ID Miniproject - Steganografi ID

ITC B370
Jeppe Øland, Laurids Thormann, Sebastian Damsgaard, Jonas Alsen

May 23, 2016

Contents

Jeppe Øland, Sebastian Damsgaard
Laurids Thormann, Jonas Alsen

Chapter 1

Intro

For this assignment we are going to develop an Android application, that can encode hidden text in pictures using steganography. The application will be made, so that the average citizen are able to use it. It does however require that the person has an Android smartphone. The purpose of this app, is to protect your privacy. For the user it does not require any sort of knowledge, on how steganography works. The app is going to be a chat client, that can be used as an everyday tool.

A group that could be interested in using the application, are people living in repressive regimes. This sort of hidden communication can be necessary, for surviving in those parts of the world. Since it is difficult to get in contact with these people, the target population will be the average citizen. This is so that we have a chance to test the application on someone who actually have an interest. (Because of all this, it is very important that it is easy to navigate in the app.)

Chapter 2

User needs in context study

In 2015, 77% of citizens in Denmark, owned a smart phone[1]. When that number is compared to the number of people living in Denmark, who have an account on Facebook, which is 72%, it's easy to conclude, that tons of information is being shared digitally every day[2]. In 2015 Amnesty International made global measure on the topic of surveillance.
It showed that 71% is against the American surveillance[3]. Based on this information, the need for a way to share information digitally, without any government gathering information about either the sender nor the receiver, has appeared. To fulfill this need, ITCB370 attempts to create an application for a smart phone that, with the help of steganography, can hide who is sharing information with each other, digitally.

When it comes to specific user needs, the statistical data on which the user needs are based on, stems from a relatively broad measure. The potential number of people that could be interested in using this product exceeds the millions in Denmark alone. This means that the application has to be user friendly, meaning that the technical skill level should become irrelevant, to the point where the user only has to be able to operate basic applications on a smart phone.
Therefore the concept of the application will build on already existing user interface layouts, such as the Android chat client, and the camera function, which makes the user able to easy recognize and use the application.

With this in mind a prototype of our conceptual model is being made.

Chapter 3

Conceptual model of the prototype

Although the application made in this project is highly technical, the goal is to hide the complexity and make the application accessible for non-technical people. The concept will be based on known metaphors and designs from similar applications. This way, we and our users can make use of existing knowledge both in designing the application and when using it.

The overall metaphor in this project is "Writing with invisible ink on paper". It is the act of writing a message on top of another, in a non-obvious way, in order to hide it. Only those who are aware of the invisible ink will think of heating up the paper in order to reveal the hidden message. This process is referred to as steganography.
The goal is to make a similar process possible on a smartphone. However, the process of steganography on a smartphone is not simple. To make the application usable for non-technical people it has been chosen to abstract away this metaphor, with a more classical inbox/outbox metaphor. This allows us, as developers, to hide the underlying "engine room" and allow our users to get things done.
The following section will describe the metaphors used in the application's user interface. Each metaphor describes a component of the conceptual model.

3.0.1 Inbox

The main concept and analogy in this application will be based around an Inbox. The inbox will contain a list of existing conversations. The conversations will be presented in a list. Each item in the list will present the participants in the conversation, as well as the timestamp for the latest message. The conversations will be sorted by date. Whenever a conversation receives a new message it will be bumped to the top of the list. This ensures that the conversations containing the latest messages will always be at the top of the inbox.

Figure 3.1: The classic snail mail inbox. Courtesy of Brian Griesbaum on sxc.hu

3.0.2 Conversations

A conversation contains all previous messages sent between a user and contact. The messages in the conversation will be presented in a threaded manner. The messages will be listed from top to bottom where the latest messages will be at the bottom of the screen so that the user can scroll towards the top to see older messages. Each message will present the name of the sender as well as the time and date it was sent/recieved.
Due to the nature of the underlying steganography, a conversation between two people must be started with mutual interest. That means that both parties in the conversation must, independently, start a new conversation with the opposing side, at the same time.

