 8 × 8 brightness values are transformed into 8 × 8 frequency coefficients by the discrete cosine transformation (DCT) as shown in Figure 3.2. Then the frequency coefficients are rounded off to integers in the range −2048 . . . 2047 by quantization [1]. The output of the JPEG compression is a JPEG image with reduced image quality and decrease in size. Input to the DCT is a JPEG image into which the secret message has to be encoded

![Figure 3.2 Flow of Information in JPEG Compressor](image)

3.1.1 Discrete Cosine Transformation

A discrete cosine transform (DCT) expresses a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies. DCT is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using only real numbers. DCT algorithms are capable of achieving a high compressing degree with
minimal loss of data. This algorithm is effective for compressing continuous-tone images in which the differences between adjacent pixels are usually small.

DCT converts spatial image representation into a frequency map. The low-order (DC) term represents the average value in the block. Higher order (AC) terms represent the strength of more and more rapid changes across the width or height of the block. After performing DCT on 8x8 pixels of image blocks we separate high and low frequency information present in the image. Then without losing low-frequency information, we can discard high-frequency data [10].

3.1.2 Quantization

The compressor divides each DCT output value by a “quantization coefficient” and rounds the result to an integer. This is done to discard an appropriate amount of information. With high quantization coefficient more data is lost because actual DCT value is represented less and less accurately. Here, higher order terms are quantized more heavily than low-order terms [10].

3.1.3 Huffman coding

Huffman coding is a method that takes symbols (e.g. bytes, DCT coefficients, etc.) and encodes them with variable length codes that are assigned according to statistical probabilities. A frequently-used symbol will be encoded with a code that takes up only a couple bits, while symbols that are rarely used are represented by symbols that take more bits to encode. There is a significant amount of redundant data in the resulting coefficients after quantization. Huffman coding removes this redundant data resulting in smaller JPEG data [10]. Figure 3.3 shows a sample 8x8 matrix DCT coefficient values
for a higher frequency image block of the image of an eye (eye ball) with 8x8 pixels shown in 2\textsuperscript{nd} picture [10].

![Image of eye with 8x8 pixel block highlighted]

<table>
<thead>
<tr>
<th>350.5</th>
<th>251.0</th>
<th>109.0</th>
<th>0.8</th>
<th>-17.7</th>
<th>-26.1</th>
<th>-6.7</th>
<th>-3.7</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0</td>
<td>-47.2</td>
<td>-43.6</td>
<td>-11.3</td>
<td>4.5</td>
<td>15.1</td>
<td>5.1</td>
<td>5.1</td>
</tr>
<tr>
<td>30.8</td>
<td>-58.4</td>
<td>-52.0</td>
<td>-26.3</td>
<td>25.0</td>
<td>14.2</td>
<td>6.4</td>
<td>-1.7</td>
</tr>
<tr>
<td>35.7</td>
<td>14.0</td>
<td>17.1</td>
<td>12.4</td>
<td>0.3</td>
<td>-6.1</td>
<td>-3.0</td>
<td>1.4</td>
</tr>
<tr>
<td>26.0</td>
<td>-19.7</td>
<td>-3.5</td>
<td>10.7</td>
<td>13.7</td>
<td>-3.1</td>
<td>-5.1</td>
<td>-1.1</td>
</tr>
<tr>
<td>20.0</td>
<td>18.6</td>
<td>20.0</td>
<td>7.5</td>
<td>-5.7</td>
<td>-6.5</td>
<td>-2.5</td>
<td>-3.1</td>
</tr>
<tr>
<td>-6.0</td>
<td>-23.6</td>
<td>-12.4</td>
<td>2.4</td>
<td>1.6</td>
<td>0.5</td>
<td>1.7</td>
<td>2.2</td>
</tr>
<tr>
<td>-3.0</td>
<td>-1.8</td>
<td>0.3</td>
<td>0.0</td>
<td>1.3</td>
<td>1.2</td>
<td>1.9</td>
<td>1.2</td>
</tr>
</tbody>
</table>

