(Image and Video Steganography)

Table of Contents

Chapter 1
Introduction

Since the rise of the internet one of the most crucial factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data to keep the message secret. Unfortunately, it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography. Steganography is the art and science of invisible communication. Steganography is the art of passing information in the manner the very existence of the message is unknown. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The formation of steganography has come from Greek word “Stegosgrafia” which means “cover writing” [1]. In Image and video steganography the information(Text) is hidden exclusively in selected file.

1.1 Purpose

The purpose of this document is to present Steganography process in Image / Video files. The main purpose of this project is to develop an application software that could take a message (secret massage) from user, encrypt it and then embed it into an image / video file using LSB algorithm and finally take a key(as a password) and embed it in image/video for make more secure data. Thus, produce a new stego_file which is alike the earlier one. The information(image, secret text ,password, file name) of that file will be saved in database along with the user email address which is logged in. And also, that all information can be seen later by the that particular user itself. The next part of this project could decrypt that stego_file and retrieve secret information(Text) from Image/Video file.

1.2 Scope

The scope of the project is to limit unauthorized access and provide better security during message transmission. To meet the requirements, I use the simple and basic approach of steganography. The scope of this application software is that it can embed selected data by applying suitable algorithm. In the same way application provide data extracting feature for extract hidden data from embedded file. Benefits of the application is that user use this for hide secret text in image/video along with password. After steganography is applied on file there is not suspicious change is noticed so this

information can easily send to other person with secure and trusted way and also this data can be seen by user itself later if the user forgets the password of particular file than user can check this password in database. Objective is providing user secure and user-friendly interface to embed text. And goal is to provide efficient way to embed and extract data without suspected. The problem I have is that this project not deals with audio in video.

1.3 Definitions, Acronyms, and Abbreviations.

LSB	Least Significant Bit.
stego_medium	It is an image/video file on which steganography have been applied.
cover_medium	It is an image/video file in which user embed secret data.
Data_to_hide(H)	It is a text file data which will be hide in cover medium.
stego_key	It is a text key which is used for making data more secure, as a password.
F	F is an algorithm which is used to implement Steganography.
Place_to_save(PS)	It's a place or directory where user will save file.
Hidden_data	Data which had been hidden in stego_medium.

1.4 References

[1] T. Morkel, "Steganography", An overview of steganography,
http://repository.root-me.org/.../EN%20-%20Image%20Steganography%20Overview.pdf

1.5 Overview

This document consists of briefly explanation about the functionality of project. This includes functional requirement and the non-functional requirement of the project. Its include use cases of the functions. This explained the reaction of the system on the inputs.

1.6 Product Perspective

This steganography technique is implemented for two platforms one is desktop application using c# and second is android application using advance java. Both Products must be hide data into cover_medium and makes it stego_medium with or without password. Also extract data from stego_medium with or without password. Password is a stego_key. This application software's is a secure way of encrypting data and hide it into another file by which way user can feel secure about their data. After using this product user can send that file though network easily and receiver can easily extract his/her data by using this application software. Desktop application is performing both image/video steganography and android version only implement steganography in image only.
As far as dependencies concern the desktop application needs window operating system up to window 7 to window 10 with latest Framework. And android application needs

minimum 4.3.0 android version. If we talk about the similarities and differences of products with other in market than the first and major difference is the database is present in both application platforms and other products in market doesn't use databases And might be used different algorithms. Similar thing is that after all differences all that kind of products hide and unhide secret data.

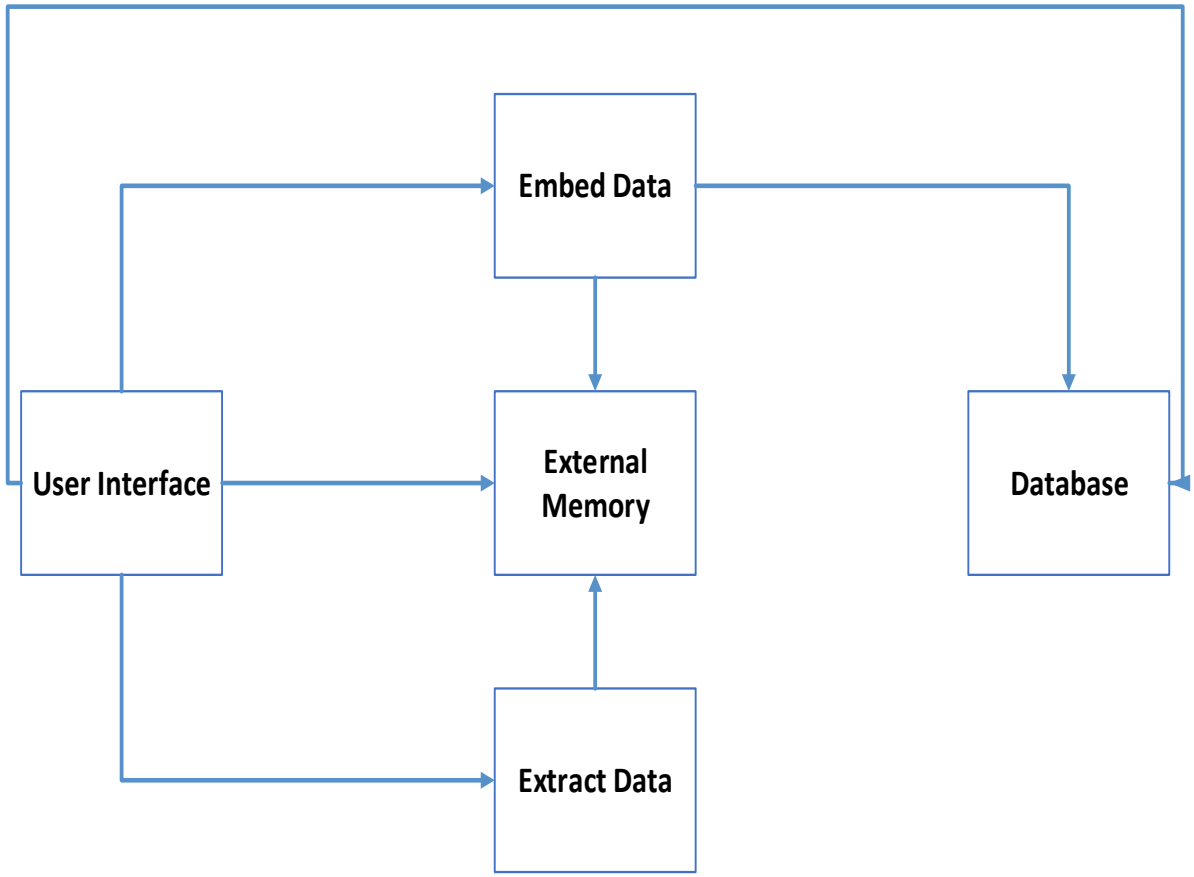


Figure 1: Block diagram of system

The following subsections describe how the software operates inside various constraints.

1.6.1 System Interfaces

- ✓ Windows platform needed for desktop application and for android application needed minimum 4.3 android version.
- ✓ In windows minimum Net framework 4.0 or higher needed.
- ✓ Microsoft SQL server needed for desktop application
- ✓ Firebase is needed for android application

1.6.2 Interfaces

- ✓ GUI (Graphical user interface)
- ✓ GUI interfaces for both application android and desktop.
- ✓ The interface is quite simple and user friendly.
- ✓ Event driven interface
- ✓ There is no need to learn how to use these applications even a regular computer user can easily use these applications jbut condition is the user must know for what purpose he/she uses this application.

1.6.3 Hardware Interfaces

- ✓ Personal PC needed with efficient hardware specification for desktop application.
- ✓ Android device needed.
- ✓ Secondary memory to store embedded data.

1.6.4 Software Interfaces

- ✓ Microsoft Windows minimum 7 to latest with latest Net framework for desktop application.
- ✓ Android minimum 4.3 KitKat or higher for android device.
- ✓ Microsoft SQL server management studio 2017

1.6.5 Communications Interfaces

- ✓ Uses only local memory for desktop application.
- ✓ Uses firebase cloud system for android application.

1.6.6 Memory Constraints

- ✓ Needs primary memory(RAM) minimum 1GB or more.
- ✓ Needs secondary memory(Hard drive) 512MB or more.

1.6.7 Operations

- ✓ Information about image(name, image itself, password, secret text) must be saved in database in desktop application as a backup.
- ✓ Information about video(name, password, secret text) must be saved in database in desktop application as a backup.
- ✓ Image must be display on UI before and after steganography applied.
- ✓ Video must be display on UI before and after steganography applied.
- ✓ Information must be shown according to the email address logged in.

1.6.8 Site Adaptation Requirements

Hardware Requirements	**Software requirements**
A standalone computer	Microsoft windows with Net Framework latest
In Windows exe. File must be installed.	Windows 8 or higher
Secondary memory to store all the images and videos	Windows 8 or higher

1.7 Product Functions

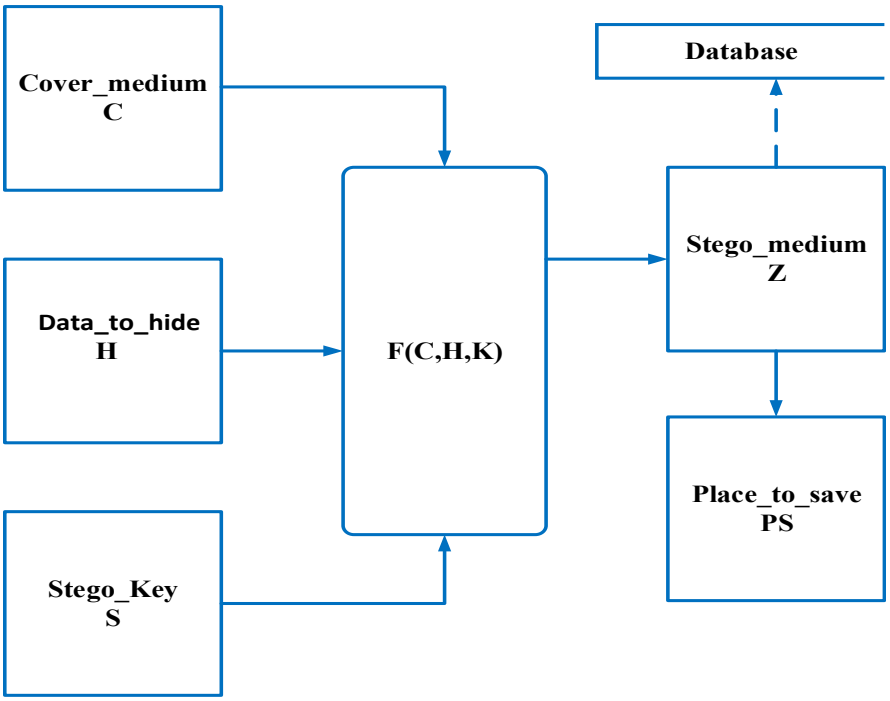


Figure 2.1: Steganography Encoder

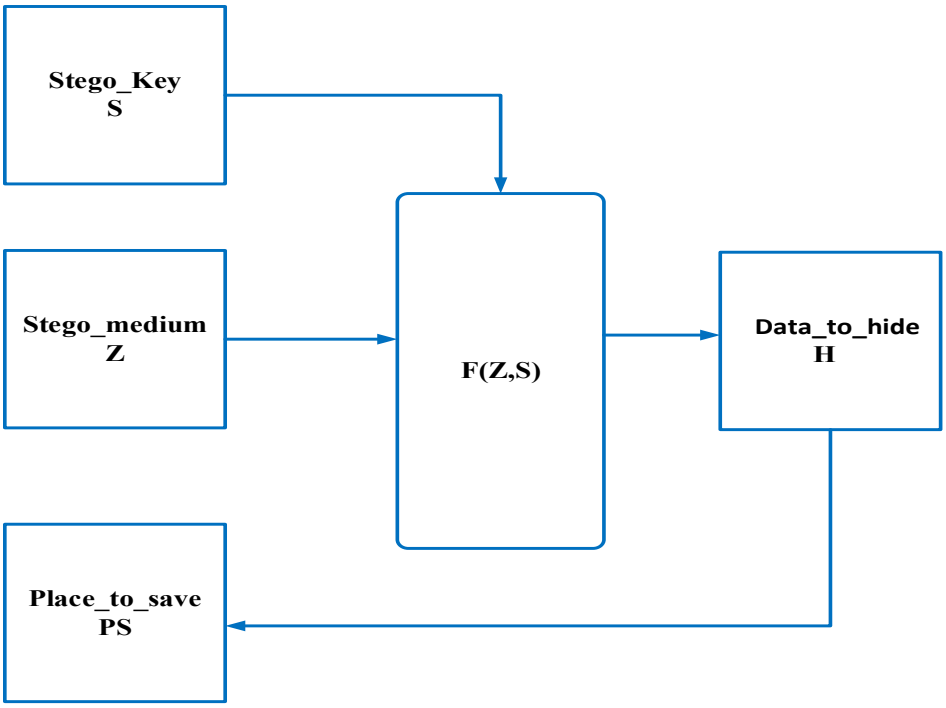


Figure 2.2: Steganography Decoder

1.8 User Characteristics

All users can use this application those are at least familiar with Microsoft windows operating system and familiar with installation of applications. User can perform steganography task, if user known about what this technique do not how this is done.

- ✓ User should know about what Steganography is.
- ✓ User should be normal user of computer.
- ✓ No need of specific educational level.

1.9 Constraints

- ✓ Every user can only see its own information about image and video information in database.
- ✓ Every user must first login or register to use desktop application
- ✓ In android not, compulsory login to use application this is only for user easiness.
- ✓ For desktop application there must be Microsoft windows platform available and machine having at least 1GB ram and 2.0 GHZ processer.
- ✓ For android minimum 4.3 KitKat must be used.
- ✓ Only jpg, bmp, png formats can be used in Image steganography
- ✓ Only avi. Format can be used for video steganography

1.10 Assumptions and Dependencies

Assumptions: Here's assumption is that the software would install on Microsoft operating system e.g. (Window 7-10) and on that operating system Net framework would be installed for desktop application. And for android application there is minimum 4.3 KitKat version available.

Dependencies: If software is updated with the passage of time user could be installed latest version of this software and this document will also updated according to the situation.

1.11 Apportioning of Requirements

- ✓ Audio steganography
- ✓ Image in image steganography
- ✓ Desktop Application could use to cloud(Real time database) system along with local database.

Chapter 2
Software Requirements Specification

2.1 Specific Requirements

2.1.0 Specific Requirements for desktop application

2.1.1 Registration

- ✓ New user must first get register himself to use desktop application not necessary in android version.
- ✓ Once specific email is registered than this email never again could register means unique email is important.

2.1.2 Login

- ✓ Every user must log in using register email address and password in desktop application not necessary in android version.
- ✓ There must be forget password facility available.

2.1.3 Image Steganography

Image steganography section must present in menu bar. And this section further having two more sections given below.

2.1.3.1 Image Embed

- ✓ Image embed section must present in menu bar. Which will take user to text embed in image steganography process form.
- ✓ Here user must choose or select image on that user want to apply steganography this image must show in picture boxes before and after steganography applied and the path of that image must be shown in textbox.
- ✓ Than user must type secret text which user want to hide in image.
- ✓ Than user should type password in textbox to secure secret text this password is necessary to extract text.
- ✓ Last and important step is there must be Embed button present on form. After button click by user, steganography is applied and information about image must store in database if any necessary requirement skipped than there must be message shown.

2.1.3.2 Image Extract

- ✓ Image extract section must present in menu bar. Which will take user to text extract from image steganography process form.
- ✓ Here user must choose or select image on that user want to apply steganography this image must show in picture boxes before and after steganography applied and the path of that image must be shown in textbox.
- ✓ Than user should type password(if required) in textbox to extract secret text this password is used to extract text.
- ✓ Than user must click on extract button if secret text is extracted successfully than show message also text will show in textbox if not than also show message.
- ✓ If secret text extracted successfully than there should be save button present from where user can easily save this text to secondary memory in txt. File.

2.1.4 Video Steganography

Video steganography section must present in menu bar. And this section further having two more sections given below.

2.1.4.1 Video Embed

- ✓ Video embed section must present in menu bar. Which will take user to text embed in video steganography process page.
- ✓ Here user must select video on which user want to apply steganography .
- ✓ Selected video must show on form with running state.
- ✓ User must enter secret text which user want to hide in video.
- ✓ User should enter password to secure secret text.
- ✓ Finally, user must click on Embed button to apply video steganography and if process completed or not must show message.

2.1.4.2 Video Extract

- ✓ Video extract section must present in menu bar. Which will take user to text extract from video steganography process form.
- ✓ Here user must select video.
- ✓ User should enter password(if necessary).
- ✓ Click on extract button to extract secret text if process completed information about video must save in database or not show message.

2.1.5 More

- ✓ More section must present in menu bar. Which having further two sections given below

2.1.5.1 View image data record

- ✓ In this section user must see information(path and name, secret text, password, image itself) about image that used in image embed process according to the email.
- ✓ Here user can search image by id and can see image in picture box if click on image id.

2.1.5.2 View video data record

- ✓ In this section user must see information(path and name, secret text, password) about video that used in video embed process.
- ✓ Here user can see information about video according to the email.

2.1.6 Specific Requirements for android application(only image steganography)

2.1.6.1 Registration

- ✓ User should register itself by using email and password and this information saved in cloud database.

2.1.6.2 Login

- ✓ User should login before using application this process can be skipped once user skipped the login fragment never shown as first page in application.