3.0.3 Messages

A message in this application is a short text, about the size of an SMS. As stated above a text is always contained within a conversation.
Sending a text message is a three step process. Messages are never sent directly to the receiver due to security concerns. Before transmission, a message is encoded in a user selected image, and then published as a status update on a social network. The process is as follows:

1. Write the message.
2. Select an image, in which the message will be hidden.
3. Publish the image containing the message on a social network.

Received messages appear in the corresponding conversations. The user do not have to take any actions in order to read them.

3.0.4 Addressbook

When a new conversation is started, a user can select a contact from the address book, which contains the necessary contact information for favorite contacts. New contacts can be added by searching the social network, which the application is connected to. In addition to contact information, a contact will also have an optional associated name (ie nickname) associated with it.

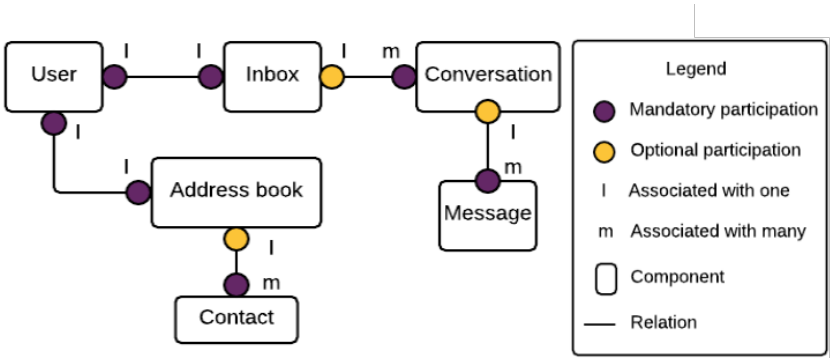


Figure 3.2: Relation between objects in the conceptual model.

To illustrate how the components mentioned above work together, the following storyboard (figure 3.3) has been drawn. It illustrates the core use case of one user sending a message to another.

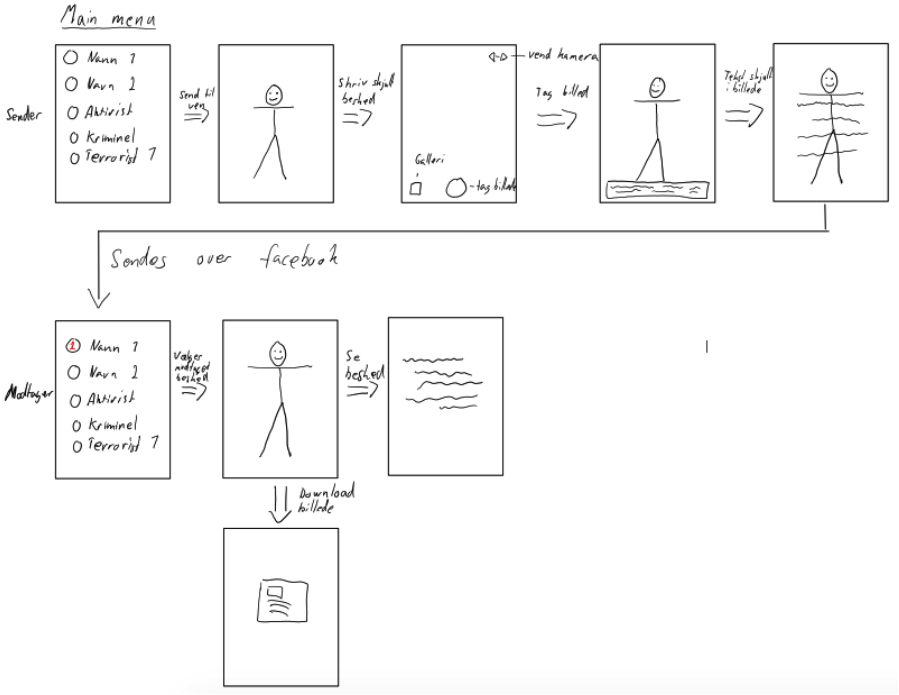


Figure 3.3: Rudimentary flow chart of the usage.