**Figure 3.3 Example of Discrete Cosine Transformation Coefficients for a Higher Frequency Region [10]**

### 3.1.4 Huffman Decoding

The approach used to decode and extract the data hidden in the image using Huffman encoding is achieved using Huffman decoding technique. The data structure used in Huffman decoding is Huffman tree. In general, the Huffman tables used at the encoding are the same as that used at decoding. The process of decoding is simply a matter of translating the stream of prefix codes to individual byte values, usually by traversing the Huffman tree node by node as each bit is read from the input stream.
3.2 Permutative Straddling

Permutative Straddling is used to uniformly spread out the changes made by matrix encoding to embed the message over the whole steganogram. Only a few of the major steganographic algorithms scatter message over carrier medium which have poor time-complexity. If we lessen the steganographic capacity, they tend to get slow. If the capacity of the carrier medium is known exactly, straddling is easy. All the coefficients are shuffled using permutation first and then embed them into the permuted sequence (result of the permutation straddling shown in Figure 3.4) [1]. This permutation is created based upon the key generated from the user credit card. Then the steganographically changed coefficients are delivered in its original sequence to the Huffman coder. The receiver is able to repeat the permutation only with the correct key. The permutation has linear time complexity $O(n)$ [1].

![Figure 3.4 Permutative Straddling Scatters the Changes (x) [1]](image)

3.3 Matrix Encoding

Matrix Encoding technique was introduced by Ron Crandall to improve embedding efficiency and F5 is possibly the first implementation of this technique. It
decreases the necessary number of changes if most of the capacity is unused in a steganogram. Considering the uniformly distributed secret message and uniformly distributed values at the positions to be changed without matrix encoding we have an embedding efficiency of 2 bits per change. If we embed a very short message comprising only 1736 bits, F5 embeds the same message using matrix encoding with only 459 changes with an embedding efficiency of 3.8 bits per change [1].

3.4 Flow of Execution

Figure 3.5 shows the flow of execution of online payment system using Discrete Cosine Transformation and Permutative Straddling. The entire decision making situation that is involved in the project is also shown.
Figure 3.5 Flow Chart Diagram for the Proposed System

Figure 3.6 shows the input output flow of the proposed system with the output file names written. The flow starts after user submits his payment details on the E-commerce application.
Figure 3.6 Input Output Flow of Proposed System

Figure 3.7 shows the flow of F5 steganography, once the XML file is generated from the payment information given at the shopping site.

Figure 3.7 F5 Steganography on the Input Image

Figure 3.8 shows the process of decoding image contents with huffman decoder and parsing the result into XML file.
3.5 Step-by-step process of project development

The following describes a brief overview of the step by step process of proposed system:

1. Understanding the mechanism of existing Steganography techniques that are incorporated in securing consumer information in online transactions on E-commerce applications.

2. Developing designs of web based steganography featured payment system to successfully transfer consumer information over the network from application to CA.

3. The proposed web application is built on MVC architecture and is developed on Java2 Enterprise edition technology, in which the data is collected from the user and processed through servlets and JSPs.

4. MySql enterprise data software is used in this application for building the data tables, which is hosted on WAMP server. These data tables are used to store user authentication details.

5. Encoding and decoding techniques are created based on the F5 steganography technique.

6. Deployment and execution are done on the local host using Wamp Server.
4. FUNCTIONALITY OF THE APPLICATION

Overall functionality of application for this system is divided into number of features that are implemented. Modular approach for development process is observed and implementation of each feature is considered as an application. There are 2 different applications - E-commerce application for user login, product selection, payment information, Central Authority application for user information validation, communication with bank and merchant.

4.1 Applications

4.1.1 E-commerce Application

E-commerce application is the portal which makes varied products available to the consumers. Merchant logs in with their profile and make the products available for the consumer to consume. Consumers select the items of his/her choice available from different merchants on the application and proceed to the payment. Consumer information provided at the time of payment screen is encoded using F5 steganography by this application.

4.1.2 Central Authority Application

A certificate authority or central certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. A CA is a trusted third party - trusted both by the subject (owner) of the certificate and by the party relying upon the certificate.
In the proposed system Central Authority gets the private key encoded file submitted at the payment screen from the E-commerce Application and input the private key of the particular merchant to extract the encoded file. Then it decodes the information in the image using Huffman Decoding. Then the application looks with the payment gateway of the issuing bank to check the authenticity of the consumer which he notifies to the merchant (out of scope of the project). By this, the merchant is notified only with the confirmation receipt of the consumer’s authenticity and not complete details of consumer credit/debit card information like credit card number, expiry, and name on credit card.