2.1.6.3 Embed Text

- ✓ In this section user must select Image and that image will show in image box.
- ✓ Then secondly user must type secret text which user want to hide .
- ✓ Lastly user should be type password(optional) and click on embed text and finally save image in secondary memory. Which can be see in gallery with “stego” folder tag. These three steps take place in three different tab.

2.1.6.4 Extract Text

- ✓ In this section user must select Image and that image will show in image box.
- ✓ Secondly user click on extract button and if image having password protection then asked for password otherwise extract text and show in textbox.

2.2 External Interfaces

2.2.0 External Interfaces for desktop application

2.2.1 Login and registration

- ✓ Registration takes email(string or text) password(string or text) and recovery pin(string or text) as input and after registration this provide output as take user to login page.
- ✓ Login takes email(string or text) and password(string or text) as input and takes user into the application.

2.2.2 Embed Image

- ✓ This section takes image(.JPEG, .BMP, .PNG), password(string or text) , and secret text(string or text) as input from user and provide embedded image as an output to user which user can save on external memory.

2.2.3 Extract image

- ✓ This section takes image(.BMP, .PNG), password(string or text) as input and provide output as secret text(string or text) which is extracted from embedded image.

2.2.4 Embed Video

- ✓ This section takes video(.avi), password(string or text) , and secret text(string or text) as input from user and provide embedded video(.avi) as an output to user which user can save on external memory.

2.2.5 Extract Video

- ✓ This section takes video(.avi), password(string or text) as input and provide output as secret text(string or text) which is extracted from embedded video.

2.2.6 Image information in database

- ✓ Information of image like (name and path, secret text, password, image itself) takes as input where name and path(string or text) secret text(string or text) password(string or text) image(image converted in byte[] array) from image embed section and this data display in information in database section.

2.2.7 Video information in database

- ✓ Information of video like (name and path, secret text, password) takes as input where name and path(string or text) secret text(string or text) password(string or text) from video embed section and this data display in information in database section.

2.2.8 External Interfaces for android application(only image steganography)

2.2.8.1 Login and registration

- ✓ Registration takes email(string or text) password(string or text) as input and after registration this provide output as take user to login page.
- ✓ Login takes email(string or text) and password(string or text) as input and takes user into the application.

2.2.8.2 Embed Image

- ✓ This section takes image(.JPEG, .BMP, .PNG), password(string or text) , and secret text(string or text) as input from user and provide embedded image as an output to user which user can save on external memory.

2.2.8.3 Extract image

- ✓ This section takes image(.BMP, .PNG), password(string or text) as input and provide output as secret text(string or text) which is extracted from embedded image.

2.3 Functions

2.3.0 Main Functions for desktop application

- ✓ Registration(**mandatory**).
- ✓ Login(**mandatory**).
- ✓ Take input secret text, image, password.
- ✓ EmbedText(string text, Bitmap bmp).
- ✓ Take input image, password.
- ✓ ExtractText(Bitmap bmp).
- ✓ Take input secret text, video, password.
- ✓ EmbedText(string text, Bitmap bmp) for video.

- ✓ Take input video, password.
- ✓ ExtractText(Bitmap bmp) for video.
- ✓ SaveImageInformation.
- ✓ SaveVideoInformation.

2.3.1 Main Functions for android application

- ✓ Registration(**optional**).
- ✓ Login(**optional**).
- ✓ Take input secret text, image, password.
- ✓ EmbedText(string text, Bitmap bmp).
- ✓ Take input image, password.
- ✓ ExtractText(Bitmap bmp).

2.4 Performance Requirements

2.4.1 Static numerical requirements for desktop application

- ✓ User can terminate application any moment, but software will ask once to leave confirmation.
- ✓ Only one user can use this application simultaneously its offline application.
- ✓ For image(30 MB) and for video memory as less as video could be but in time less than 240 to second and format must be only .avi.

2.4.2 Dynamic numerical requirements for desktop application

- ✓ Only one task can be proceeded in single time.
- ✓ Registration and login done offline and done in maximum 2 second it also depends on machine speed.
- ✓ Image steganography embed, or extract will be done in 4 sec maximum this process mostly depends on machine speed rather than application.
- ✓ Video steganography embed, or extract will be done according to the size of video.

2.4.3 Static numerical requirements for android application

- ✓ User can terminate application any moment, but software will ask once to leave confirmation.
- ✓ Only one user can use this application simultaneously its use cloud for only register users in cloud system and create backup for admin.
- ✓ For image size (5 MB).

2.4.2 Dynamic numerical requirements for desktop application

- ✓ Only one task can be proceeded in single time.
- ✓ Registration and login verify by cloud database, so internet and the speed of login and registration depends on internet speed.
- ✓ Image steganography embed, or extract will be done in 20 sec maximum this process mostly depends on device speed rather than application.

2.5 Logical Database Requirements

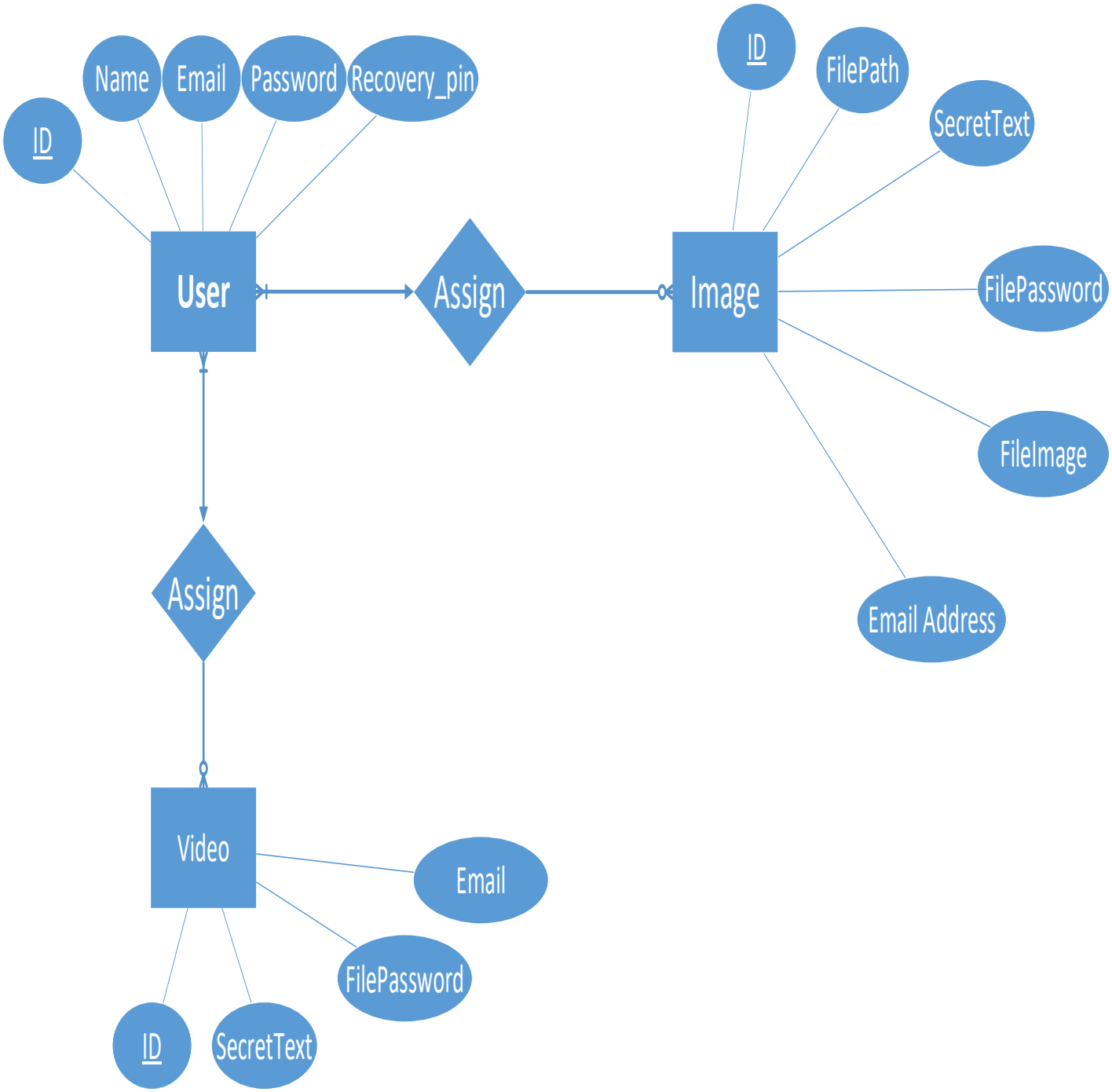


Figure 3.1 ER diagram for desktop application

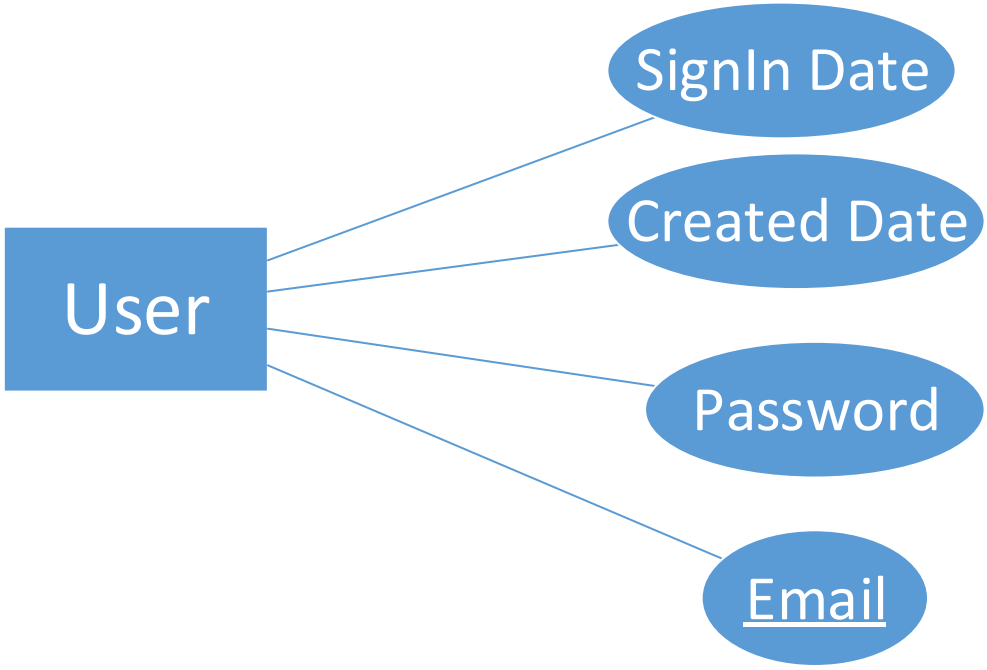


Figure 3.1 ER diagram for android application

2.6 Design Constraints

- ✓ To get better performance while using desktop application or android application better to use best performance machines in hardware .
- ✓ Don’t use less than 1gb ram and 2.0 Ghz processer for desktop application .
- ✓ Don’t use big video to apply steganography.

2.6.1 Standards Compliance

2.7 Software System Attributes

2.7.1 Reliability

Applications should not crash in any situation e.g. if user enter invalid entries or load unsupported files. In this situation applications should popup error message. Applications interface should be easy to use and user-friendly. If user input large data than user must wait until process complete, but the applications should be responsive in this situation.

2.7.2 Availability

Applications should be accessible for everybody to use. Applications must start when ever user want to use. Applications must never start like service in background after exit. If applications fail in any unexpected situation than user should restart the applications and application must be available for use.

2.7.3 Security

Application should be secure not everyone can change code else than developer.
Log of user must exist in android application to watch unexpected entrance.
For malicious access user should use antivirus there is no anti malicious program in products.

2.7.4 Maintainability

With the passage of time applications should have update for better performance and as a response of user feedback. One of the key points is, maintenance cost of applications should not exceed from the cost of making application.

2.7.5 Portability

Applications should be portable, but desktop application is not platform independent desktop application is only useable on Microsoft windows systems and android app must be run on android devices. Applications should be easily reuse on any windows platform without any problem. Which windows having minimum 4.3 NET framework. And for android up to 4.3 KitKat application must run on that devices efficiently.

ID	Characteristic	H/M/L	1	2	3	4	5	6	7	8	9	10	11	12
1	Correctness	H											*	
2	Efficiency	H											*	
3	Flexibility	M							*					

4	Integrity/Security	H											*	
5	Interoperability	L	*											
6	Maintainability	H											*	
7	Portability	M							*					
8	Reliability	M							*					
9	Reusability	H											*	
10	Testability	H											*	
11	Usability	H											*	
12	Availability	H											*	

2.8 Organizing the Specific Requirements

For anything but trivial systems the detailed requirements tend to be extensive. For this reason, it is recommended that careful consideration be given to organizing these in a manner optimal for understanding. There is no one optimal organization for all systems. Different classes of systems lend themselves to different organizations of requirements in section 3. Some of these organizations are described in the following subclasses.

2.8.1 System Mode

- ✓ There is only one mode of system.
- ✓ No user and admin mode separated.
- ✓ User mode is the only mode which having all possible access at certain level.

2.8.2 User Class

- ✓ Every user is considered as equal level users.
- ✓ There is no admin user.
- ✓ All possible accesses are granted to all users.

2.8.3 Objects

- ✓ User
- ✓ Image
- ✓ Video

2.8.4 Feature

- ✓ Image Steganography
- ✓ Video Steganography
- ✓ Save image data in database
- ✓ Save video data in database

2.8.5 Stimulus

Some systems can be best organized by describing their functions in terms of stimuli.

- ✓ Not used in applications

2.8.6 Response

- ✓ Applications must be highly responsive.
- ✓ In any case even if application gets stuck.

2.8.7 Functional Hierarchy

- ✓ **Registration**

1. Input required Email, password etc.

- ✓ **Login**

1. Input registered email and its corresponding password to enter in application

- ✓ **Image steganography(text embed) used in both applications**

1. Input image
2. Input secret text
3. Input password(optional)
4. Embed
5. Data will be saved in database about image.

- ✓ **Image steganography(text extract) used in both applications**

1. Input image
2. Input password(optional)
3. Extract
4. If process complete successfully than secret text will be display in separate textbox
5. This text can be saved in txt. File on external memory.
6. Data about image can be seen in view data in database section.

- ✓ **Video steganography(text embed) used only in desktop application**

1. Input video
2. Input secret text
3. Input password(optional)

4. Embed
5. Data about video stored in database about video

✓ **Video steganography(text extract) used only in desktop application**

1. Input video
2. Input password(optional)
3. Extract
4. If process complete successfully than secret text will be display in separate textbox
5. This text can be saved in txt. File on external memory.
6. Data about video can be seen in view data in database section.

2.9 Additional Comments

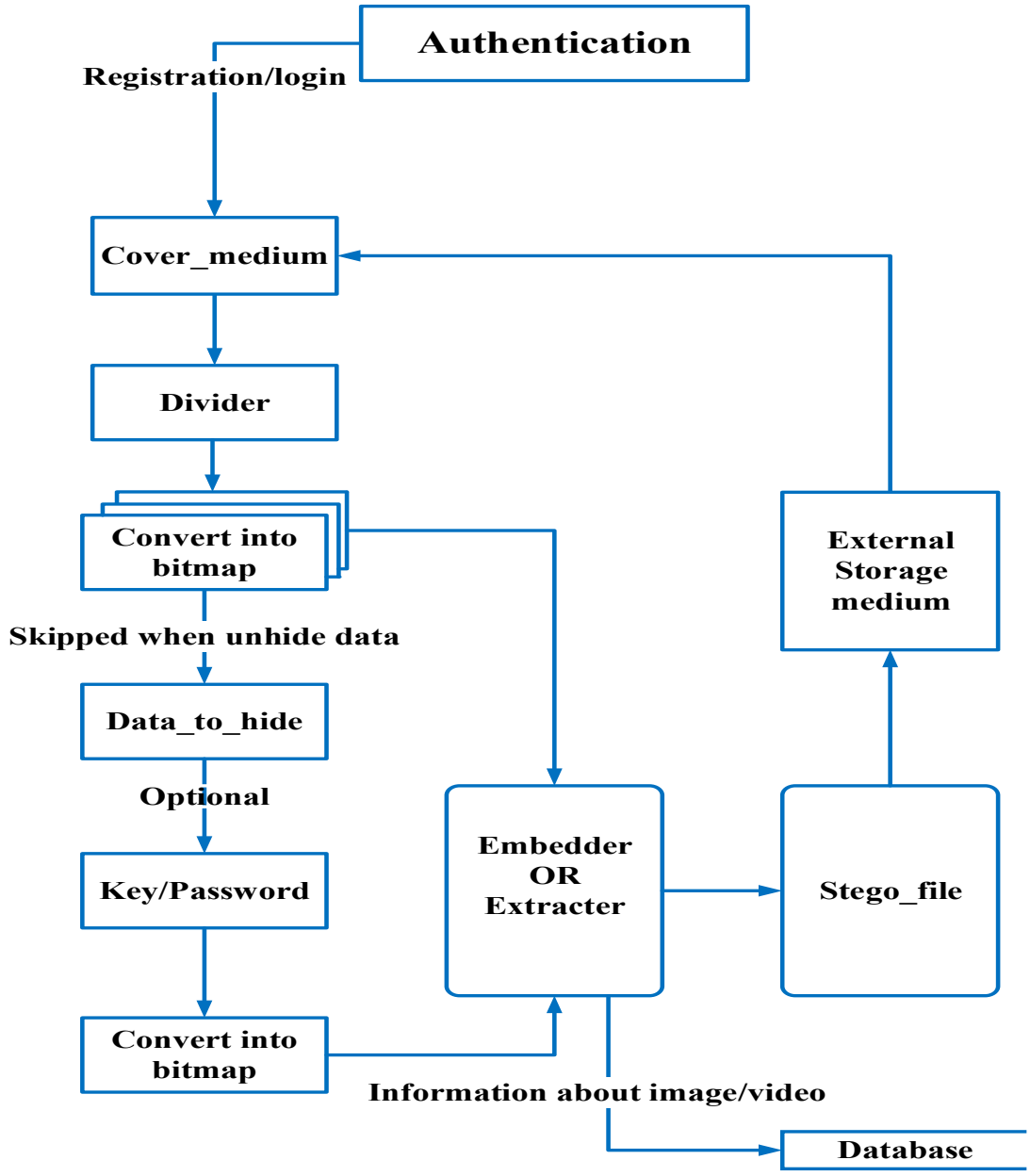
Whenever a new SRS is contemplated, more than one of the organizational techniques given in 3.7 may be appropriate. In such cases, organize the specific requirements for multiple hierarchies tailored to the specific needs of the system under specification.

