**Chapter 1**

**Introduction**

* 1. **Detailed Problem Definition**

The recent procedure in issuing a passport document is by using the computer in fixing the passport photo. All the passport offices are connected through a network to exchange information to verify the correctness and authenticity of the passport. Passport images can also be transferred between offices to verify the authenticity of the passport holder.

The main problem is how to confirm the authenticity of the passport photo with the holder’s details. The passport document contains holder’s signature in addition to the holder’s details. But there is no association between the passport photo and the passport owner details. So a passport photo can be replaced with other person’s photo.

**1.2 Current Market Survey**

Juels *et al* (2005) discussed security and privacy issues that apply to e-passports. They expressed concerns that, the contact-less chip embedded in an e-passport allows the e-passport contents to be read without direct contact with an IS and, more importantly, with the e-passport booklet closed. They argued that data stored in the chip could be covertly collected by means of “skimming” or “eavesdropping”. Because of low entropy, secret keys stored would be vulnerable to brute force attacks as demonstrated by Laurie (2007).

Kc and Karger (2005) suggested that an e-passport may be susceptible to “splicing attack”, “fake finger attack” and other related attacks that can be carried out when an e-passport bearer presents the e-passport to hotel clerks. There has been considerable press coverage (Johnson, 2006; Knight, 2006; Reid, 2006) on security weaknesses in e-passports. These reports indicated that it might be possible to “clone” an e-passport.

**1.3 Need of the System**

As per the survey, we noticed that, the available systems are not that efficient in terms of verifying & authenticating documents of users means it cannot detect forgery or fraud or mask like things.Users need an application which will provide them with accurate and efficient results which will help them in proving their proof of ownership.Moreover, right now, if they want to do so they need to spend lot of time for waiting in long queues for registration purpose and after entire verification process they receive their documents at home which is quite time consuming project. To overcome these problems, our system will help applicant to easily prove their ownership.

The purpose of the improved authentication scheme is to establish a firm connection between the passport photo and passport details.

**1.4 Updations to the previous system**

As we have mentioned in the section 1.2, the current document verification & authentication methods are inefficient in terms of security & robustness and they are quite time consuming when document issual is done. To overcome the disadvantages of existing algorithm,we are using some of the modified algorithms.

**Modification of Existing algorithm**

**1.4.1. Algorithm 1: Acquire Parameters**

1. Get holder’s first name, second name, third name and surname.

2. Get holder’s Passport Number.

3. Validate the holder’s details.

4. Assign a number to each letter of the name according to the table 1.

5. Store each name’s numbers for future reference

**4.2. Algorithm 2: Watermark**

1. Consider the key value. E.g. K = "1,2,3,4".

2. Create a new key value for first name by summing the consecutive key values in a round robin fashion say K1.

Where K1(1)=K(1)+K(2)

K1(2)=K(2)+K(3)

K1(3)=K(3)+K(4)

K1(4)=K(4)+K(1)

Compute the summation of the first name by adding the code value of each character multiplied by the new key’s character in succession.

E.g. codeval(1)\*K1(1) + codeval(2)\*K1(2) +

codeval(3)\*K1(3)+……

3. Consider the result as "row".

4. Create a new key value for second name by summing the alternate key values in round robin fashion say K2.

Where K2(1)=K(1)+K(3)

K2(2)=K(2)+K(4)

K2(3)=K(3)+K(1)

K2(4)=K(4)+K(2)

Compute the summation of the second name by adding the code value of each character multiplied by the new key’s character in succession.

E.g. codeval(1)\*K2(1) + codeval(2)\*K2(2) +

codeval(3)\*K2(3)+…….

5. Consider the result as "column ".

6. Compute the summation of the third name and family name by adding the code value of each character multiplied by the actual key's character in succession.

E.g. codeval(1)\*K(1) + codeval(2)\*K(2) +

codeval(3)\*K(3)+……

7.Compute the summation of passport number by adding the code value of each character. E.g. codeval(1) +

codeval(2)+ codeval(3)+……

8. Compute the sum of third name, family name and the passport number and store the result in "sum".

**4.3. Algorithm 3: Hide Watermark**

1. Get the pixel value at (row, column) location from the original Image.

2. Find the average value of RGB [6] color for that pixel, add 1 to it and assign it to "avg".

3. Divide "sum" on "avg" to get number of pixels.

4. Compute the modulo division of "sum" over "avg" and store result in "value ".

5. Calculate Rcolumn which is equal to "column" +"number of pixel" + 1.

6. Get the pixel value at location (row, Rcolumn).

7. Get the largest value of (R,G,B) for the pixel at that location and replace it with "value".

8. Restore the pixel (R,G,B) values at the same location.

**4.4. Algorithm 4: Authenticate**

1. Select the image for which watermarking is to be applied.

2. Read the passport number for which the authentication is to be performed.

3. Perform row, column and sum computations as shown in algorithm 2 by retrieving the details from the database based on the passport number.