**User Interface**

The proposed system is visually shown in the form of a web site which is designed using JavaScript.

**4.2 E-commerce User**

E-commerce User is a user whoever uses the shopping application.

**4.2.1 Login**

In the Login page (as shown in Figure 4.1), the user can find a button by name login. Here the user enters his valid authentication details - username and password. If the details given by the user are valid (this is verified using authentication process), then the user will be taken to his account and can be able to access various features of the system. Else an error message is popped by asking the user to enter valid username or password. This is the common page for both the merchant and user. Depending on the access type of the user they are redirected to respective pages.
4.2.2 Home Page

The user is directed to his account, where he can see all the products made available by the different merchants as shown in Figure 4.2.

Figure 4.1 Login Page of the E-commerce Application

Figure 4.2 User Home Page in the E-commerce Application after Logging In
4.2.3 Available Products

From the available products (as shown in Figure 4.3) user enters the required quantity of his choice of product.

![Figure 4.3 Available Products in the Category of Notebooks](image)

4.2.4 Add items to cart

User once inputs the required quantity he adds it to the cart as shown in Figure 4.4.
4.2.5 View Items in the cart

Once the user is done with selecting the items, he checks out and finds the list of items added to the cart and total price (as shown in Figure 4.5).

Figure 4.4 Adding Items to Cart

Figure 4.5 Items in the User Cart
4.2.6 Payment screen

After review of the products, user moves to the payment screen where he/she is prompted with payment and billing details (as shown in Figure 4.6).

![Payment Screen](image)

Figure 4.6 Payment Screen

4.2.7 Order Confirmation

Confirmation of the order is displayed on the web browser after performing the proposed system process resulting in order confirmation (as shown in Figure 4.7).
4.2.8 XML file generation at E-commerce Site

XML file is generated after user inputs his payment details on the website. Merchant details are also sent within the same file as shown in Figure 4.8.
4.2.9 Encoding xml file data into input image

XML file details are encoded into an input jpg image as shown in Figure 4.9 which results in an encoded output jpg image after performing F5 steganography as shown in Figure 4.10. The input image has a size of 294 with dimensions 2048 x 1496 and output image has a size of 224 kb with 80 quality factor with same dimensions.

![Figure 4.9 Input Image to be Encoded](image-url)
4.2.10 Generating XML file at CA after decoding

Figure 4.11 shows XML file generated at CA site after performing huffman decoding on the input image received from E-commerce application.
4.3 Merchant Login

Merchant logs in to the E-commerce application where he can perform various activities like adding a product, editing and updating a product, deleting a product, viewing all the existing products.

4.3.1 Merchant Home Page

Figure 4.12 shows the home page of the merchant after he logs in to the web site. He/she is prompted with various activities to perform on a product.

![Figure 4.12 Merchant Home Page on E-commerce Site](image)

4.3.2 Merchant Product View

Figure 4.13 shows the list of all items and details of the products made available on the site by the merchant. The figure shows available items in the category of Electronics.
Figure 4.13 View of the Existing Products in the Electronics

4.3.3 Add New Item

Figure 4.14 shows the web page to add a new item to the E-commerce site in the selected category. Merchant is prompted to enter products details like name, store, description and price.

Figure 4.14 Adding a New Item in the Selected Category
4.3.4 Product Update

Merchant can edit and update the details of the items previously added to the site (as shown in Figure 4.15).

![Image of Product Update Interface]

Figure 4.15 Updating Existing Items

4.3.5 Delete a Product

Merchant can delete a product from the existing products on the site which will no longer be available on the E-commerce site for the user (as shown in Figure 4.16).
Central Authority

Figure 4.16 Delete a Product

4.4 Central Authority

Central Authority user can login to the website and view the account details submitted by the user on the shopping site.