Three are many notations, methods, and automated support tools available to aid in the documentation of requirements. For the most part, their usefulness is a function of organization. For example, when organizing by mode, finite state machines or state charts may prove helpful; when organizing by object, object-oriented analysis may prove helpful; when organizing by feature, stimulus-response sequences may prove helpful; when organizing by functional hierarchy, data flow diagrams and data dictionaries may prove helpful.

In any of the outlines below, those sections called “Functional Requirement i” may be described in native language, in pseudocode, in a system definition language, or in four subsections titled: Introduction, Inputs, Processing, Outputs.

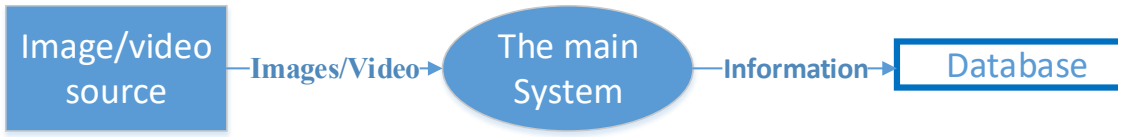
Chapter 3
System Design and Architecture

3.1 Architectural Design



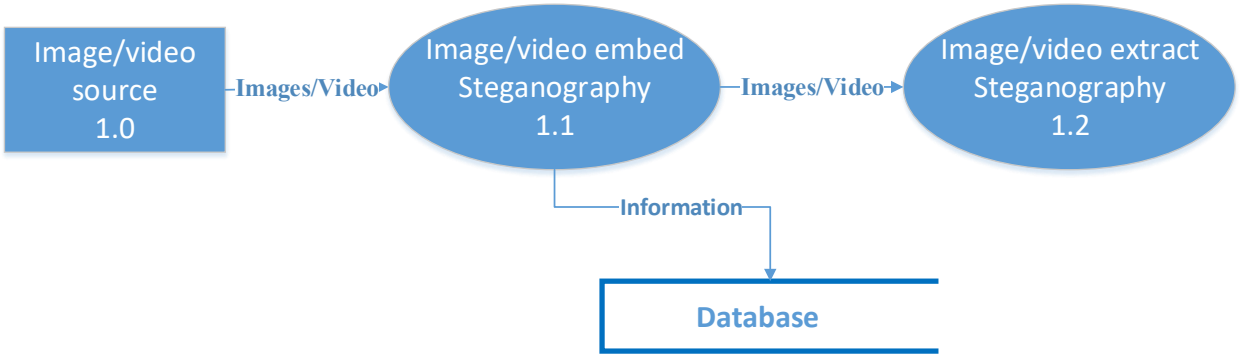
3.2 Decomposition Description

Level 0 DFD

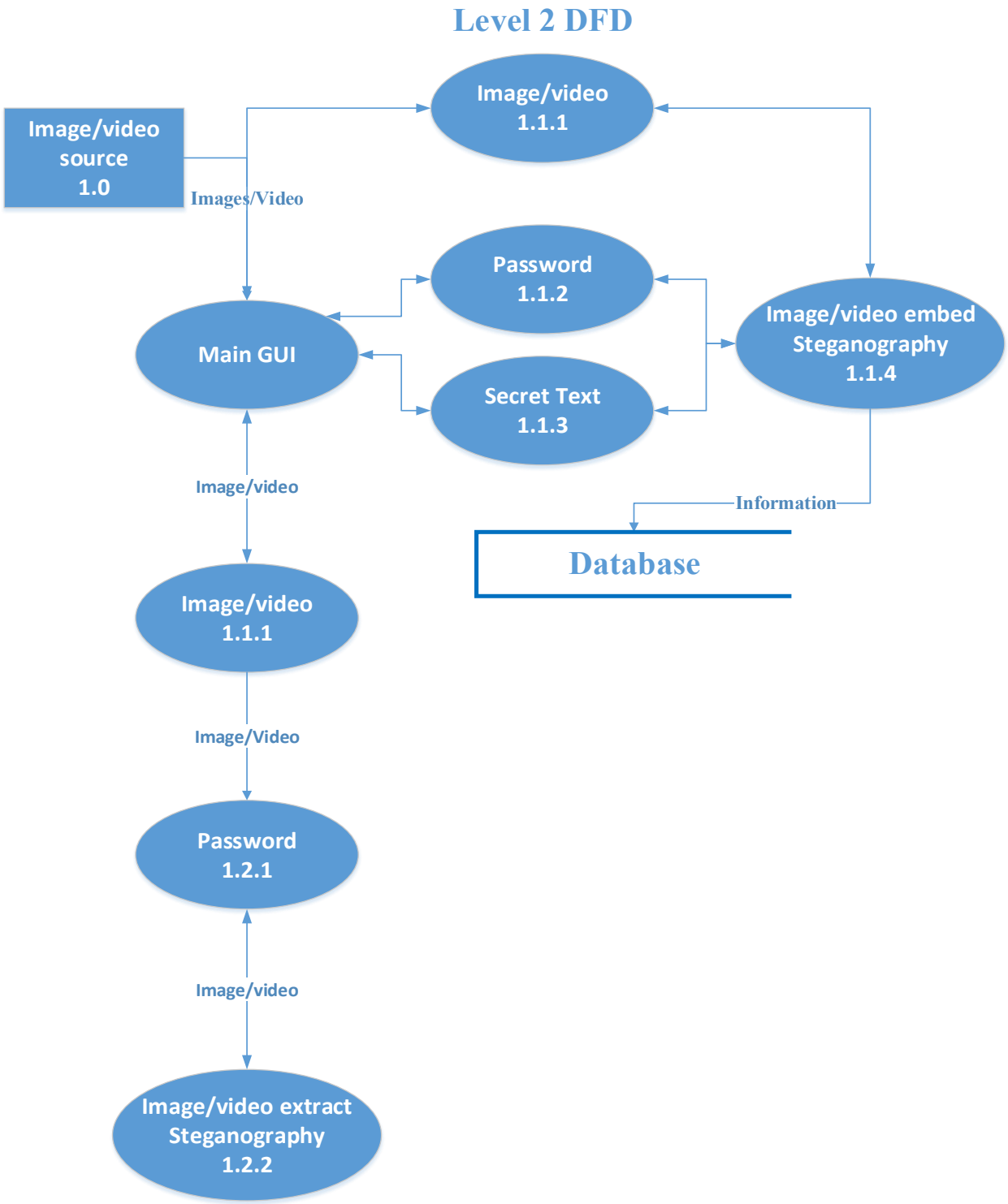


Level 0: In this level only, main working and dataflow shown in diagram. There are basically three main steps in desktop application.

Level 1 DFD



Level 1: In this level more, detail is provided about processes in application and data flow. Where 1.0 is process in which user input image/video. 1.1 is process of apply embed steganography also save information in data base about image and video.1.2 is process of apply extract steganography.



Level 2: In this level more and precise detail is provided about processes and data flow in application step by step.

3.3 Design Rationale

Reason of selecting this design is it's easy to understand and easy to implement.
Design process is mostly depended on developer. Any developer can make design according to the user will and some time his own will. Because user mostly just tell what the application or system will gone be work not how.
we select Microsoft windows dependent platform because mostly its easy to develop design and maintain. Visual studio c# is used to develop desktop application in which everything is available to develop advance applications. We don't use java in desktop application because we use it in android version. Audio steganography is tradeoff from project because of introduction in future versions.
And for android I use android studio and java. Android studio is powerful tool to develop android applications design. In android application we tradeoff video and audio steganography because of small device slower machines as compare to personal computers but video and audio could be considered in future versions.

3.4 Data Description

✓ **Image steganography Process used in both applications:**

- Images treated as bitmap[] to process steganography.
- Secret Text treated as string to process steganography.
- Password treated as string to process steganography.

✓ **Image and its information storage:**

- Image stored on external memory as png, bmp format also used in android application.
- Image stored in dataset using byte[].
- Secret Text stored in SQL database as varchar.
- Password is stored in SQL database as varchar.

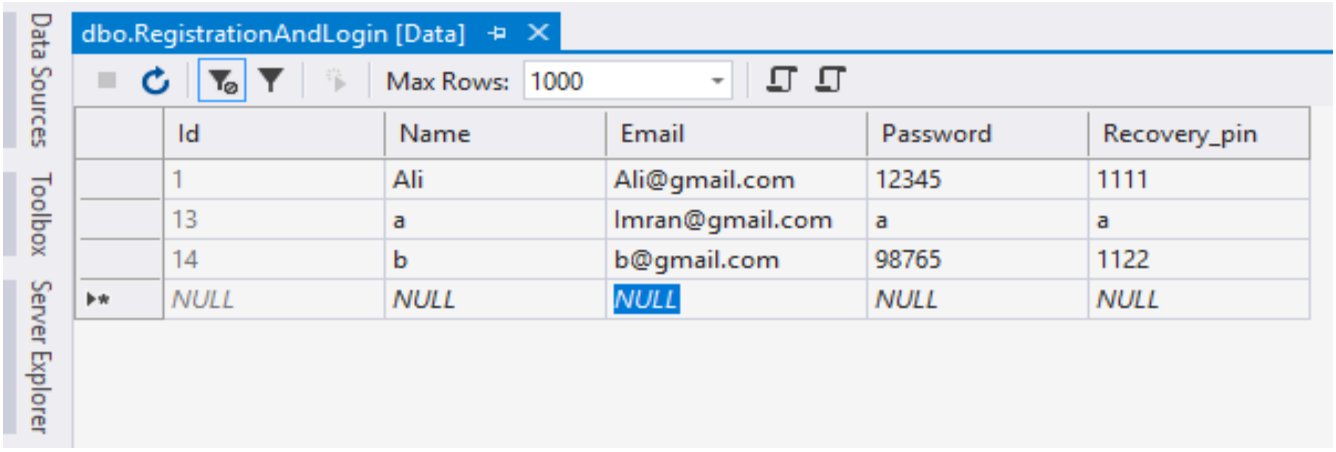
✓ **Video steganography Process:**

- For Read and write video, treat as a per frame as a bitmap[].
- Secret Text treated as string to process steganography.
- Password treated as string to process steganography.

✓ **Video and its information storage:**

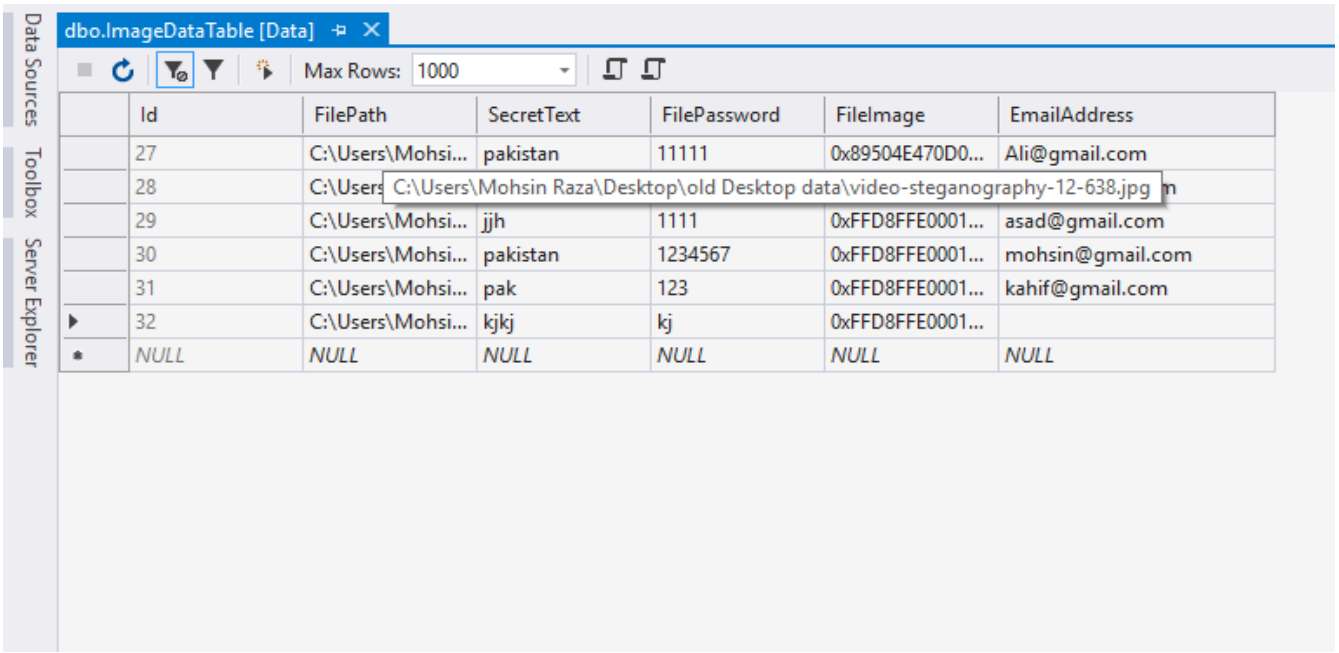
- Video stored on external memory as avi. format.
- Secret Text stored in SQL database as varchar.
- Password is stored in SQL database as varchar.

3.5 Data Dictionary



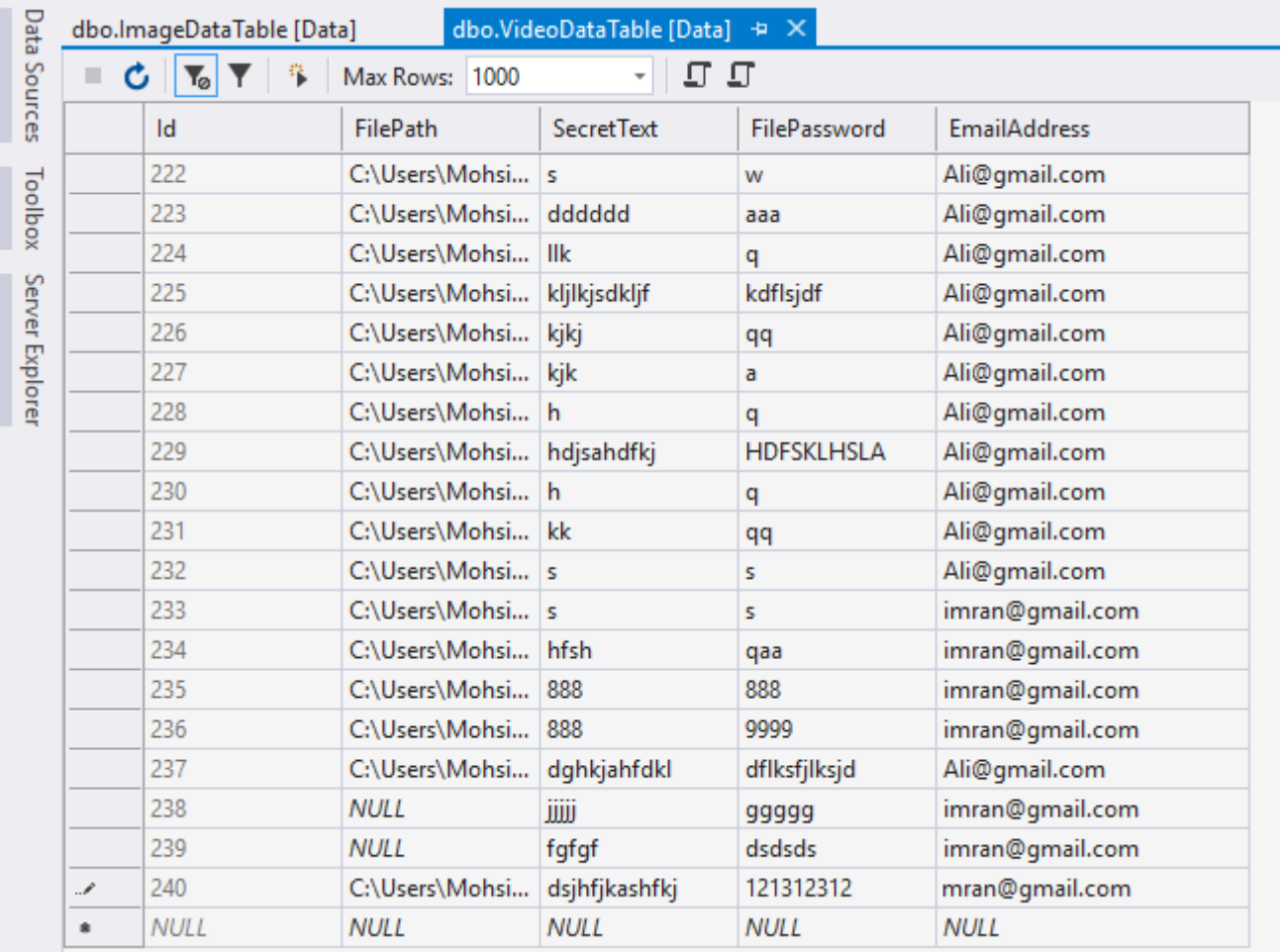
Id	Name	Email	Password	Recovery_pin
1	Ali	Ali@gmail.com	12345	1111
13	a	Imran@gmail.com	a	a
14	b	b@gmail.com	98765	1122
NULL	NULL	NULL	NULL	NULL