4. Compare the row, column and sum values obtained with the values stored in the database

5. If the step 4 is successful, perform number of pixels and value computations as shown in algorithm 3 and compare the results with the values stored n the database.

6. If the step 5 is successful, allow the holder to travel otherwise take legal proceedings on the passport holder.

**1.5 Organization of the report**

This report has been organized after the project has been done in an orderly manner.

Chapter 1 deals with Introduction of project.

Chapter 2 includes requirement analysis.

Chapter 3 includes the Methodology in detail.

Chapter 4 includes modeling & design. It gives diagrammatic overview of the project using UML diagrams.

Chapter 5 states the conclusion.

**Chapter 2**

**RequirementAnalysis**

Requirement analysis in systems engineering and software engineering encompasses those tasks that go into determining the needs or conditions to meet the needs of stakeholders ,customers. Requirement analysis is critical to success of software project.

**2.1.1 Product Functions**

Categorized in to following way by Developers and users point of view.

2.1.1.1Necessary functions:

* The system must user friendly.
* The system must platform independent.
* System should take as input (image) with any extension.
* Fast to access and process.

2.1.1.2Desirable functions:

* It should produce correct image card.
* It should not be time consuming.

2.1.1.3Other Requirement:

* User can give one input images for processing.
* Complexity should be less.

**2.1.2 User Classes and Characteristics**

* **Applicant** - They are the people who desire to obtain the documents like passport, driving license, pan card,etc and submit the information to the database.
* **Administrator** - He has the certain privileges to add the document status and to approve the issue of document. He may contain a group of persons under him to verify the documents and give suggestion whether or not to approve the dispatch of passport.
* **Verification Officer** - He is the person who upon receiving intimation from the DVAA, perform a personal verification of the applicant and see if he has any criminal case against him before or at present. He has been vetoed with the power to decline an application by suggesting it to the Administrator if he finds any discrepancy with the applicant then he communicates via this DVAA.

**2.1.3 Operating Environment**

## OE-1: Document Verification & Authentication shall operate with the following web browsers: Microsoft Internet Explorer version 5.0 & 6.0,Netscape Communicator version 4.7,netscape versions 6 & 7 and Google Chrome.

OE-2:Document Verification & Authentication shall operate on the server running current approved versions of Red Hat Linux and Apache Web Server.

OE-3:Document Verification & Authentication shall permit access to only authorized users.

Testing Tool: W3C Markup Validation Service, Auto It, Quick Test Professional (QTP)

**2.1.4 System Features**

This subsection contains the requirements for the Documentation Verification & Autheentication. These requirements are organized by the features discussed in the vision document. Features from vision documents are then refined into use case diagrams and to sequence diagram to best capture the functional requirements of the system. All these functional requirements can be traced using tractability matrix.

* + - 1. **User Registration**
         1. Description and Priority

User should provide their personal information along with their passport size photo and submit to server database.

Priority=High

2.1.4.1.2 Stimulus/Response Sequences

Stimulus: An applicant registers himself for new document approval.

Response: The system queries the applicant to submit his personal information along with his passport size photo.

2.1.4.1.3Functional Requirements

The System must provide following functionalities—

1. Provides UI to user to register himself.
2. Information filled by the applicant is stored in the database.
   * + 1. **Generate Unique keys and parameters**
          1. Description and Priority

User information and photo will analyzed for watermark information like validating user information, generating unique keys and parameter information from given user information.

Priority=High

2.1.4.2.2 Stimulus/Response Sequences

Stimulus: An applicant submits all his personal information to server.

Response: The system processes this information and generates unique key and parameters.

2.1.4.2.3Functional Requirements

The System must provide following functionalities—

1. The system should generate key for user’s confirmation.
2. The information should be watermarked on the basis of selected key.
   * + 1. **Creation of Image Card**
          1. Description and Priority

A new image card will be created for user id proof. Then we will analyze the image card to set watermark and hide watermark. The watermark can contain generated unique keys and parameter information about the user and their proof.