4.4.1 Login

Central Authority can login to the application with his/her login details which are provided at the time of registering on the application (as shown in Figure 4.17).
4.4.2 User Credit Card Details

Central Authority has been made available with the credit card details of the authentic users (as shown in Figure 4.18).

![Central Authority Application Login Page](image1)

![Credit Card Details of the Users](image2)
Table 4.1 shows the resultant size of the image produced after performing F5 steganography on the input image with their dimensions. XML containing payment information which is to be encoded having size of 489 bytes has been used for all these cases.

<table>
<thead>
<tr>
<th>Dimensions of the Image (Input &amp; Output)</th>
<th>Size of Input Image (in KB)</th>
<th>Size of Output Image (in KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2048 x 1496</td>
<td>294</td>
<td>224</td>
</tr>
<tr>
<td>768 x 768</td>
<td>160</td>
<td>34.2</td>
</tr>
<tr>
<td>880 x 660</td>
<td>393</td>
<td>49.0</td>
</tr>
<tr>
<td>256 x 188</td>
<td>5.8</td>
<td>4.0</td>
</tr>
<tr>
<td>441x567</td>
<td>34.7</td>
<td>19.9</td>
</tr>
</tbody>
</table>

**Table 4.1 Dimensions and Size of Input and Output Image**
5. TESTING AND EVALUATION

Testing is the process used to check the errors in the program. It is considered as the major quality measure which is employed in software development. During testing, the program is executed with a set of test cases and the output of the program for the test cases is evaluated to determine if the program is performing as it is expected to perform. Testing is vital to the success of the system. System testing makes a logical assumption that if all parts of the system are correct, the goal will be achieved successfully. In the testing process we test the actual system in an organization and gather errors from the new system by taking the initiative to correct them. System testing is the stage of implementation, which is aimed to ensure that the system works accurately and efficiently. The front-end and back-end connectivity are tested to be sure that the new system operates in full efficiency.

The process of testing considered as a significant one as it uncovers errors from system. For achieving this process proper input data is given to the system. So the user should have more awareness to give input data. It is important to give correct inputs for efficient testing. Inadequate or non-testing lead to errors that may appear few months later. The following problems can generate inadequate testing scenarios.

- Time delay arises between the cause and appearance of the problem.

- The effect of the system errors can be observed on the files and records within the system.
The testing process focuses on logical intervals of the software ensuring that all the statements have been tested on the function intervals, where tests are conducted to uncover errors and ensure that the defined inputs will produce actual results that agree with the required results. Testing has to be done using the two common steps Unit testing and Integration testing.

*Unit testing*

Unit testing is also referred to as module testing. In unit testing, all the individual units of the project are tested so as to verify the functionality of each unit to see if it provides the output as expected or not. Each module of the application is tested separately to test for the expected output.

*Integration Testing*

Testing each module individually will not be sufficient in some cases, where the functionality of one unit causes hindrance to the functionality of other module. Therefore, testing is performed after making all the modules of the application work after integrating them together.

**5.1 Test Cases**

Testing in the proposed system is done by making the procedure level testing first. This is done by giving improper inputs; the errors occurred are noted and eliminated. This is the final step in system life cycle. It implements tested error-free system into real-life environment and make necessary changes, which runs in an online fashion. Following are the test cases used to test the working of the proposed project.
Test case 1: Verifying user Password

The user will be given username and password to login to the E-commerce application site. If the user tries to login to the site with incorrect or no password provided, then the system shows an error message and he is not able to login to the site (as shown in Figure 5.1).

![Figure 5.1 Login Validation](image-url)
Test Case 2: Username & Password Validation at Shopping site

Figure 5.2 shows the screen where user cannot login into the application when he tries to login using invalid Username and Password. User must provide the login details which he have created while registering into the application.

Figure 5.2 Username and Password Validation at Shopping site
Test Case 3: Testing for payment screen credit card details

Figure 5.3 shows on input field validation at payment screen. User cannot place the order with giving his card details like name on card. Payment information has several validations - few of them are all fields are mandatory, card number must be only number with 16 digits, zip code must be only number.