A new conversation is started by selecting a contact. When the conversation is opened, the sender enters the text message. Then an image is selected from the camera or gallery, and the text is hidden inside the image. The image is uploaded to a social network where the receiver's phone detects the new message. The image is downloaded and the message is decoded. Finally the message is presented in the receivers conversation window.

Chapter 4

Physical design

In the conceptual model, there is a couple of objects, that interacts with each other. The objects can interact different with each other. For example if the user wants to sent a message, then the user has to go through the objects; Open conversation, enter text, select image - and so on. It is very important that these objects come in a natural order. By coming in a natural order, it is very user friendly. Since this app is on an Android smartphone, some of the objects are inspired by already existing functions on Android. This means that "natural order" are for example when choosing a contact to start/continuing a conversation, are the same method as writing a text and writing a text in the steganography app. By Using some of Androids functions and orders in the app, the user is able to navigate naturally around in the app.

So the idea is to use already existing functions, so that the user is familiar with the order. However with some of the functions, we have to make changes because they does not exist on Android.

For example when the user needs to choose a picture from the gallery or the camera(see figure 4.1).

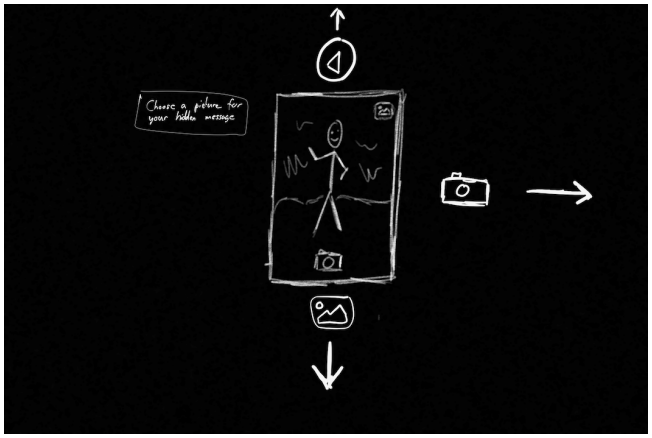


Figure 4.1: Function: choose picture from camera or gallery

For the user to be at this step (figure 4.1) in the app, require that the user, has already entered a text. Because the text needs to be hidden inside the picture, these two must be entered/chosen separately. If we look at an already existing function; MMS(multi media message), there is only so little that we can copy/use. In an MMS the user can input a picture before or after the text is written. With an MMS the text is posted next to the picture. In the app, the text will be hidden inside the picture, which means that we can not do it in the same way as writing an MMS.

Another function that is new to the user is the steganography part. Since the picture with the hidden message is published on social media, it is important that the user, knows when posting the hidden message and the public message. So to make the user experience safe, we have made a warning(see figure 4.2)

Figure 4.2: Function: Warning

The warning tells the user, that the next text entered is public. This is very important information for the user, so that the person does not, expose the hidden text.

The function mentioned earlier in the chapter; starting a conversation. Is taken from the normal way of sending a sms(text message). First the user needs to open the inbox. In the inbox the latest conversations are organized by date and time. This means that the latest comes on top, just like the inbox on an android smartphone. If we look at figure 4.3, we see the latest conversations and that there is a "plus" icon, which lets the user start a new conversation.