Priority=High

2.1.4.3.2 Stimulus/Response Sequences

Stimulus: An applicant submits all his personal information to server.

Response: The system processes this information and generates unique key and parameters. After this, it creates image card and saves it to the database.

2.1.4.3.3Functional Requirements

The System must provide following functionalities—

1. The system should generate key for user’s confirmation.
2. The information should be watermarked on the basis of selected key.
   * + 1. **Image Card Viewer**
          1. Description and Priority

User can view/access their image card. User can check/verify an image card is valid or not.

Priority=High

2.1.4.4.2 Stimulus/Response Sequences

Stimulus: An applicant wants to view his/her image card.

Response: The system retrieves the card from the database and displays it on the screen.

2.1.4.4.3Functional Requirements

The System must provide following functionalities—

1. The system should generate unique image card for each user/applicant.
2. User can check/verify whether image card is valid or not.
   * + 1. **Apply for image card verification**
          1. Description and Priority

User can apply their image card to an application. Then the application will verify the given image card is original or duplicate.

Priority=High

2.1.4.5.2 Stimulus/Response Sequences

Stimulus: An applicant gives his/her say passport a airport checkpoint for entrance inside airport.

Response: The system queries the database and perform check/compare image card with database if it matches then allow to enter system else don’t allow to enter the system as it is an intruder.

2.1.4.5.3Functional Requirements

The System must provide following functionalities—

1. The system should cross check image card with database and based on which decisions should be taken.
   * + 1. **Customer Support:**

2.1.4.6.1Description and Priority

Customer Support is used to provide online help for any query that is encountered by them while registeration.

Priority=High

2.1.4.6.2Stimulus/Response Sequences

Stimulus: A user can query about how to register on system.

Response: The system should reply for the given query.

2.1.4.6.3Functional Requirements

The System must provide following functionalities—

1. Help user to understand basic functionality of the system.
2. Allows user to follow simple steps to deal with complex tasks.

## 2.1.4.7Email Confirmation:

2.1.4.7.1Description and Priority

Email Confirmation is about confirmation of document registration that user has registered for like passport or driving license or pan card.

Priority=High

2.1.4.7.2Stimulus/Response Sequences

Stimulus: A user confirms the registration form.

Response: The system should send registeration confirmation on his/her email address.

2.1.4.7.3Functional Requirements

The System must provide following functionalities—

1. Send confirmation of successful registration on user’s Email ID.

**2.1.5 Nonfunctional Requirements**

## 2.1.5.1 Performance Requirements

1. In order to maintain an acceptable speed at maximum number of uploads allowed from a particular applicant will be any number of users can access the system at any time. Also connections to the servers will be based on the criteria of attributes of the user like his location, and server will be working whole 24X 7 times.
2. The product shall be based on web and has to be run from a web server.
3. The product shall take initial load time depending on internet connection strength which also depends on the media from which the product is run.
4. The performance shall depend upon hardware components of the client/customer.

## 2.1.5.2 Safety Requirements

The system will be safe for all the transactions.

The system must satisfy safety certifications like SSL certificates, https (http security).

## 2.1.5.3 Security Requirements

### 2.1.5.3.1 Data Transfer

The system shall use secure sockets in all transactions that include any confidential applicant information.

The system shall automatically log out all applicants after a period of inactivity.

The system shall confirm all transactions with the applicant’s web browser.

The system shall not leave any cookies on the applicant’s computer containing the user’s password and any of the user’s confidential information.

### 2.1.5.3.2 Data Storage

The applicant’s web browser shall never display a applicant’s password. It shall always be echoed with special characters representing typed characters.

The applicant’s web browser shall never display a applicant’s system generated number after retrieving from the database. It shall always be shown with just the last 4 digits of the system generated number.

The system’s back-end servers shall never display a applicant’s password. The applicant’s password may be reset but never shown.

The system’s back-end servers shall only be accessible to authenticated administrators.

The system’s back-end databases shall be encrypted.

## 2.1.5.4Software Quality Attributes

**Usability:** The system will have ease of use or ease of learning of how to register for any document like passport,driving license,pan card etc...

**Maintainability:** The system is easy to maintain. It can be easily modifiable as per changing needs of users.

**Correctness:** The system can satisfy all the required specifications and fulfill the applicant’s mission objectives.

**Integrity:** The system can provide secure access to all valid applicants. Unauthorized user access is completely controlled.

**Interoperability:** The system can be coupled with another system having same type of characteristics like verification & authentication of any document that contains photo in it.