Table of Registration and login(desktop application)



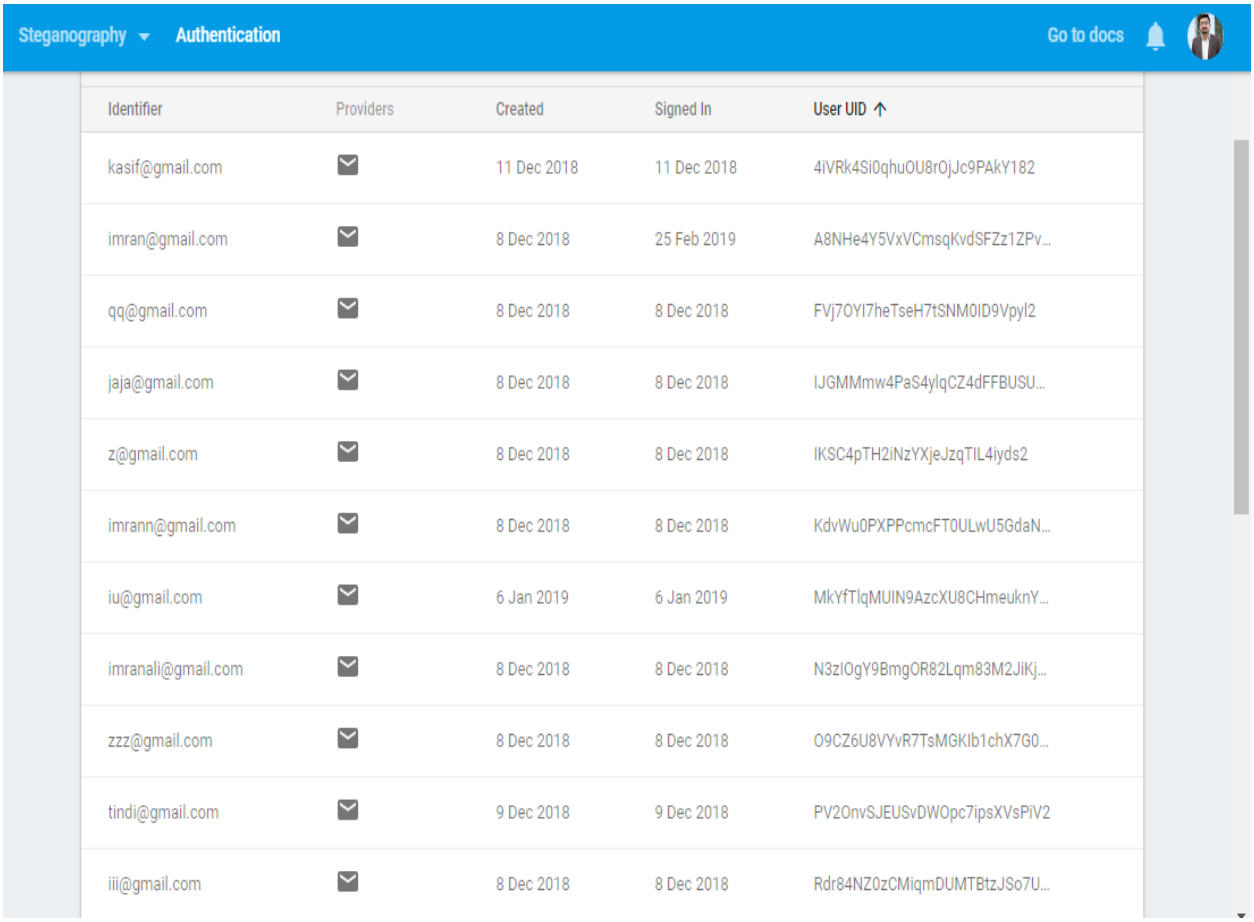
Id	FilePath	SecretText	FilePassword	FileImage	EmailAddress
27	C:\Users\Mohsi...	pakistan	11111	0x89504E470D0...	Ali@gmail.com
28	C:\Users				
29	C:\Users\Mohsi...	jjh	1111	0xFFD8FFE0001...	asad@gmail.com
30	C:\Users\Mohsi...	pakistan	1234567	0xFFD8FFE0001...	mohsin@gmail.com
31	C:\Users\Mohsi...	pak	123	0xFFD8FFE0001...	kahif@gmail.com
32	C:\Users\Mohsi...	kjkj	kj	0xFFD8FFE0001...	
NULL	NULL	NULL	NULL	NULL	NULL

Table of Image Data Table(desktop application)



	Id	FilePath	SecretText	FilePassword	EmailAddress
	222	C:\Users\Mohsi...	s	w	Ali@gmail.com
	223	C:\Users\Mohsi...	dddddd	aaa	Ali@gmail.com
	224	C:\Users\Mohsi...	llk	q	Ali@gmail.com
	225	C:\Users\Mohsi...	kljlkjsdkljf	kdflsjdf	Ali@gmail.com
	226	C:\Users\Mohsi...	kjkj	qq	Ali@gmail.com
	227	C:\Users\Mohsi...	kjk	a	Ali@gmail.com
	228	C:\Users\Mohsi...	h	q	Ali@gmail.com
	229	C:\Users\Mohsi...	hdjsahdfkj	HDFSKLHSLA	Ali@gmail.com
	230	C:\Users\Mohsi...	h	q	Ali@gmail.com
	231	C:\Users\Mohsi...	kk	qq	Ali@gmail.com
	232	C:\Users\Mohsi...	s	s	Ali@gmail.com
	233	C:\Users\Mohsi...	s	s	imran@gmail.com
	234	C:\Users\Mohsi...	hfsh	qaa	imran@gmail.com
	235	C:\Users\Mohsi...	888	888	imran@gmail.com
	236	C:\Users\Mohsi...	888	9999	imran@gmail.com
	237	C:\Users\Mohsi...	dghkjahfdkl	dflksfjlksjd	Ali@gmail.com
	238	*NULL*	jjjjj	ggggg	imran@gmail.com
	239	*NULL*	fgfgf	dsdsds	imran@gmail.com
	240	C:\Users\Mohsi...	dsjhfjkashfkj	121312312	mran@gmail.com
*	*NULL*	*NULL*	*NULL*	*NULL*	*NULL*

Table of Video Data Table(desktop application)



Identifier	Providers	Created	Signed In	User UID ↑
kasif@gmail.com		11 Dec 2018	11 Dec 2018	4iVRk4Si0qhuOU8rOjJc9PAkY182
imran@gmail.com		8 Dec 2018	25 Feb 2019	A8NHe4Y5VxVCmsqKvdSFZz1ZPv...
qq@gmail.com		8 Dec 2018	8 Dec 2018	FVj7OYI7heTseH7tSNM0ID9Vpyl2
jaja@gmail.com		8 Dec 2018	8 Dec 2018	IJGMMmw4PaS4ylqCZ4dFFBUSU...
z@gmail.com		8 Dec 2018	8 Dec 2018	IKSC4pTH2iNzYXjeJzqTIL4iyds2
imrann@gmail.com		8 Dec 2018	8 Dec 2018	KdvWu0PXPPcmcFT0ULwU5GdaN...
iu@gmail.com		6 Jan 2019	6 Jan 2019	MkYfTlqMUIN9AzcXU8CHmeuknY...
imranali@gmail.com		8 Dec 2018	8 Dec 2018	N3zIOgY9BmgOR82Lqm83M2JiKj...
zzz@gmail.com		8 Dec 2018	8 Dec 2018	O9CZ6U8VYvR7TsMGKIb1chX7G0...
tindi@gmail.com		9 Dec 2018	9 Dec 2018	PV2OnvSJEUSvDWOpc7ipsXVsPiV2
iii@gmail.com		8 Dec 2018	8 Dec 2018	Rdr84NZ0zCMiqmDUMTBtzJSo7U...

Authentication table for android application

3.6 Component Design

In this section, we take a closer look at what each component does in a more systematic way. If

Software Design Document you gave a functional description in section 3.2, provide a summary of your algorithm for each function listed in 3.2 in procedural description language (PDL) or pseudo code. If you gave an OO description, summarize each object member function for all the objects listed in 3.2 in PDL or pseudo code. Describe any local data when necessary.

Chapter 4
Implementation and Testing

4.1 Code Modules

4.2 Database Connectivity

4.3 Overview of User Interface

4.3.1 Desktop application

4.3.1.1 Registration

- ✓ For use desktop application user must first registered by using email and password and recovery pin(useful when user forget its email password).
- ✓ While register user must use unique email means if the email already exists in database of application then user cannot login with that email. Application must show kind of message email is already existing.

4.3.1.2 Login

- ✓ After registration user must login with its specific email and password every time when application is reopened.
- ✓ In case user forget emails password, user can reset password using forget password option on login page.
- ✓ if user login successfully then user must enter in application main page otherwise error message will be displayed.

4.3.1.3 Image steganography of embed text

- ✓ After login user will moved on image steganography page.
- ✓ Here user can choose image file on which user wants to apply steganography by clicking browse button(section is restricted only jpg, bmp, png files can be selected).

- ✓ After choosing image user must enter some secret text in textbox given labeled as Text for hide. If user don't enter any text in this field user must get error message of this filed cannot be empty.
- ✓ After secret text entered user should be enter password to make secure image data which user wrote as secret text. Password is optional.
- ✓ After these things has been done. User must click on embed button then if process of image steganography is successfully done message will be display and vice versa.
- ✓ After this new image is created just user must save it on secondary memory(in hard drive) by using save button(new image saved in png format by default).
- ✓ Remember Whenever user click on embed button and process of steganography completed successfully information about image and also image itself must save in database which can be seen by user in more section in menu bar than in "view image information" section.

4.3.1.4 Image steganography of extract text

- ✓ When user use image steganography to extract text user must select the embedded image by clicking on browse button as user done before in embed process(section is restricted only bmp, png files can be selected).
- ✓ Then user must enter password (if required) and if user gives wrong password than application must show error message and vice versa.
- ✓ If process completed successfully than text will be display in text box shown on form.
- ✓ User can save this in the form of text file or copy this text.

4.3.1.5 Video steganography of embed text

- ✓ Here user can choose video file on which user wants to apply steganography by clicking browse button(section is restricted only avi. files can be selected, and video cannot be large).
- ✓ After choosing video user must enter some secret text in textbox given labeled as Text for hide. If user don't enter any text in this field user must get error message of this filed cannot be empty.
- ✓ After secret text entered user should be enter password to make secure video data which user wrote as secret text. Password is optional.
- ✓ After these things has been done. User must click on embed button then if process of video steganography is successfully done message will be display and vice versa.
- ✓ After this new video is created just user must save it on secondary memory(in hard drive) by using save button(new video saved in avi. format by default).
- ✓ Remember Whenever user click on embed button and process of steganography completed successfully information about video must save in database which can be seen by user in more section in menu bar than in "view video information" section.

4.3.1.6 Video steganography of extract text

- ✓ When user use video steganography to extract text user must select the embedded video by clicking on browse button as user done before in embed process(section is restricted only avi. files can be selected).
- ✓ Then user must enter password (if required) and if user gives wrong password than application must show error message and vice versa.
- ✓ If process completed successfully than text will be display in text box shown on form.
- ✓ User can save this in the form of text file or copy this text.

4.3.1.7 Database image record

- ✓ In is form user can easily see information about image in list view also.
- ✓ Also, user can see image itself by clicking id of image in picture box given on form.
- ✓ user can search image by id by enter id in textbox and click on search button.
- ✓ Also, user can copy all information about image by clicking on id and all fields along particular id data must copied in text fields shown on form where user can copy all information.
- ✓ Benefit of this is if user forget the password of image which user embedded before than user can easily find and get that password.
- ✓ Remember data about images only shown along or associative with logged in email.

4.3.1.8 Database Video record

- ✓ In is form user can easily see information about video in list view also.
- ✓ Also, user can copy all information about image by clicking on id and all fields along particular id data must copied in text fields shown on form where user can copy all information.
- ✓ Benefit of this is if user forget the password of image which user embedded before than user can easily find and get that password.
- ✓ Remember data about images only shown along or associative with logged in email.

4.3.2 Android application

4.3.2.1 Registration(optional)

- ✓ By opening application user can see login page where in the bottom user can see label button “don’t have account” user can click on it and create new account by register himself.
- ✓ Email and password only needed to register.
- ✓ Email must be unique.
- ✓ That is only worked in internet access not offline.

4.3.2.2 Login(optional)

- ✓ After register user can easily login using that registered email and password.
- ✓ That is only worked in internet access not offline.

4.3.2.3 Image Steganography to embed text

- ✓ After login or skipped login process user will moved on home page.

- ✓ There user can see two options in form of two buttons 1 is Embed Text 2 is Extract Text.
- ✓ On click on Embed Text there will be 3 tabs display on screen of device
- ✓ First tab used for selecting image from gallery selected image will be displayed on screen.
- ✓ Second tab used for entering text which user want to embed in image.
- ✓ Third tab is used for entering password(optional), also embed text button is present on that tab screen.
- ✓ After clicking on Embed Text button if process of image steganography embed text is not completed successfully than user must gets error message and vice versa.
- ✓ After this user must have to save this new created image by using save image button this image will be saved on device local memory and can be seen in gallery and directory also shown after clicking save image button.

4.3.2.4 Image Steganography to extract text

- ✓ After clicking on extract text button user will be moved on extract text page here user can see two tabs.
- ✓ First is used to select image from gallery make sure that image should be embedded image otherwise at the end user gets error message.
- ✓ Second tab is used to see extracted text if present in image.
- ✓ By clicking on Extract Text if text is present in image text will be display on tab textbox. Here user can copy this text easily.

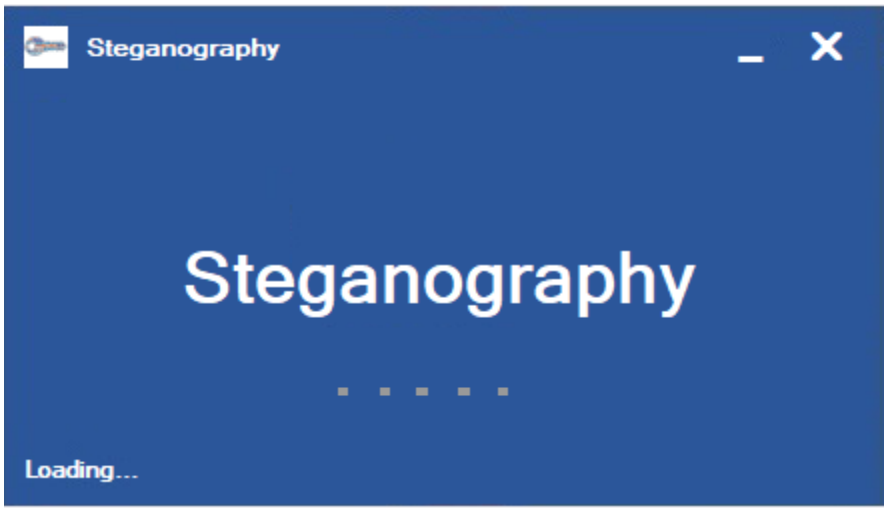
4.3.2.5 Share app

- ✓ User can share this app using Bluetooth etc. by clicking on Share button in Navigation drawer.