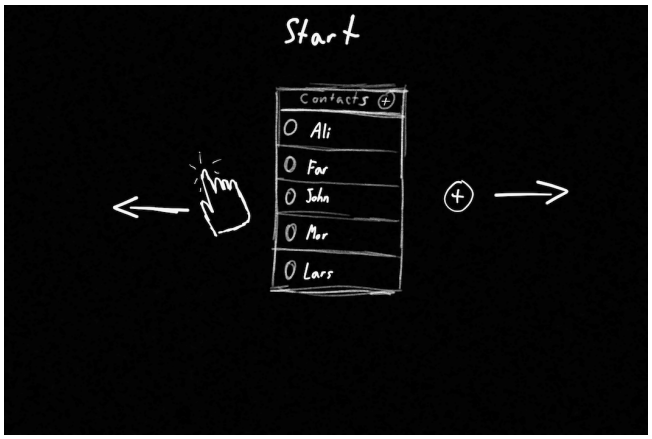


Figure 4.3: Function: Choosing a contact from the inbox

The user needs to choose from an existing conversation or start a new one by clicking/tapping the "plus" icon. Lets assume that the user has chosen "John Smith". After clicking/tapping on John, the conversation pops up, so that the user can write a new text. This text is the one that is hidden in the picture taken afterwards. When the conversation pops up, it looks just like it does on an android smartphone. It even looks like every other chat client, such as facebook messenger and others(see figure 4.4).

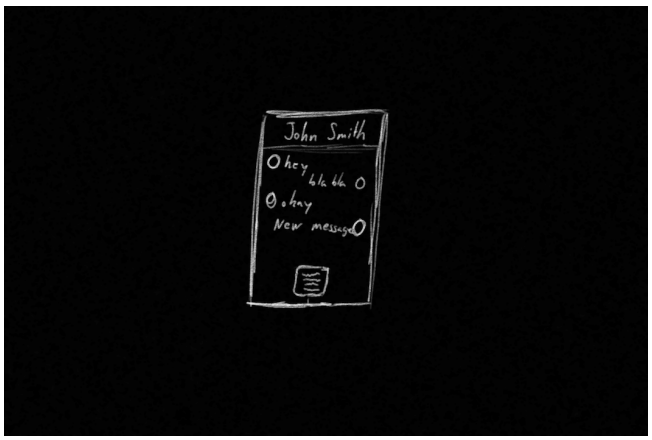


Figure 4.4: Function: writing a hidden message

Looking like every other chat client, makes it user friendly. Especially when the requirement for having the app, requires an android smartphone, that uses the same system!

All objects and the order they are coming in, will be tested in the Lo-Fi prototype.

Chapter 5

Conduct a Lo-Fi prototype user test

5.1 Lo-Fi prototype

The Lo-Fi prototype was developed in a program called Plumbago. The Lo-Fi prototype was created to be used with a "think-aloud" test. The prototype is made up of different pages. Each page simulates an action on the application.

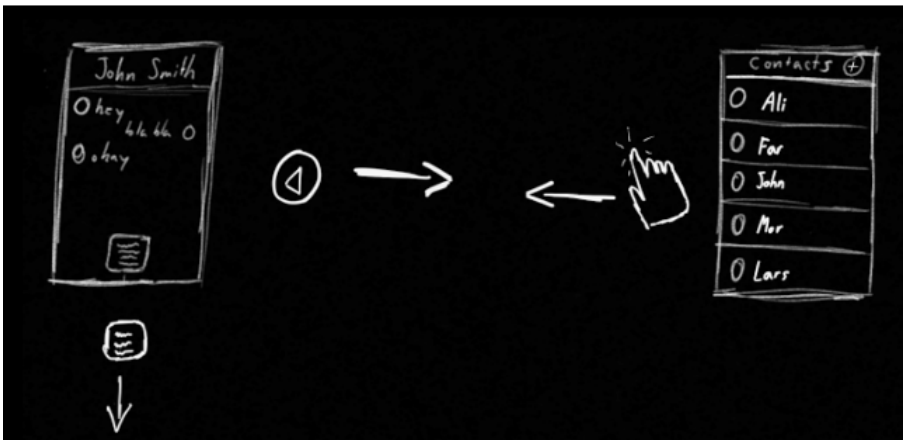


Figure 5.1: A cutout of the Lo-Fi prototype.