# 2.1.5.5Other Requirements

## 2.1.5.5.1Licensing Requirements

As per ISO 9001:2000 standard for product of spectacles, lens, contact lens and frames. Website will be official web hosted over internet.

## 2.1.5.5.2Legal, Copyright, and Other Notices

Comfort glasses will display the disclaimers, copyright, word mark, trademark and product warranties of all types of spectacles, lenses & frames of different brands like United Colors Of Benetton ,Nikon ,Levis ,Puma ,Guess Eye wear, Tom Ford Eye Wear, etc.

**2.1.5.5.3Applicable Standards**

The system will be as per the industry standard

**2.1.6 Design and Implementation Constraints**

**2.1.6.1 General constraints:**

1. The interface will be in English only.
2. The main constraint here would be the checking the genuineness of the buyer, which is not always possible. There can be security risks involved.
3. The design constraints are that the browser at each place may not follow similar screen resolutions, browsers etc. This can lead to the website not having the impact it is planned to have.
4. Also the rules of the land will prohibit certain items to be sold on the site. Hence all those factors need to be filtered in.
5. Also storage space constraints may come if the listing becomes too large. Hence a strong server needs to be chosen to host the database.

### 2.16.2 Standard Development Tools:

The system shall be built using a standard web page development tool that conforms to either IBM’s CUA standards or Microsoft’s GUI standards such as ASP.NET.

### 2.1.6.3 Web Based Product:

1. There are no memory requirements
2. The computers must be equipped with web browsers such as Internet explorer.
3. The product must be stored in such a way that allows the client easy access to it.
4. Response time for loading the product should take no longer than five minutes.
5. A general knowledge of basic computer skills is required to use the product

**2.1.7 User Documentation**

As the product is Document Verification & Authentication, On-line help system becomes a critical component of the system which shall be provide like –

* It shall provide specific guidelines to a user for using the system and within the system.
* To implement online user help, link and search fields shall be provided.

**2.2 Project plan**

**Major Milestones and Dates**

|  |  |  |  |
| --- | --- | --- | --- |
| **Milestones** | **Start Date** | **Due Date** | **Priority** |
| Group Finalization | 1st of July 2013 | 8th of July 2013 | High |
| Domain finalization | 9th of July 2013 | 20th of July 2013 | High |
| Title finalization | 21st of July 2013 | 13th of August 2013 | High |
| Sponsorship Searching And Finalization | 13th of August 2013 | 16th of August 2013 | Medium |
| Requirement Gathering | 17th of August 2013 | 30th of August 2013 | High |
| Scope and Objectives finalization | 1st of September 2013 | 5th of September 2013 | High |
| Study Of IEEE Paper | 25th of August 2013 | 8th of September 2013 | Medium |
| Study of watermarking algorithms | 8th of September 2013 | 15th of September 2013 | Medium |
| SRS Preparation | 15th of September 2013 | 21st of September 2013 | High |
| Mathematical Model | 22nd of September 2013 | 30th of September 2013 | Medium |
| Design Part Completion (UML Diagrams) | 1st of October 2013 | 5th of October 2013 | High |
| Test Plan preparation | 6th of October 2013 | 10th of October 2013 | Medium |
| Preliminary Project Report Preparation | 11th of October 2013 | 12th of October 2013 | Medium |
| Implementation | 15th of December 2013 | 5th of February 2014 | High |
| Testing | 6th of February 2014 | 16th of February 2014 | High |
| Deployment and Maintenance | 17th of February 2014 | 22th of February 2014 | High |
| Final Project Report preparation | 23th of February 2014 | 2nd of March 2014 | Medium |