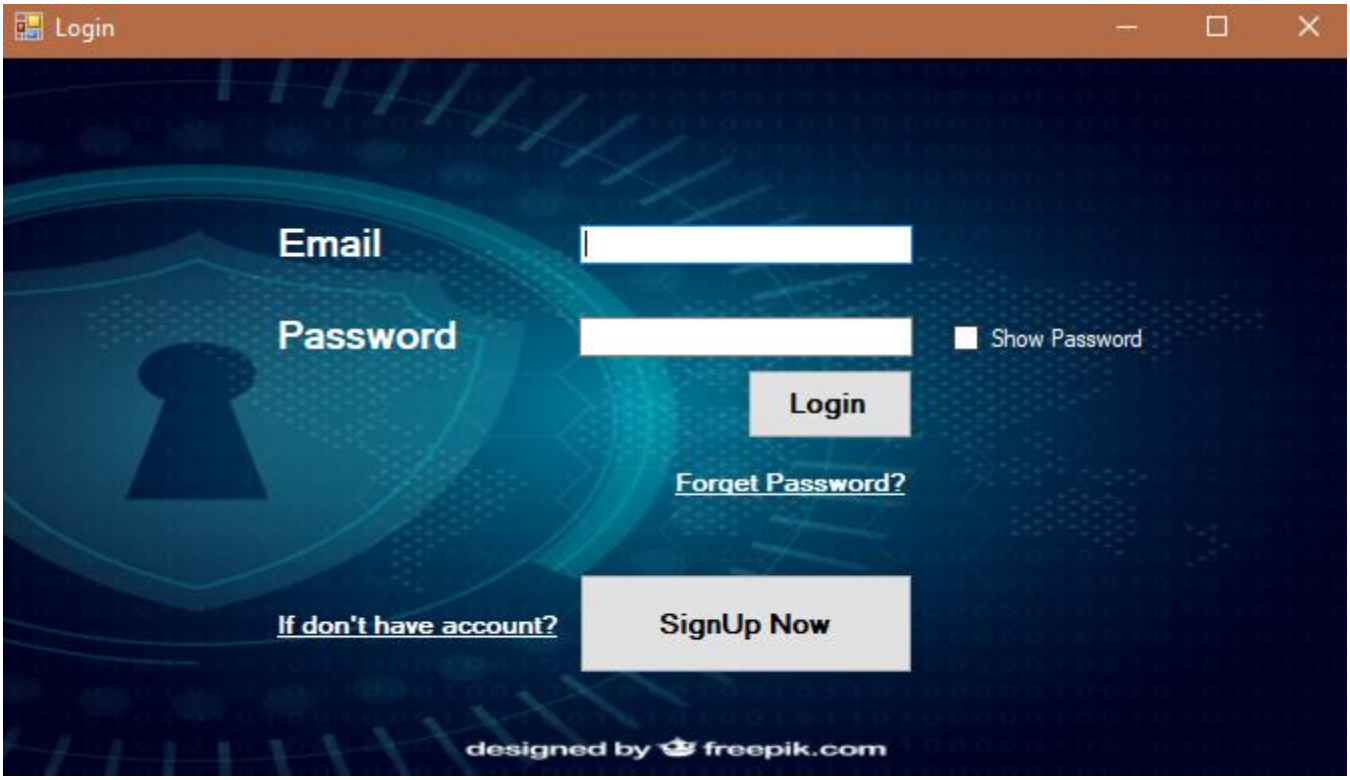
4.4 Screen Images

4.4.1 Desktop Application Screen Images

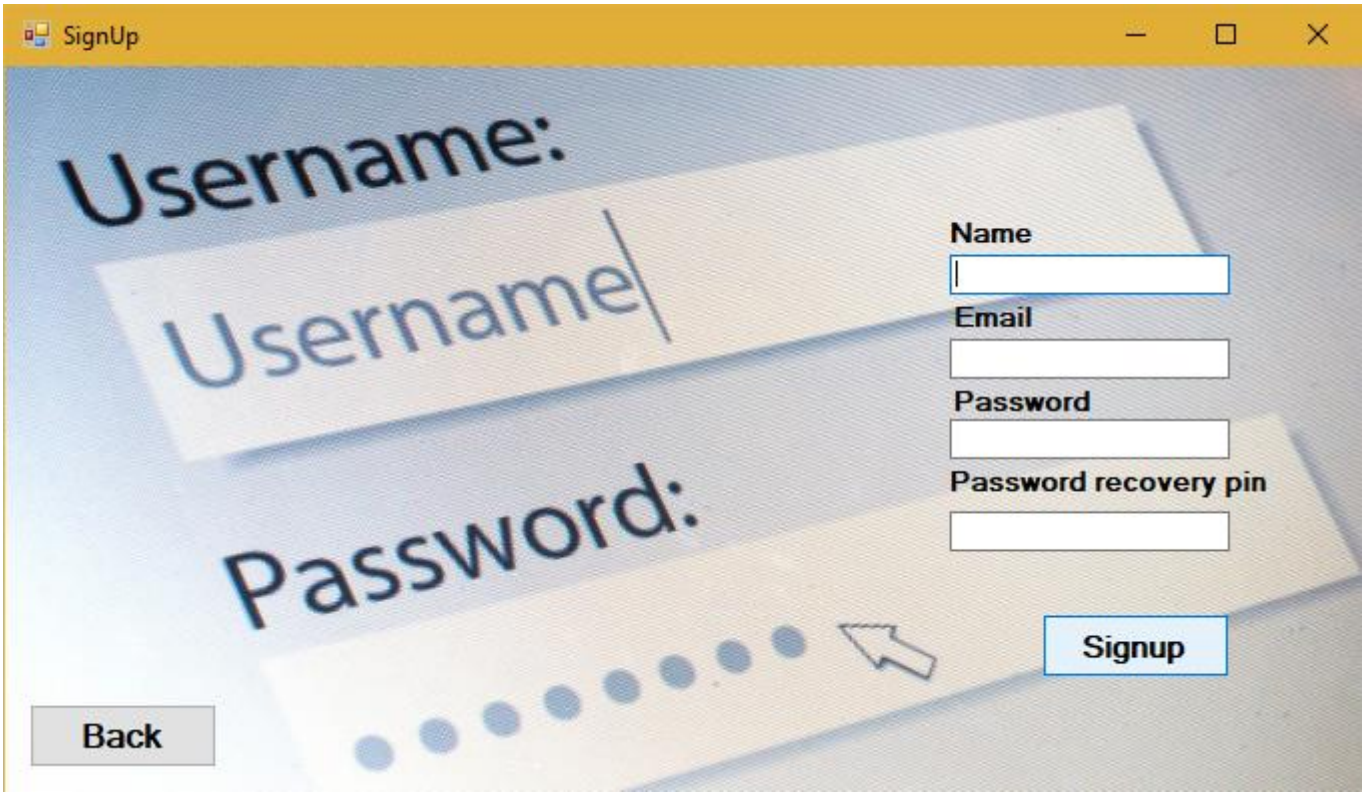
4.4.1.1 Splash(desktop application)



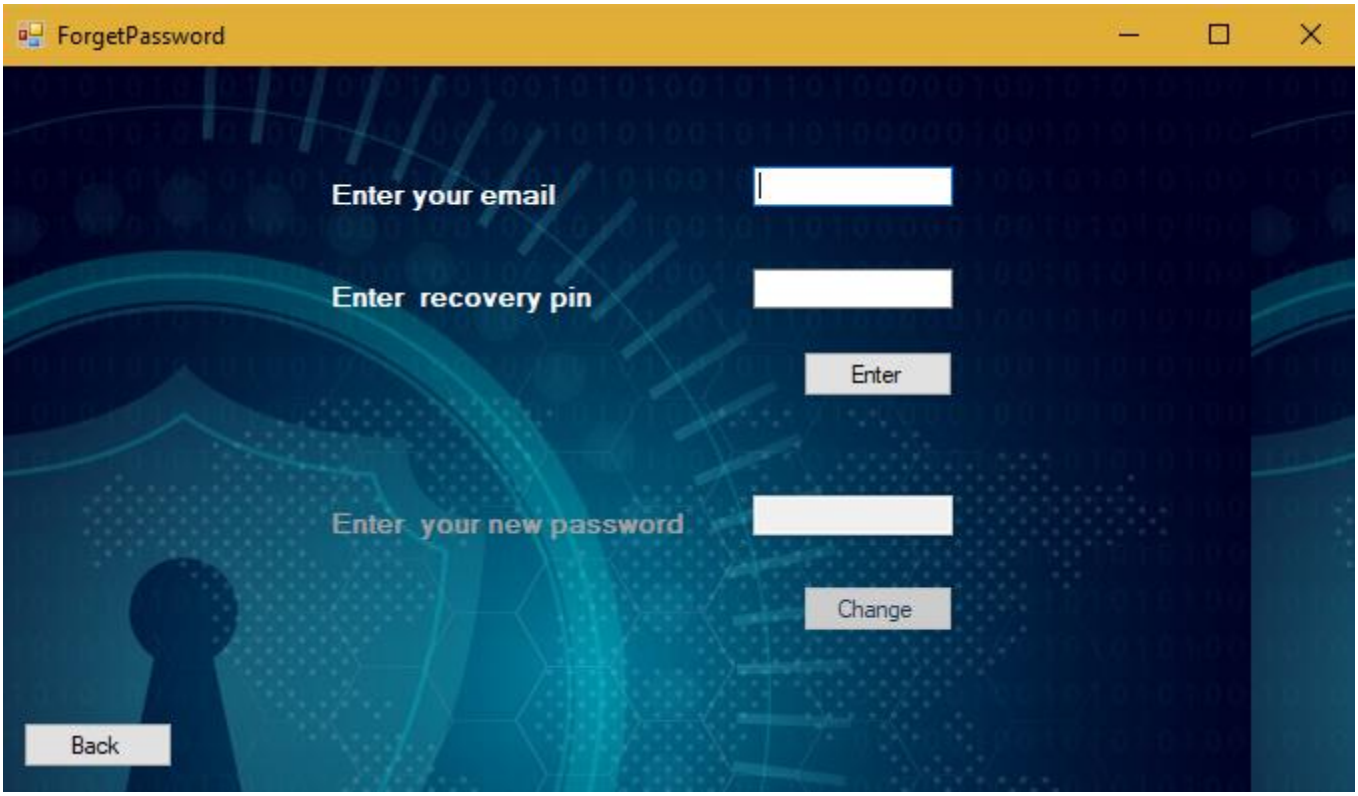
4.4.1.2 Login(desktop application)



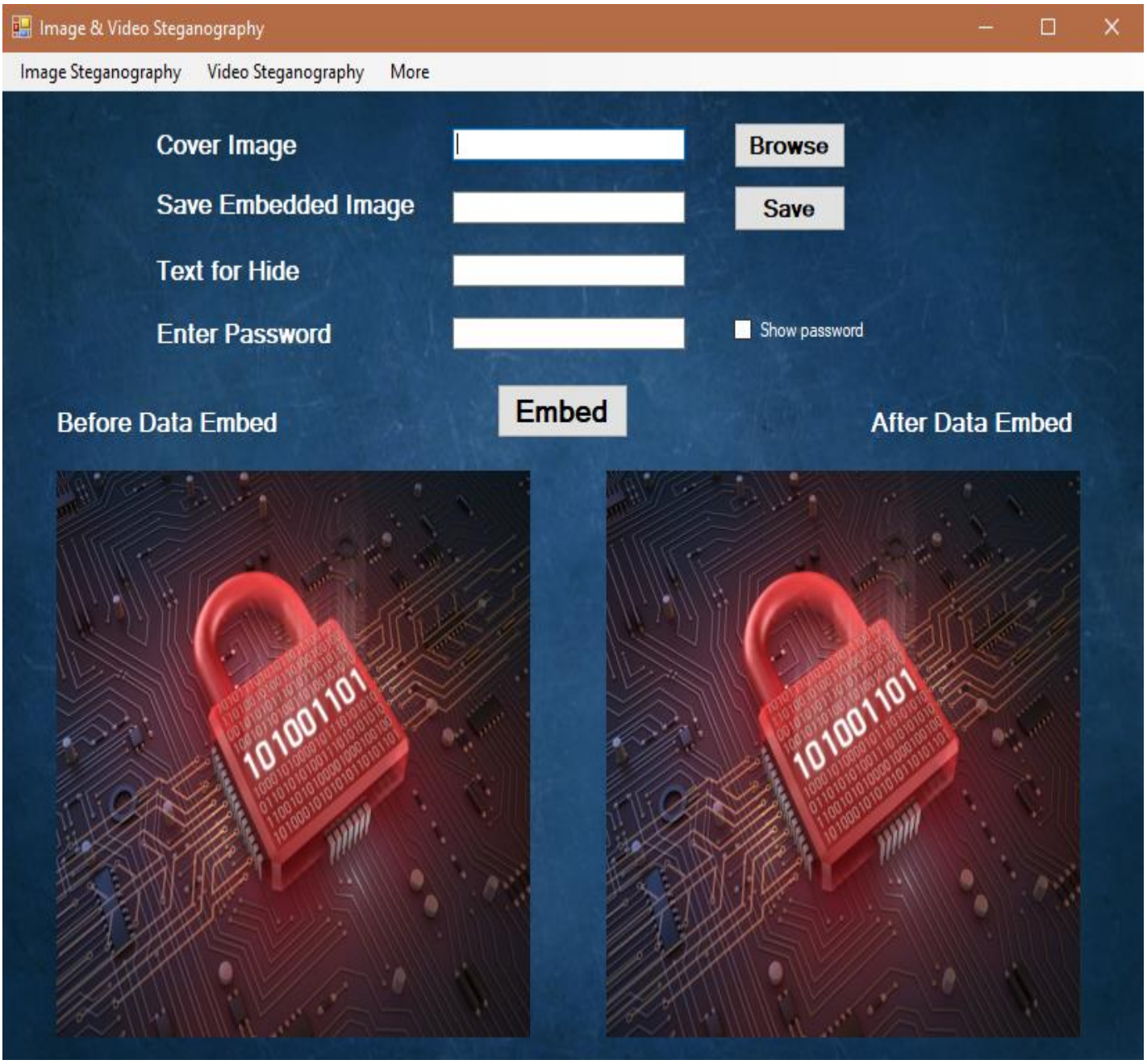
4.4.1.3 SignUp(desktop application)



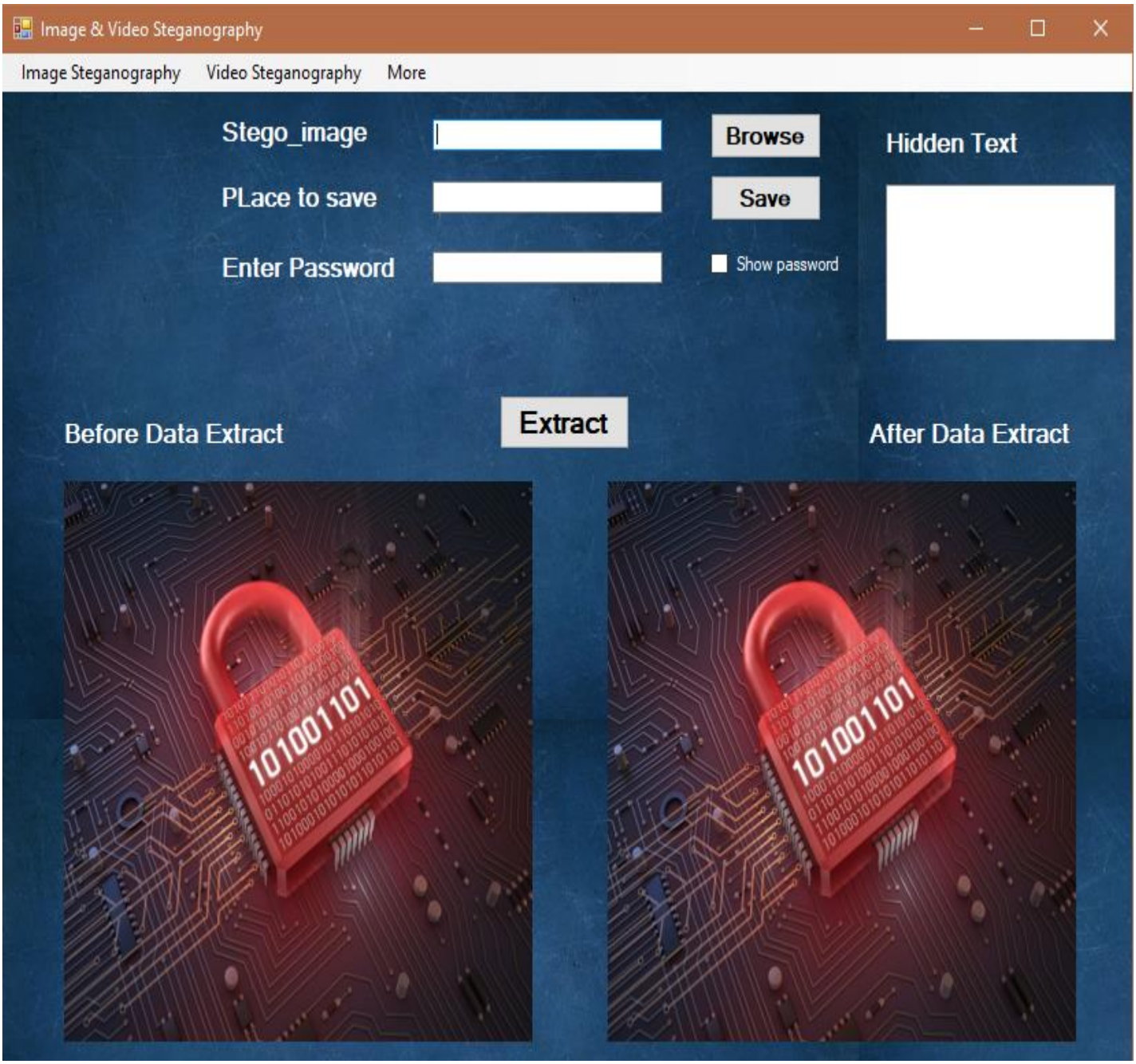
4.4.1.4 ForgetPassword(desktop application)