In figure 5.1, two of the pages are shown. The user testing the application would then have access to one of these pages. The user starts on the page 'Contacts', an action is then presented with the 'click' icon, and a direction in which to move. This means that the user has to move/slide to the left to complete the 'click' action, and in doing so the user will arrive at the next page.
The full Lo-Fi prototype can be viewed in appendix A.1.1.
The goal of the test is:

- Goal 1: Test whether the warning in figure 4.2 work, and helps the user take an informed decision.
- Goal 2: Test if the user understands the chosen icons.
- Goal 3: Test if the user understands the concept of the application.

5.2 Test setup

First, the participants, where gathered in a room. Here they were informed on what steganography is and a little bit on how it works. Not too much information, but a little to help them understand why, the text will be hidden in a certain picture. After the information and questions has been answered, everybody left the room.

The users will now be called in the room one at a time, to try to complete tasks. The room has been emptied for distractions, such as sodacans, posters and text on blackboards. When a testuser enters the room, the person will be sat at a tablet. Once the test is started two persons will join the user on each side to help out with questions. Another person sits across with a computer to record the audio in the room, so that we can transcribe the tests.

The user was then presented with the start page of the prototype. The user was given a short introduction to what the intended function of the program was, and how it works. The user was then told to select a user from the list of contacts, write a message and send it. The user then has to speak out loud at each action they take, or if anything is unclear.

Beside speaking out loud, the testuser will be asked to tell us, when he or she thinks they have completed a given task. After the test, we will discuss problems, that happened underway and ask for critic of the test. That includes critic on the test itself, but also on the pictures in the low-fi test. Each test subject was also asked for any closing remarks. The full test document including the introduction and test instructions can be found in Appendix A.

5.3 Test results

When the tests have been completed, each of the test-recordings are transcribed as text documents to make it easier to process (The fill transcriptions can be found in the Bibliography[4]). Once transcribed, the data is organized in a spreadsheet as shown in table 5.1. Each cell in a column describes one users response to a slide in the Lo-Fi test. The user's performance is noted in each cell, and a status color indicates whether the test is completed (green), not completed (red), no data (grey) or completed with help (yellow). Each of the colors are classified as Good, warning, bad and no data. Any additional remarks from the user, such as direct criticism, is noted in the cell. A link to the complete spreadsheet can be found in the in the bibliography[5].

Table 5.1: Spreadsheet for data overview

Slide	User 1	User 2	User 3	User 4
1. Slide	Completed without problems. Thought the icon was nice.	Not completed. Did not understand the gestures.	N/A	Completed but needed some help.

	A	B	C	D
1		User 1	User 2	User 3
2	Contacts	Correctly choose a contact, but did not understand the difference between "New message" and "Add contact" icons.	Understood contacts.	Understood contacts.
3	Add contact 1	Understands searching for new contacts	N/A	N/A
4	Add contact 2	Understands search results.	N/A	N/A

Figure 5.2: Screenshot of spreadsheet

In order to get an overview of the results, each of the Lo-Fi tests has been graphed as a stacked column chart. This helps locate the strongest and weakest parts of the Lo-Fi prototype. Based on the overview in figure 5.3 it is clear that test slide 2, 3 did not produce enough data to be conclusive with only a single data point each. The weakest slides, which will some redesigning, are slides 4, 5 and 7.

Here we will need to study the response in-depth to understand what needs to be changed. Slides 1, 8 and 9 was quite good, although 1 and 8 still had some warnings to work with.