Table 2.1 Project Plan

**Chapter 3**

**Methodology**

3.1 Software Requirements

Operating System : Windows XP or Higher

Coding Language : Asp.Net

Back End : Sql Server 2000 or Above

3.2 Hardware specification:

CPU type : Intel Pentium V or above

Clock speed : 3.0 GHz

Ram size : 1 GB

Hard disk capacity : 80 GB

Monitor type : 15 Inch color monitor

3.3 Programming language: C#.net

3.4 Platform: Windows XP or Higher

3.5 Tools

IDE Environment : Microsoft Visual studio 2010

.Net Framework : 4.0 or above

Rational rose : 2000e

Microsoft Word : Word 2007

**Chapter 4**

**Modeling and Design**

* 1. **System Architecture**

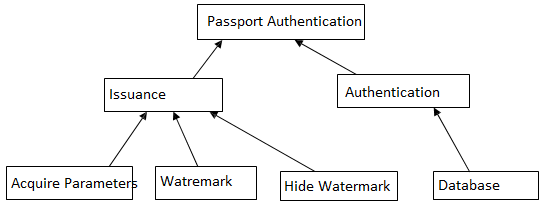


Fig: System Architecture of DVAA

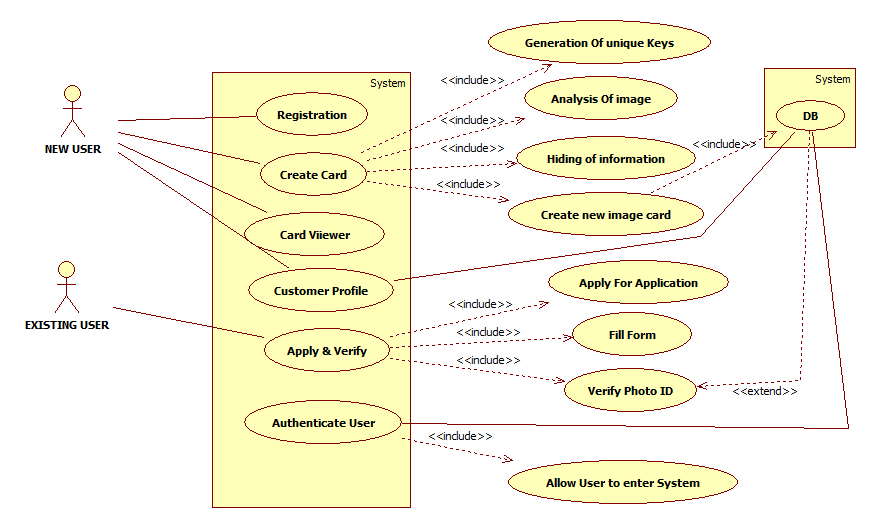
* 1. **UML Diagrams:**

Fig 4.2.1: Use Case Diagram of DVAA

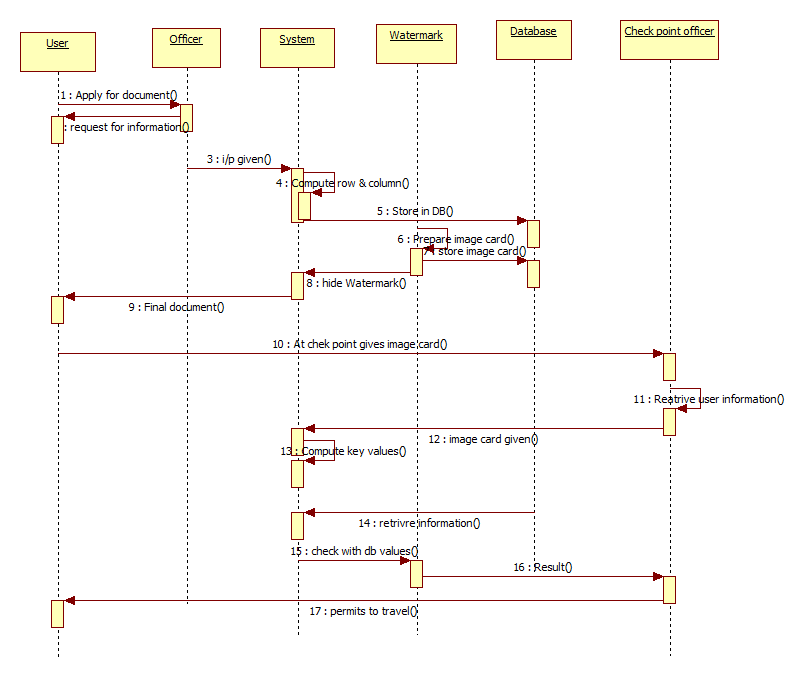
****

Fig 4.2.2: Sequence Diagram of DVAA

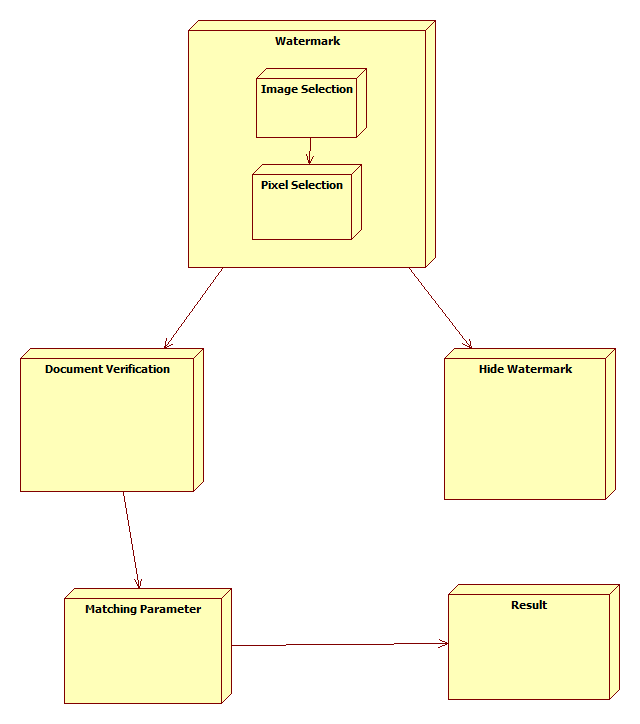


Fig 4.2.3: Deployment Diagram

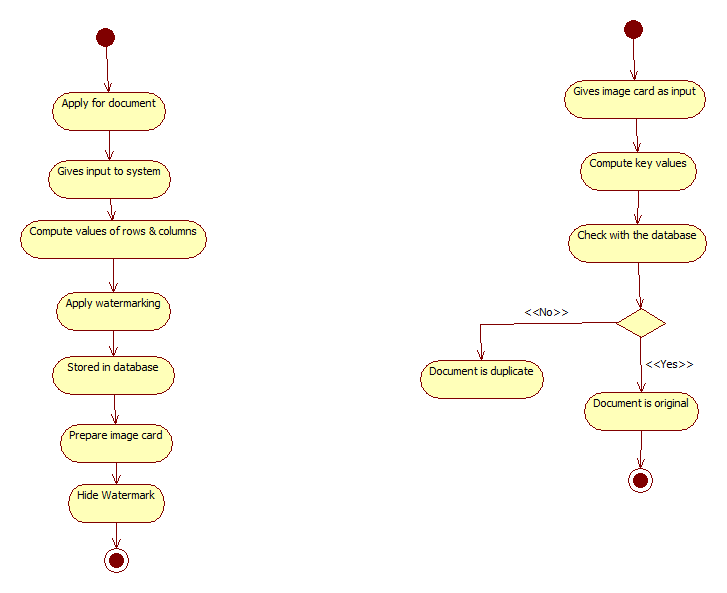


Fig 4.2.4: Activity Diagram for DVAA

**Chapter 5**

**Conclusion**

This authentication scheme embeds the invisible watermark into the passport photo to authenticate the passport’s owner. This modified scheme meets all the requirements for the watermark technique.The invisible watermark has satisfied the robustness, Invisibility, Undetectability and Security requirements. Because this technique has used only one pixel for hiding the watermark, it satisfied the robustness against image compression. The detection of presence of hidden information is a daunting task as it is time consuming to predict the key value. So it satisfies the security requirement of watermarking. It also satisfies invisibility requirement because change in one pixel is not visible to the human eye. The watermark also satisfies the Undetectability requirement since the pixel size is very small compared to the size of an image and is not easily noticeable. This method is effective