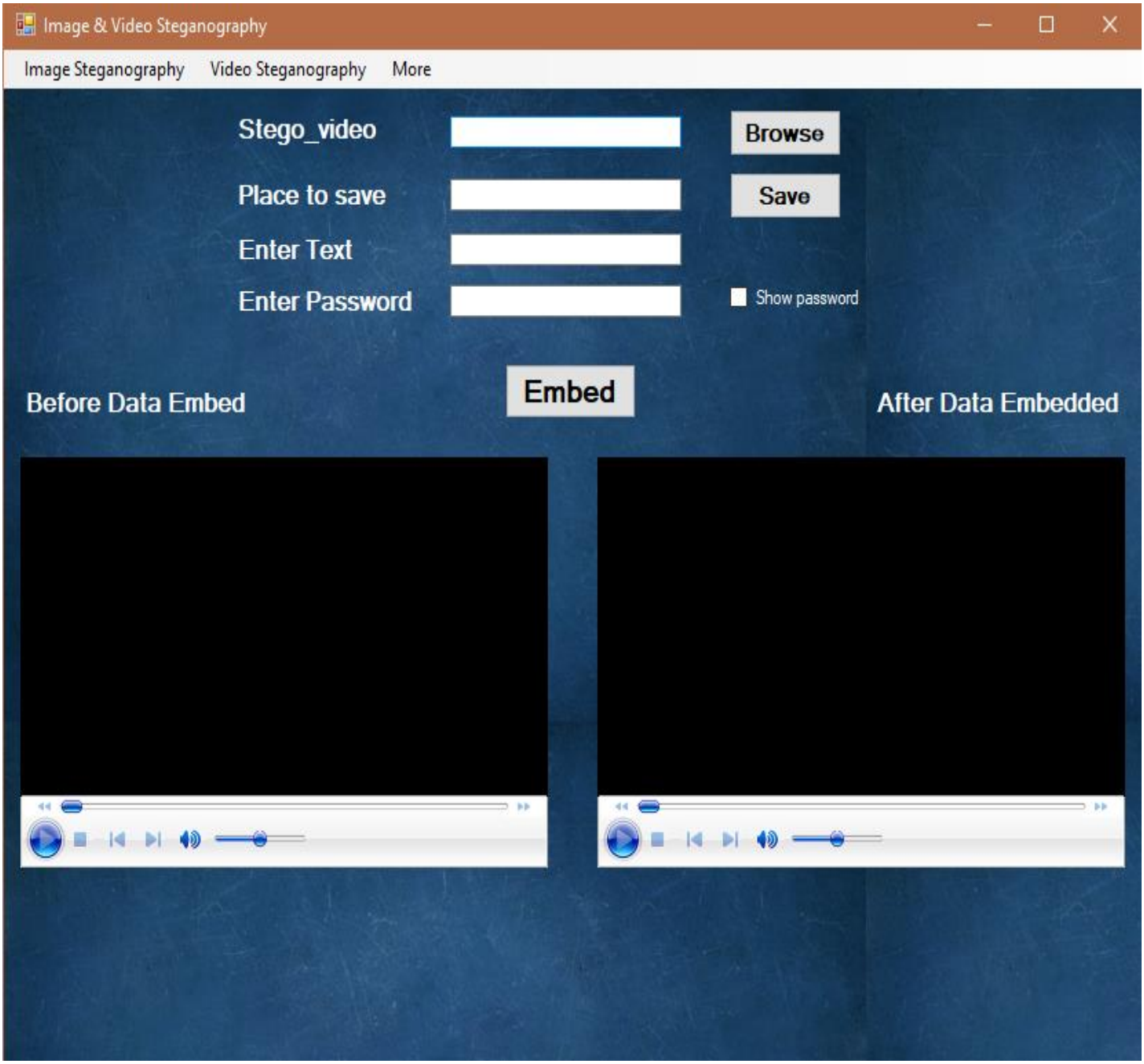
4.4.1.5 Image Steganography to embed text (desktop application)



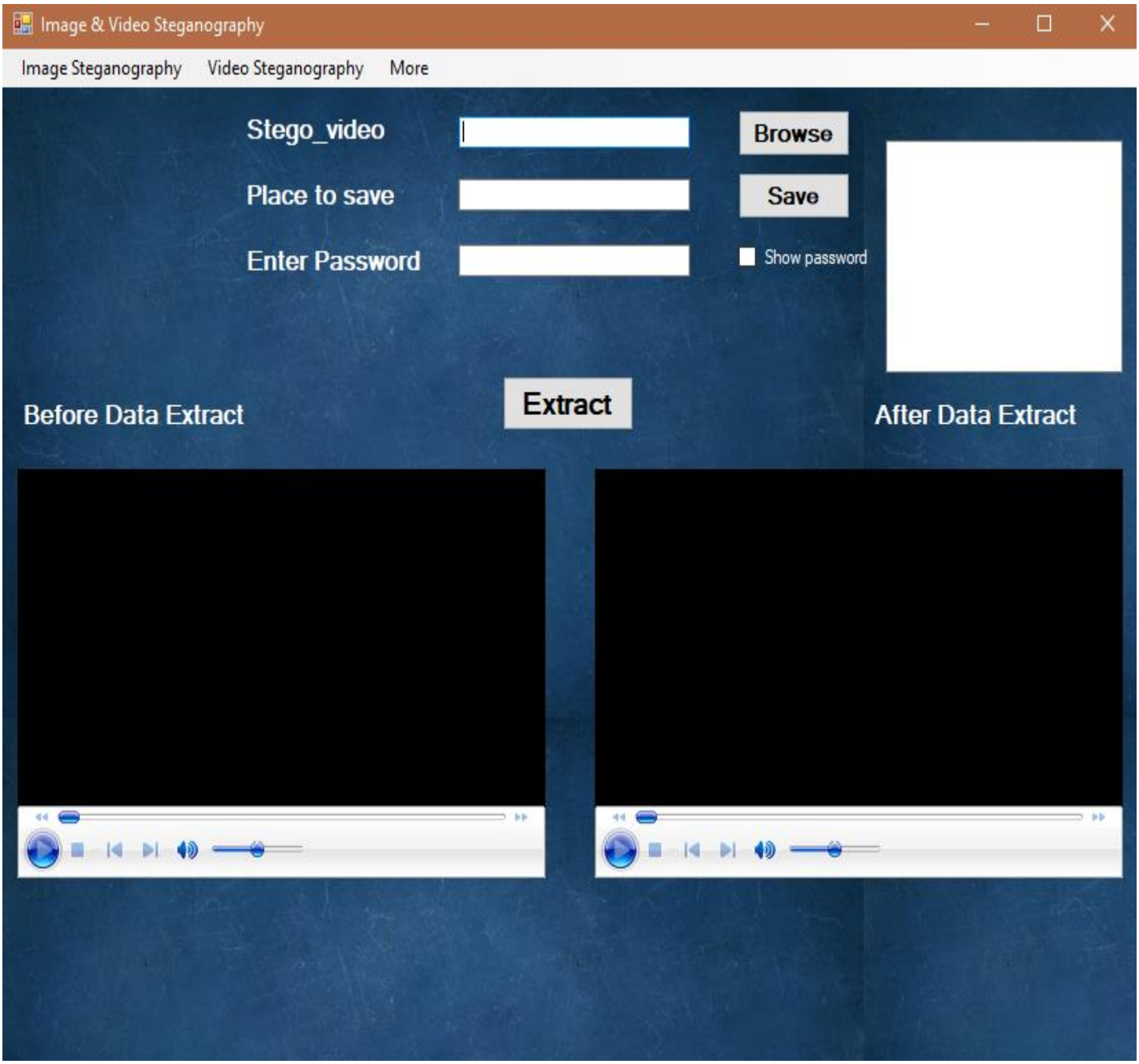
4.4.1.6 Image Steganography to extract text (desktop application)



4.4.1.7 Video Steganography to embed text (desktop application)

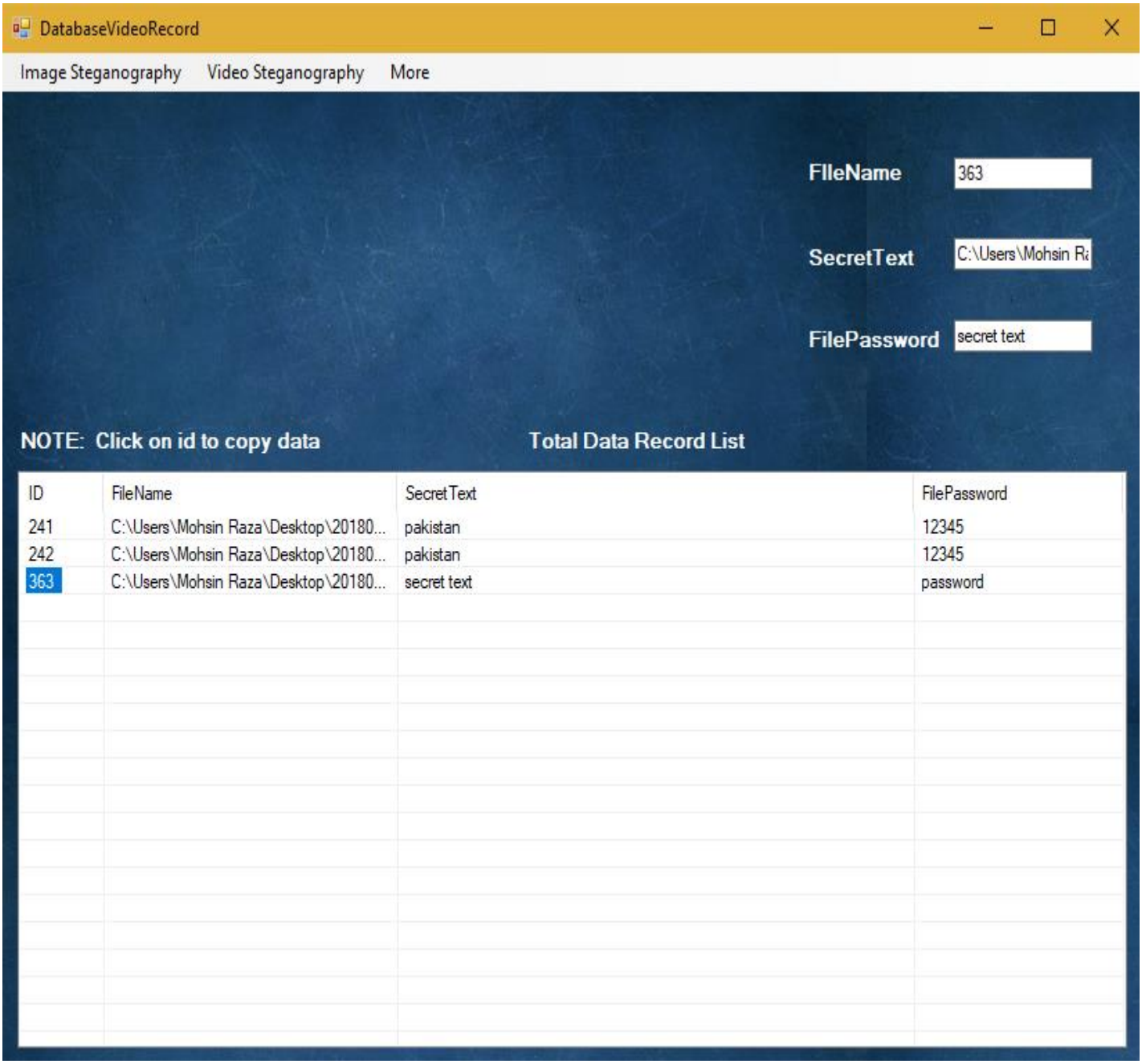


4.4.1.8 Video Steganography to extract text (desktop application)



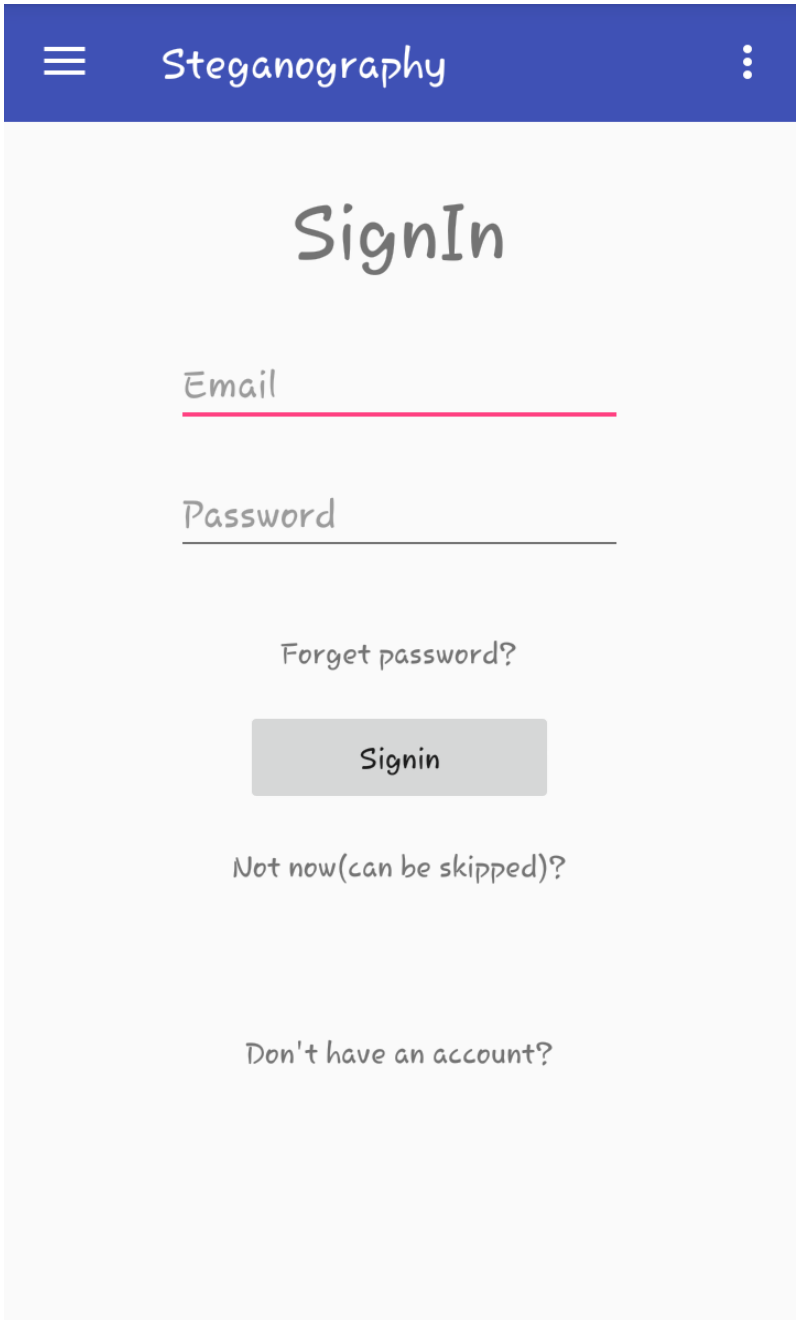
4.4.1.9 Image database record (desktop application)