![Payment Information Form](image)

**Figure 5.3 Input Credit Card Information**

Test Case 4: XML file generation from payment details

After user inputs the payment details on the payment screen on E-commerce application. The data is parsed from at E-commerce server and generates xml with the consumer card details and merchant account details (as shown in Figure 5.4).
Figure 5.4 XML File Generation

Test Case 5: Username and Password validation at Central Authority site

Figure 5.5 shows all fields are mandatory while a user to login onto the central authority site thus preventing illegitimate users to login onto the site.

Figure 5.5: Validating Central Authority User Username and Password
Test case 6: Size of Encoded Image

Figure 5.6 shows the files that are being created with dynamic change in content once user submits credit card details at payment screen. The xml file content are embedded into the input image secure.jpg which results in embedded and compressed image secure1.jpg. The resulting image is observed to be decrease in size.

![Figure 5.6 Embedded Image Size after Compression](image)

Test Case 7: Matching xml file contents at shopping site and Central Authority site

The xml file generated at shopping site after user submits the payment details at shopping site must be the same with the xml contents at Central Authority site which is extracted
from the embedded image as shown in Figure 5.7 and Figure 5.8.

**Figure 5.7 Contents of XML File at Shopping Site**

```xml
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<CustomerInfo>
  <Credit_Card_Details>
    <Card_num>984032498890899</Card_num>
    <Card_Type>Discover</Card_Type>
    <Name_on_Card>ranjith boda</Name_on_Card>
    <Month>1</Month>
    <Year>2015</Year>
    <Merchant_Accountnno>24589634586</Merchant_Accountnno>
    <Merchant_Bank>StateBankofCalifornia</Merchant_Bank>
    <Merchant_ID>Shop_4567</Merchant_ID>
    <Merchant_Name>Shopping Hunk</Merchant_Name>
    <Total_payment>300</Total_payment>
  </Credit_Card_Details>
</CustomerInfo>
```

**Figure 5.8 Contents of XML File at Central Authority Site**

```xml
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<CustomerInfo>
  <Credit_Card_Details>
    <Card_num>984032498890899</Card_num>
    <Card_Type>Discover</Card_Type>
    <Name_on_Card>ranjith boda</Name_on_Card>
    <Month>1</Month>
    <Year>2015</Year>
    <Merchant_Accountnno>24589634586</Merchant_Accountnno>
    <Merchant_Bank>StateBankofCalifornia</Merchant_Bank>
    <Merchant_ID>Shop_4567</Merchant_ID>
    <Merchant_Name>Shopping Hunk</Merchant_Name>
    <Total_payment>300</Total_payment>
  </Credit_Card_Details>
</CustomerInfo>
```
Test Case 8: Embedding Efficiency

Entropy encoding is used to encode the contents of the xml file into the jpg image. Figure 5.9 shows the embedding efficiency with 2.5 bits needed per one change.

Figure 5.9 Embedding Efficiency of the jpg Image with Payment Details

Test Case 9: Testing Encoding of image with less size

F5 steganography works with image of less size and low resolution. Figure 5.10 shows encoded image secure1.jpg generated with 4.0 KB after performing F5 steganography on the input image secure.jpg with same xml size of 489 bytes used for high resolution image of more size.
Figure 5.10 Encoding Content in Image of Less Size
6. CONCLUSION AND FUTURE WORK

The scope of the proposed project is to provide the user a platform by implementing a new prototype for a secured payment online system for E-commerce applications. Such a payment system working on F5 steganography can provide consumer data privacy and prevents misuse of data at merchant’s side. The method is concerned only with prevention of identity theft and customer data security. This project removes the defects [1] caused by other traditional online payment systems which use simple steganography, visual cryptography, and temporary credit card number generation.

The proposed web application is tested considering various scenarios as shown in testing section and also the type of inputs given by the user. This testing process is done in order to verify all the features working in this application. Different features are implemented as application and every application is tested to get the expected working. The main intention is to provide the users a web application of high performance, high secured system.

There is huge scope for enhancement possible in this project. The strength of the resulting image with proposed encoding standard is not tested. The evaluation process can be done in the future enhancements, where different steganography tools can be used to crack the information in the image file. Many new features can be added to the current version of the application like encoding in video files.
BIBLIOGRAPHY AND REFERENCES