and meets all the requirements of watermarking. This scheme is applicable for only one State. So to make the authentication scheme globally feasible, every state should share keys using asymmetric key cryptography. Every state should use the public key to hide the watermark during the issue of passport and private key should be used during the

verification process at the checkpoint to check the authenticity of the passport.

**Appendix A**

**GLOSSARY TABLE**

|  |  |
| --- | --- |
| Term | Definition |
| Steganography | It is a technique of hiding messages so that no one can detect message existence except sender and receiver. |
| Robutness | The embedded information is said to be robust if its presence can be reliably detected even after the image has been modified, but not destroyed beyond recognition. |
| Digital Watermarking | Digital watermarking is a technique for embedding information into a digital signal (might be a audio, image or video signal) in order to provide identity of owner. |
| Authentication | It is the procedure to authenticate original owner to certain document |

**Appendix B**

**Assignment No: 1**

**Problem Statement:** Algorithmic Strategies used in the Project.

**Algorithms used:**

1. Acquire parameter
2. Watermark
3. Hide watermark
4. Authenticate
5. LSB Algorithm

**LSB Algorithm**

* Replaces least significant bits with the message to be encoded.
* Most popular technique when dealing with images
* Simple, but susceptible to lossy compression and image manipulation

**LSB - Example**

A sample raster data for 3 pixels (9 bytes) may be:

00100111 11101001 11001000

00100111 11001000 11101001

11001000 00100111 11101011



00100111 1110100**0** 11001000

0010011**0** 1100100 1110100**0**

11001000 00100111 11101011

**Assignment No: 2**

**Problem Statement:** Why given option is chosen?

**Algorithms:**

The Algorithms we are going to use in Project:

1. LSB (Least Significant Bit)

Why we choose above algorithms?