4.4.1.10 Video database record (desktop application)

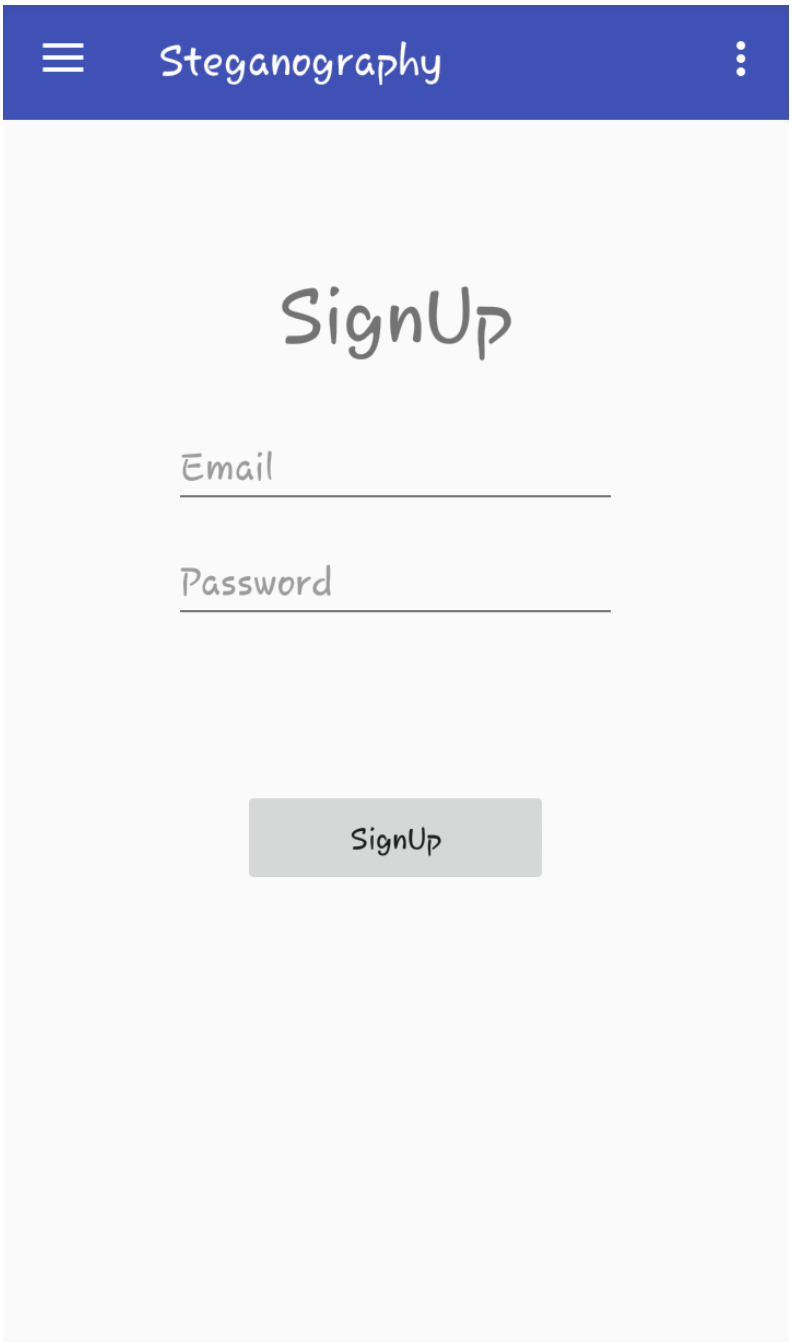


4.4.2 Android Application Screen Images

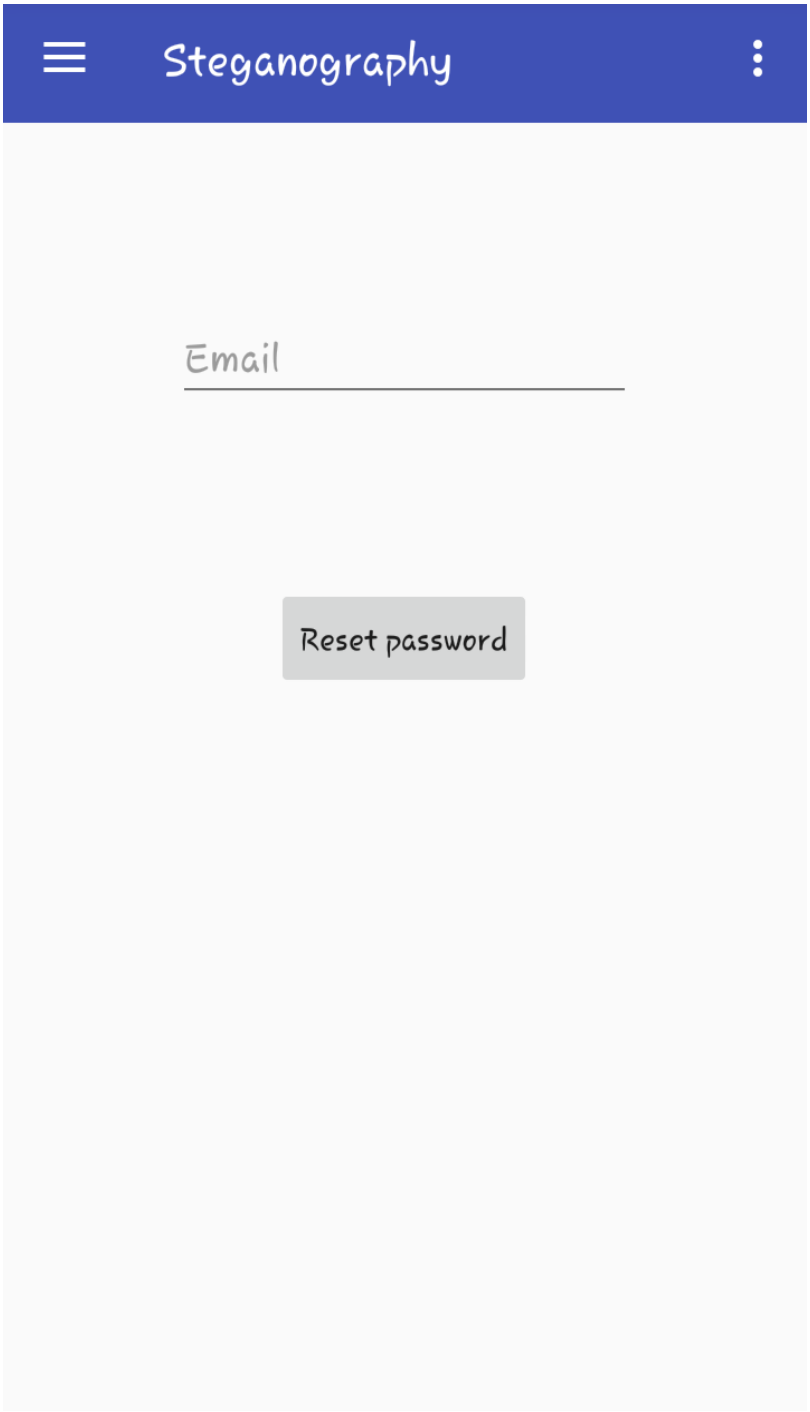
4.4.2.1 SignIn


Steganography
SignIn
Email
Password
Forget password?
Signin
Not now(can be skipped)?
Don't have an account?

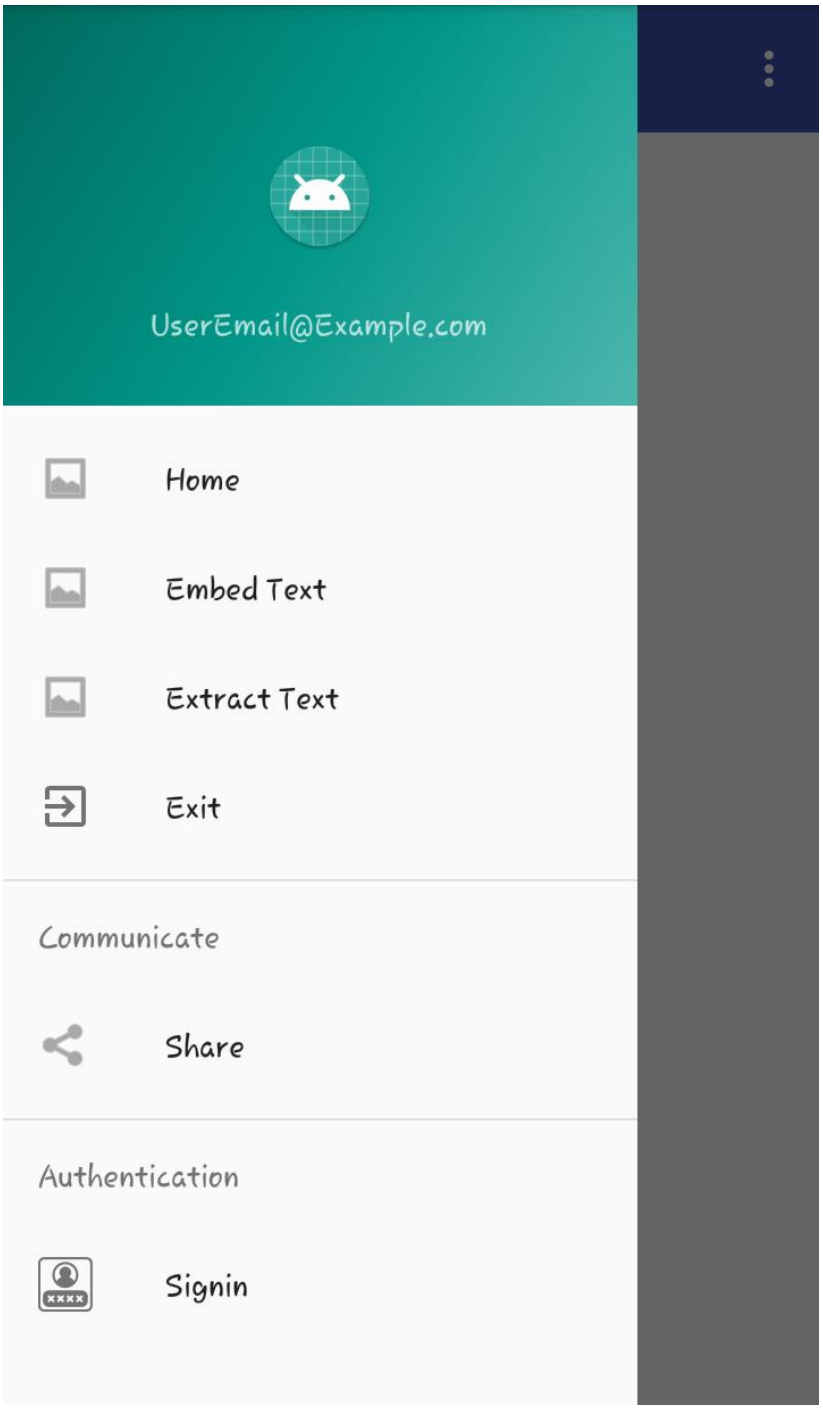
4.4.2.2 Signup



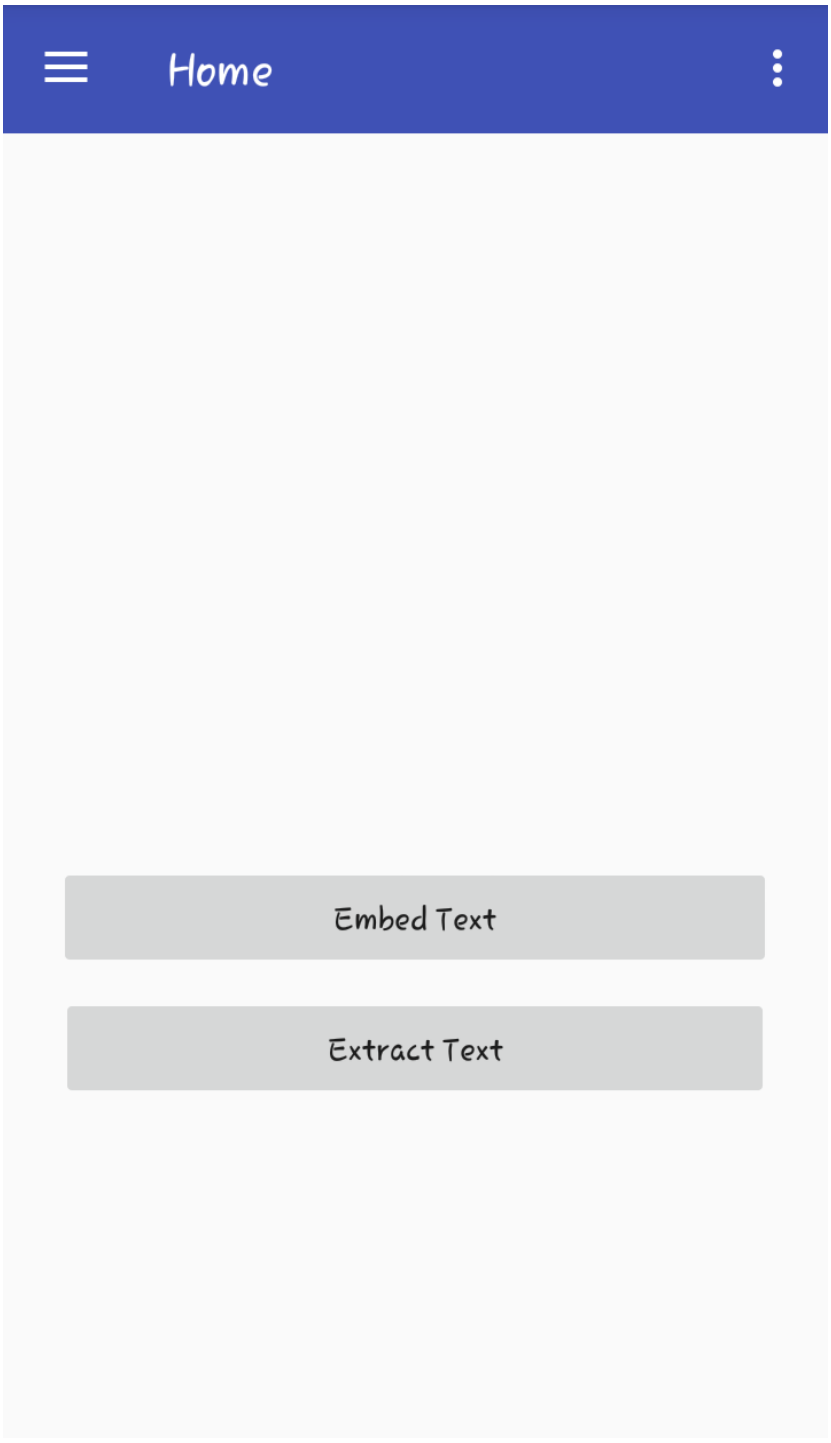
4.4.2.3 Reset Password



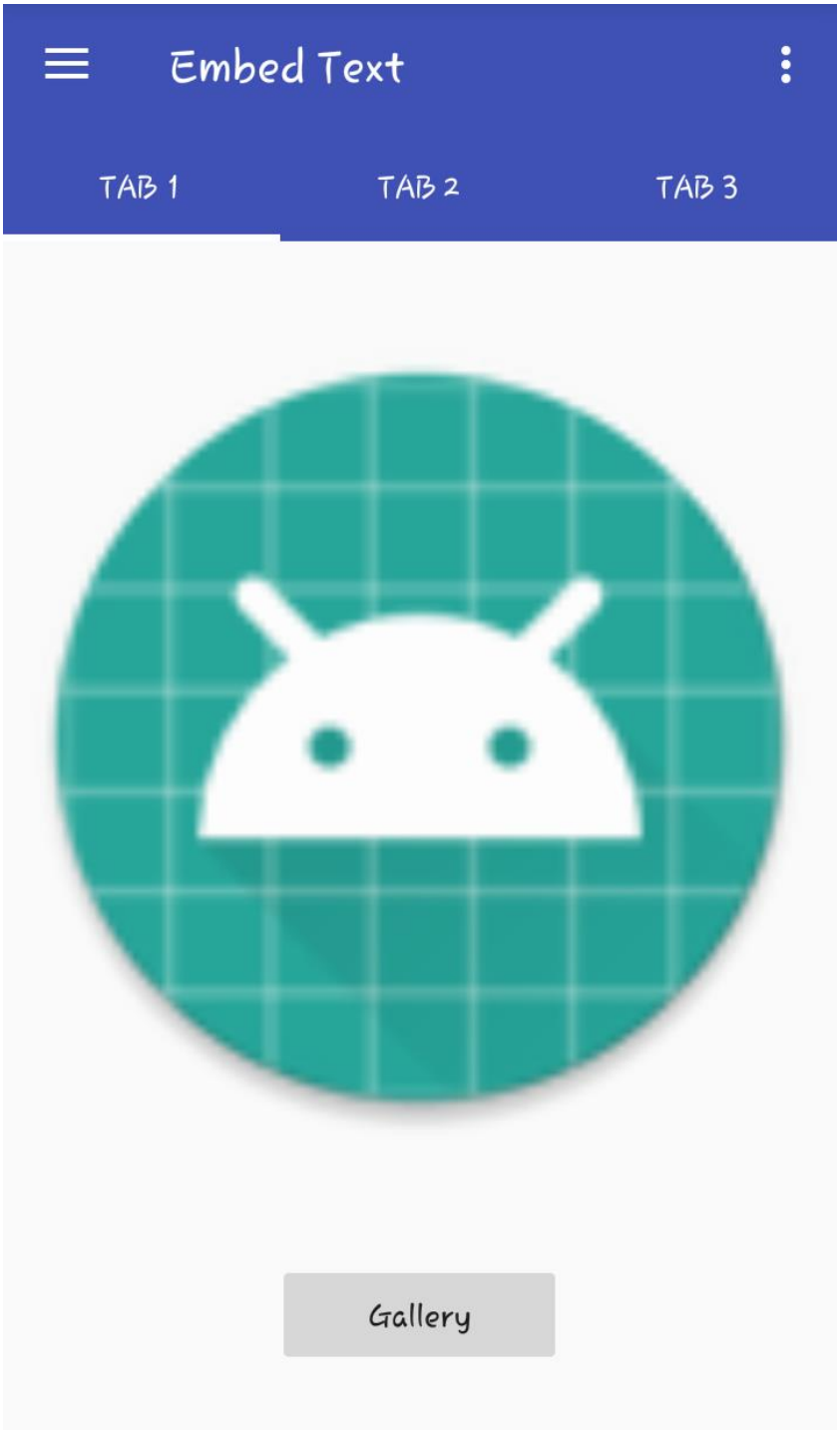
4.4.2.4 Navigation bar


UserEmail@Example.com
Home
Embed Text
Extract Text
Exit
Communicate
Share
Authentication
Signin