**Benefit of LSB:**

The benefits of LSB are its simplicity to embed the bits of the message directly into the LSB plane of cover-image and many techniques use these methods. Modulating the LSB does not result in a human-perceptible difference because the amplitude of the change is small. Therefore, to the human eye, the resulting Stego-image will look identical to the cover-image. This allows high perceptual transparency of LSB.

The Advantages of LSB Algorithm are:

* Popularity
* Easy to understand and comprehend
* High perceptual transparency
* Low degradation in the image quality

**Assignment No: 3**

**Problem Statement:** Domain Specific Analysis.

**Domain: Image Processing**

**Introduction:**

**Computer Imaging:**

It can be defined a acquisition and processing of visual information by computer. Computer representation of an image requires the equivalent of many thousands of words of data, so the massive amount of data required for image is a primary reason for the development of many sub areas with field of computer imaging, such as image compression and segmentation .Another important aspect of computer imaging involves the ultimate “receiver” of visual information in some case the human visual system and in some cases the human visual system and in others the computer itself.

Computer imaging can be separate into two primary categories:

1. Computer Vision

2. Image Processing.

(In computer vision application the processed images output for use by a computer, whereas in image processing applications the output images are for human consumption). These two categories are not totally separate and distinct. The boundaries that separate the two are fuzzy, but this definition allows us to explore the differences between the two and to explore the difference between the two and to understand how they fit.

**Image Processing:**

Image processing is computer imaging where application involves a human being in the visual loop. In other words the image are to be examined and a acted upon by people.

The major topics within the field of image processing include:

1. Image restoration.

2. Image enhancement.

3. Image compression.

**Image Restoration:**

It is the process of taking an image with some known, or estimate degradation, and restoring it to its original appearance. Image restoration is often used in the field of photography or publishing where an image was somehow degraded but needs to be improved before it can be printed.

**Image Enhancement**:

Enhancement methods tend to be problem specific. For example, a method that is used to enhance satellite images may not suitable for enhancing medical images. Although enhancement and restoration are similar in aim, to make an image look better. They differ in how they approach the problem. Restoration method attempttomodel the distortion to the image and reverse the degradation, where enhancement methods use knowledge of the human visual systems responses to improve an image visually.

**Image Compression:**

Involves reducing the typically massive amount of data needed to represent an image. This done by eliminating data that are visually unnecessary and by taking advantage of the redundancy that is inherent in most images. Image processing systems are used in many and various types of environments, such as:

1. Medical community

2. Computer – Aided Design

3. Virtual Reality

**Appendix C**

Testing, Reliability parameters and Test plan

**Testing:**

Following Testing methods & Strategies, we will perform on different-different modules:

Testing methods:

1. Black Box Testing
2. White Box Testing

Testing Strategies:

1. Unit Testing
2. Integration Testing

**Reliability Parameters:**

The system will be designed with reliability as key feature:

* The system is guaranteed of providing the services to user according to his login information.
* This system is guaranteed to be reliable with maximum time.

**Other Parameters:**

**Maintainability:**

The system will be developed using the standard software development conventions to help in easy review and redesigning of the system. The system will be backed up by a full fledge documentation of the product which is available online as well as free to download*.*

**Availability:**

The system is available on demand.

**Supportability:**

The System is able to support Images of type bmp or jpg.

**Test Plan:**

|  |  |
| --- | --- |
| Test ID | 1 |
| Testing Category | To provide a system this will give access to User Registration & Login. |
| Testing Importance | Mandatory |
| Test Description | This is an actual task intended. |
| Methodof validation/verification |  |
| Priority | Highest |
| Difficulty | High |

|  |  |
| --- | --- |
| Test ID | 2 |
| Testing Category | To provide a system this will design for issuing document. System needs input as user name and all of his details. |
| Testing Importance | Mandatory |
| Testing Description | It is for multi user task. |
| Method of validation/verification | Acquire parameter algorithm |
| Priority | Highest |
| Difficulty | High |

|  |  |
| --- | --- |
| Test ID | 3 |
| Testing Category(Technical) | Applying watermarking. |
| Testing Importance | Mandatory |
| Testing Description | From the name and all the details of user new unique number will be generated as value of row and column. |
| Method of validation/verification | Watermarking Algorithm |
| Priority | Highest |
| Difficulty | High |

|  |  |
| --- | --- |
| Test ID | 4 |
| Testing Category(Technical) | Hide the key into the image of the user for verification. |
| Testing Importance | Mandatory |
| Testing Description | After the values are computed hide the identity of the document owner in the image. |
| Method of validation/verification | LSB algorithm and hide watermark algorithm |
| Priority | Highest |
| Difficulty | High |

|  |  |
| --- | --- |
| Test ID | 5 |
| Testing Category (Technical) | Authentication of the document at check point. |
| Testing Importance | Mandatory |
| Testing Description | Again the row and column values are computed from user details and match with the values stored in the database and in image. |
| Method of validation/verification | Authentication algorithm |
| Priority | Highest |
| Difficulty | High |

Appendix D

**D.1 Progress Plan Using Smart Sheet:**

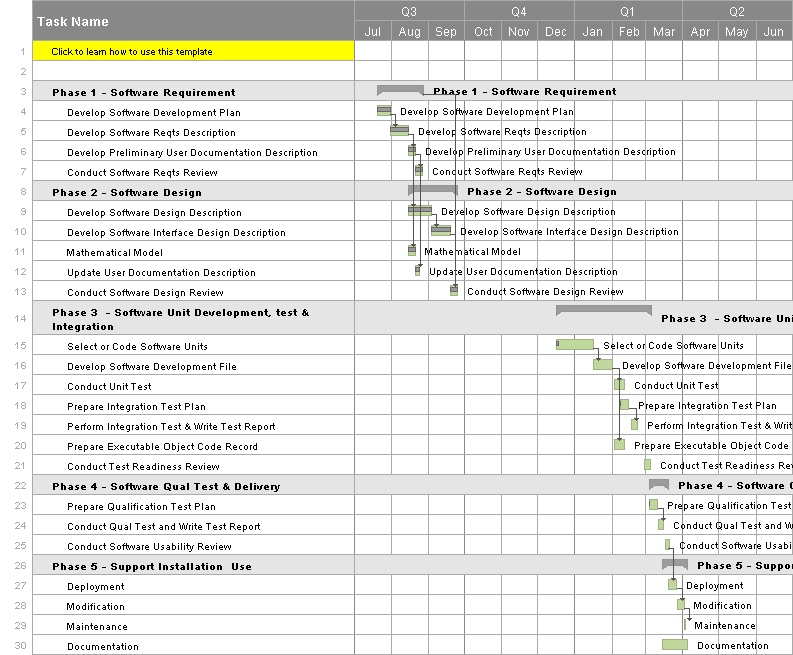
****

Fig D.1: Progress Plan

**BIBLIOGRAPHY:**

[1] AlaaH.Al-Hamami and SaadA.Al-Ani, Faculty ofInformation Technology, Amman Al-Ahliyya University, Amman, Jordan “A New Approach for Authentication Technique”Journal of Computer Science 1 (1): 103-106, 2005 ISSN 1549-3636 ©

Science Publications, 2005

[2] ManjitThapa, Dr.Sandeep Kumar Sood, A.P Meenakshi Sharma “Digital Image Watermarking Technique Based on Different Attacks”. *(IJACSA)* *International Journal of Advanced Computer Science* *and Applications, Vol. 2, No. 4, 2011*

[3] Er. Deepak Aggarwal, Er. Kanwalvir Singh Dhindsa “Effect of Embedding Watermark on Compression of the DigitalImages” JOURNAL OF COMPUTING,

VOLUME 2, ISSUE 2, FEBRUARY 2010, ISSN 2151-9617

[4] Christian S. Collberg, Member, IEEE Computer Society, and Clark Thomborson, Senior Member, IEEE “Watermarking, Tamper-Proofing, and Obfuscation

Tools for Software Protection” IEEE TRANSACTIONS ON SOFTWARE ENGINEERING,VOL. 28, NO. 8, AUGUST 2002

[5] Stefan, K. and F.A.P. Petitcolas (Eds.), 2000.Information Hiding techniques for steganography and digital watermarking. ISBN 1-58053-035-4 © Artech House, Inc.

[6] Rafael C. Gonzalez and Richard E. Woods, 2001 “Digital image processing”, second edition ISBN 0-201-18075-8Prentice hall publications