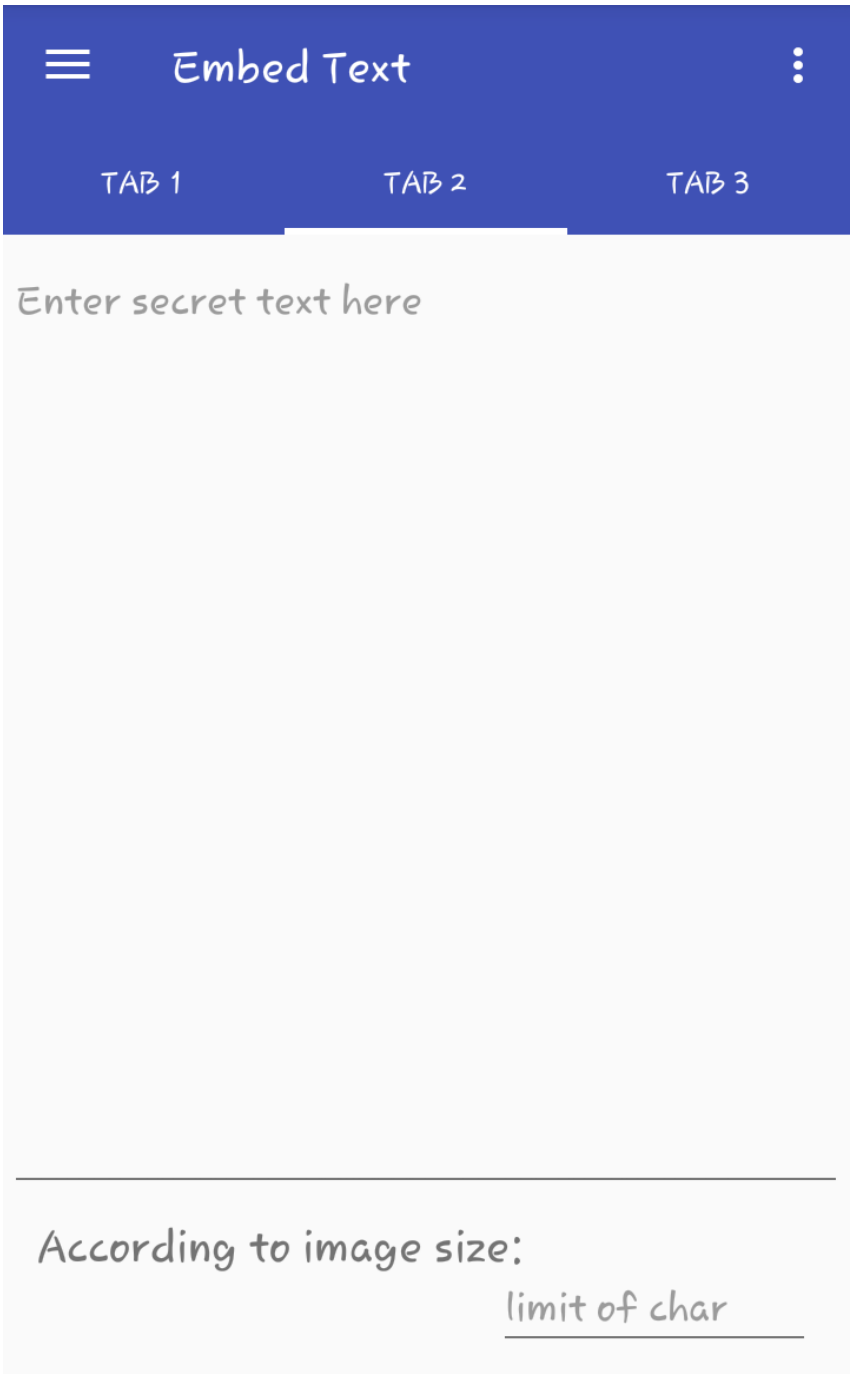
4.4.2.5 Home



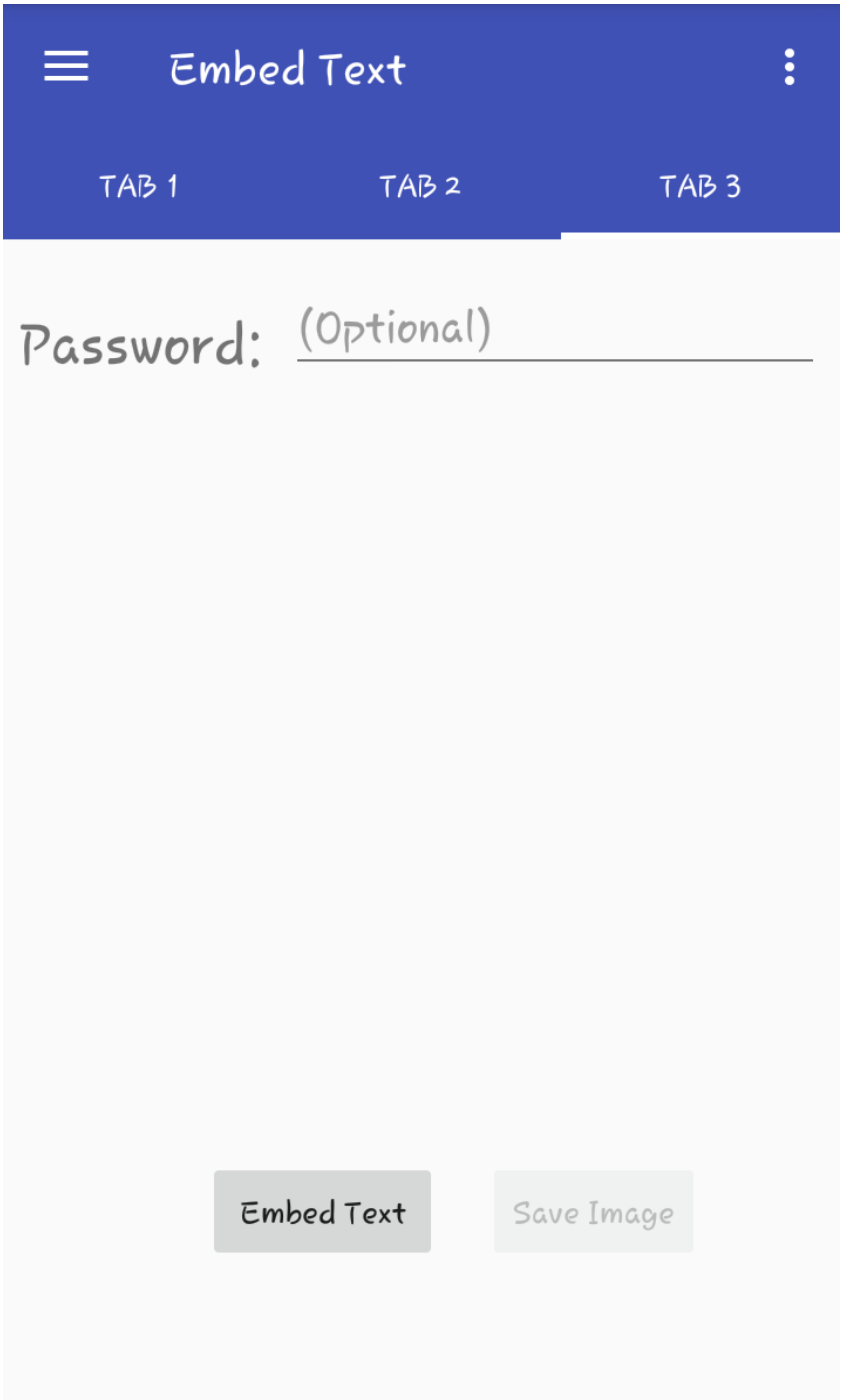
4.4.2.6 Embed Text tab1



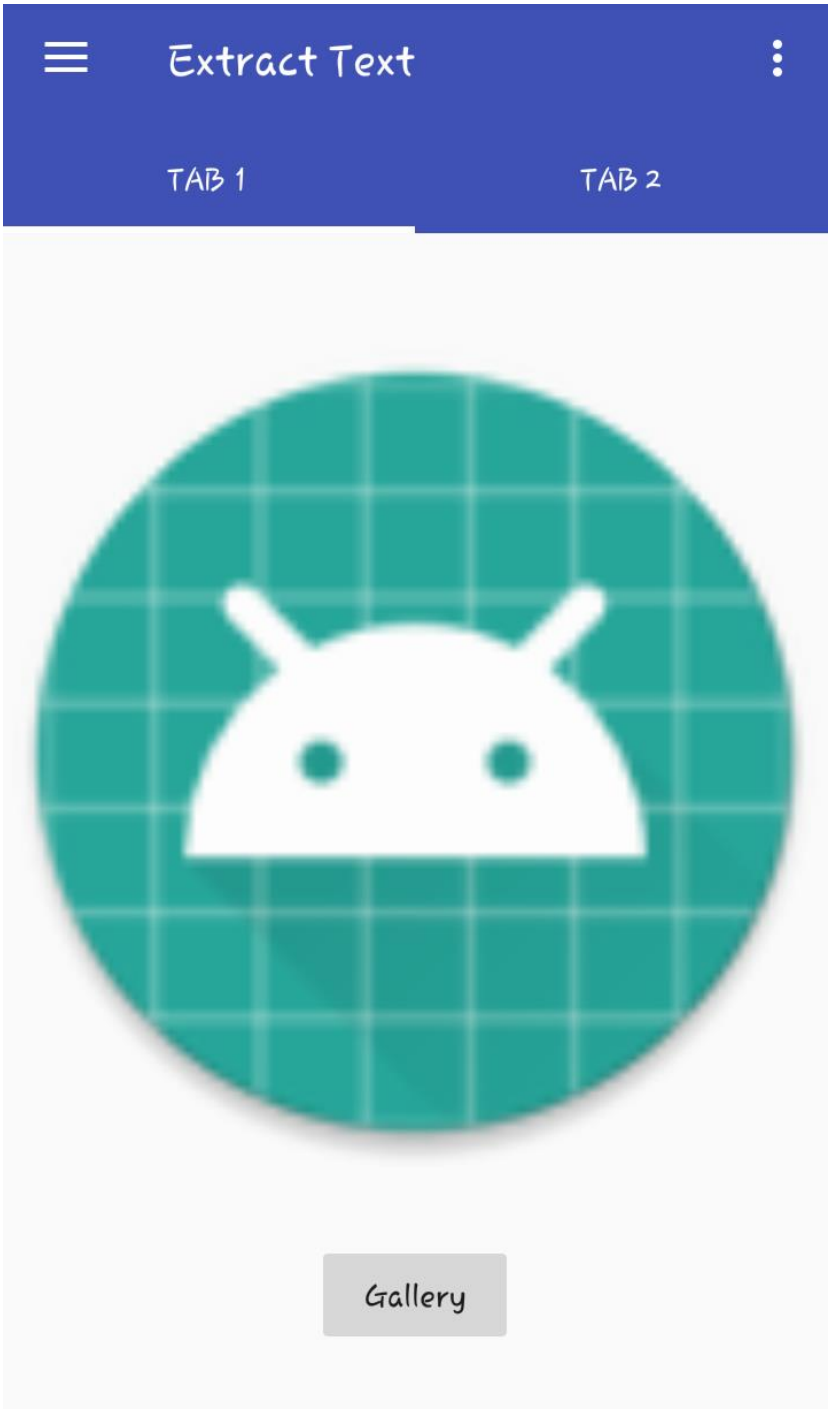
4.4.2.7 Embed Text tab2



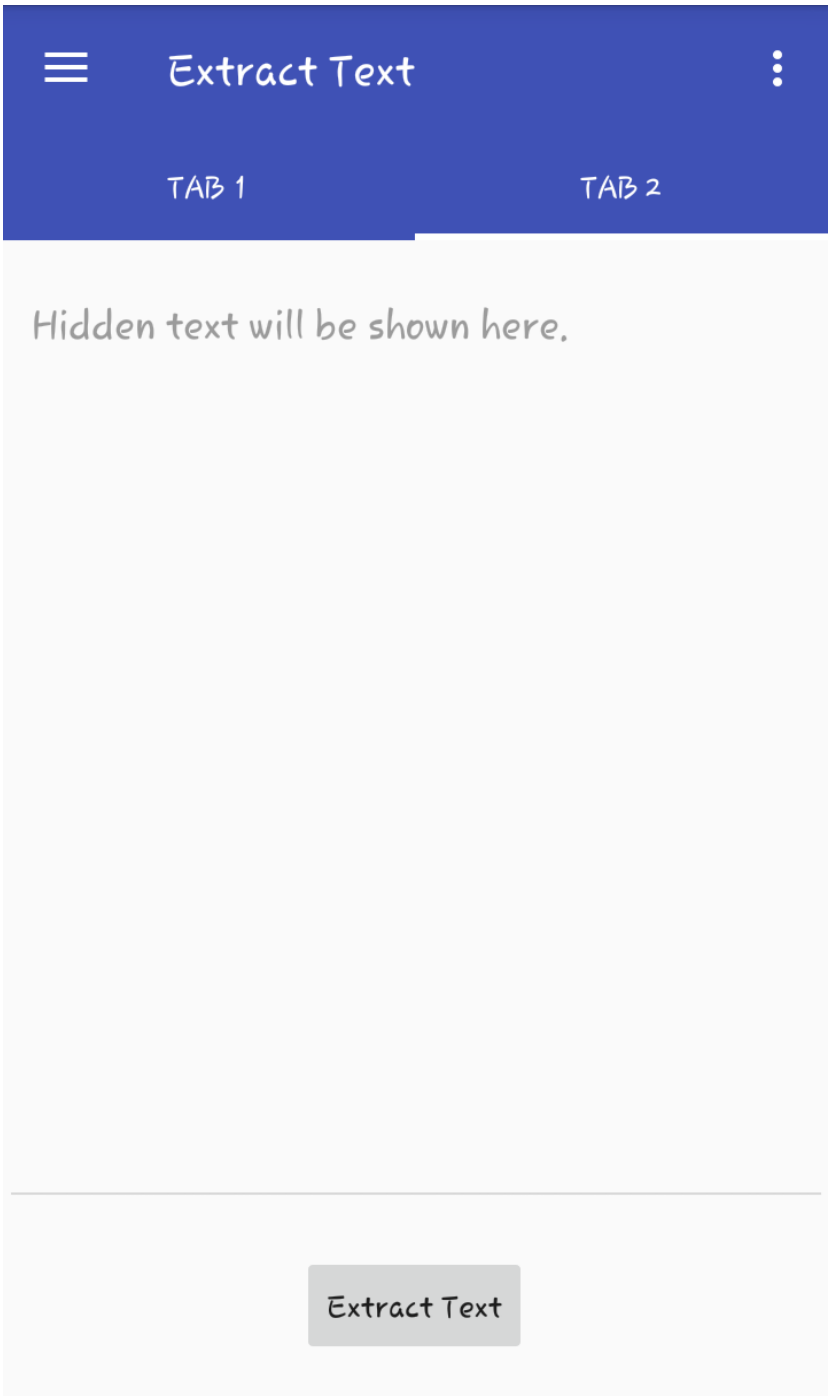
4.4.2.8 Embed Text tab3



4.4.2.9 Extract Text tab1



4.4.2.10 Extract Text tab2


Extract Text
TAB 1
TAB 2
Hidden text will be shown here.
Extract Text

4.5 Screen Objects and Actions

4.5.1 Desktop Application

4.5.1.1 Registration form

- ✓ **Four fields:** On Registration form user can see 4 text fields (Name, Email, Password, password recovery pin) these all used for getting input from user.
- ✓ **Signup button:** One signup button to signup user in database.
- ✓ **Back Button:** used to go back on login form.

4.5.1.2 Login form

- ✓ **2 Text Fields:** one for email other for password
- ✓ **Checkbox:** used to show password * into original form.
- ✓ **Two Label buttons:** one forgets password used to direct to forget password form. Second don't have account just used for information.
- ✓ **Signup button:** used to direct user to signup form.
- ✓ **Login button:** used to login user if successful than direct user to Image steganography form.

4.5.1.3 Image steganography of embed text

- ✓ **4 text fields:** used to take inputs from user 1 having image directory path 2 having saved image path 3 enter secret text 4 enter password.
- ✓ **3 buttons:** browse button is used to select image from secondary memory. Save button used to save image after steganography applied. Lastly embed button to take actual embed action and save image information in database.
- ✓ **Checkbox:** used to show password.

4.5.1.4 Image steganography of extract text

- ✓ **4 text fields:** used to take inputs from user 1 having image directory path 2 having saved text file path 3 used to enter password 4 used to display extracted text in it.
- ✓ **3 buttons:** browse used to select image from secondary memory. Save button is used to save extracted text. Extract button use to done main work of extracting text from image.
- ✓ **Checkbox:** used to show password.

4.5.1.5 Video steganography of embed text

- ✓ **4 text fields:** used to take inputs from user 1 having video directory path 2 having saved video path 3 enter secret text 4 enter password.
- ✓ **3 buttons:** browse button is used to select video from secondary memory. Save button used to save video after steganography applied. Lastly embed button to take actual embed action and save video information in database.
- ✓ **Checkbox:** used to show password.

4.5.1.6 Video steganography of extract text

- ✓ **4 text fields:** used to take inputs from user 1 having image directory path 2 having saved text file path 3 used to enter password 4 used to display extracted text in it.
- ✓ **3 buttons:** browse used to select video from secondary memory. Save button is used to save extracted text. Extract button use to done main work of extracting text from video.
- ✓ **Checkbox:** used to show password.

4.5.1.7 Database image record

- ✓ **List view:** having id, secret text, password, image path.
- ✓ **Picture box:** used to display image by clicking on id.

4.5.1.8 Database Video record

- ✓ **List view:** having id, secret text, password, video path.

4.5.2 Android Application

4.5.2.1 Registration(optional operate able only with internet)

- ✓ **2 text fields:** used to get input from user email and password.
- ✓ **1 button :** used to signup user and data stored in cloud Database.

4.5.2.2 Login(optional operate able only with internet)

- ✓ **2 text fields:** email and password used to get input from user.
- ✓ **3 label buttons:** forget password used to direct user to forget password process. Not now label used to skip login until user wants to login. Lastly don't have account use to direct user to signup page.
- ✓ **1 button:** used to Signing in user.

4.5.2.3 Image Steganography to embed text

- ✓ **Tab1:** having one button to select image from gallery and display on picture box.
- ✓ **Tab2:** having two text boxes one is used to input secret text second is used to display remaining character limit.
- ✓ **Tab3:** having one text box used to input password(optional) second Embed text button used to apply steganography third save image button use to save image in local memory.

4.5.2.4 Image Steganography to extract text

- ✓ **Tab1:** having one button to select image from gallery and display on picture box.
- ✓ **Tab2:** having one text box and one button. Text box used to display extracted text from image. Extracted text button used to apply steganography to extract image.

4.5.2.5 Share app

- ✓ **Navigation Drawer**: User can share this app using Bluetooth etc. by clicking on Share button in Navigation drawer.

4.6 Test Cases