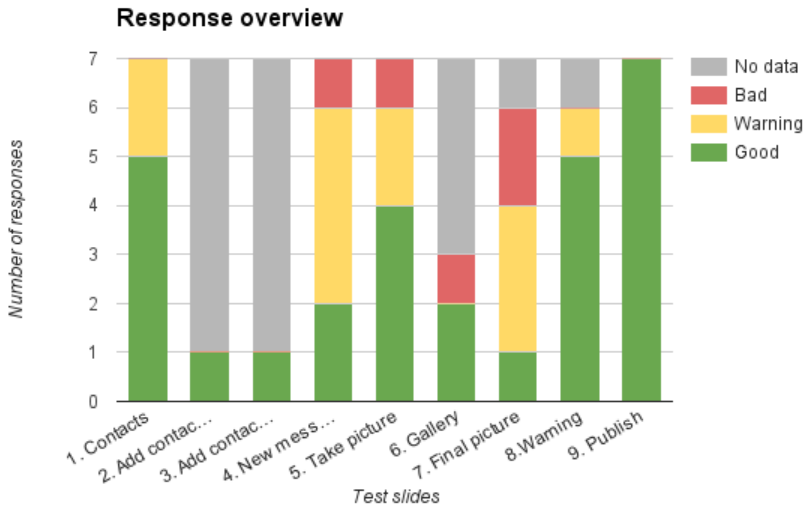


Figure 5.3: Overview of aggregated results.

Having visualized the data, and structured it in a readable format, it is now possible to analyze the test results.

5.3.1 Data related to goal 1

When testing if our security measures worked, there was one specific security hole that was looked at. The security hole appears when the user has to write the public Twitter post. In this stage, the user have entered the hidden text, and will have to make the public post, to hide the text in. Before the 'public post' page is accessed, a warning appears to make sure the user understands what they are about to do. As seen on figure 5.3, 5 users understood the warning, and one user needed some help.

5.3.2 Data related to goal 2

There was only one icon the user had trouble understanding, which was the gallery icon. This had more to do with a badly made icon for the Lo-Fi prototype, in the end a standardized icon will be used.

5.3.3 Data related to goal 3

Most of the test users understands the concept, but one part caused confusion for all users. When the user -wants to write the message, the program was made like this: Picture - Hidden text - Public post. So they where meant to take the picture before writing the message.

All the users expected the application to work like any other message, and wrote the text in the screen for their chosen contact. So the order will have to be changed to look like this: Hidden text - Picture - Public post.

Chapter 6

Reflect upon redesigns possibilities for a potential Hi-Fi prototype

6.1 From Lo-Fi to Hi-Fi

A lot of the response we have received from the Lo-Fi test, have been criticism of the pictures in the test. Because of the pictures, some of the testusers were confused. This is because it isn't easy to draw a gallery icon for example. So for the redesigns to make a High-Fi test, we will upgrade to the Androids icons. Instead of making a new icon for entering the gallery, we will simply use the already known gallery symbol for android users. If we look back at chapter 4(figure 5.3), we see that more than half of the testusers were confused with number 4 "new message"(6.1).

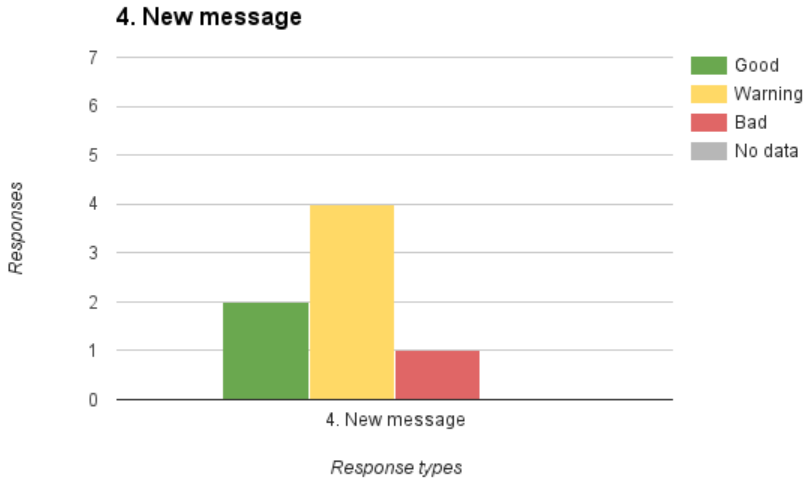
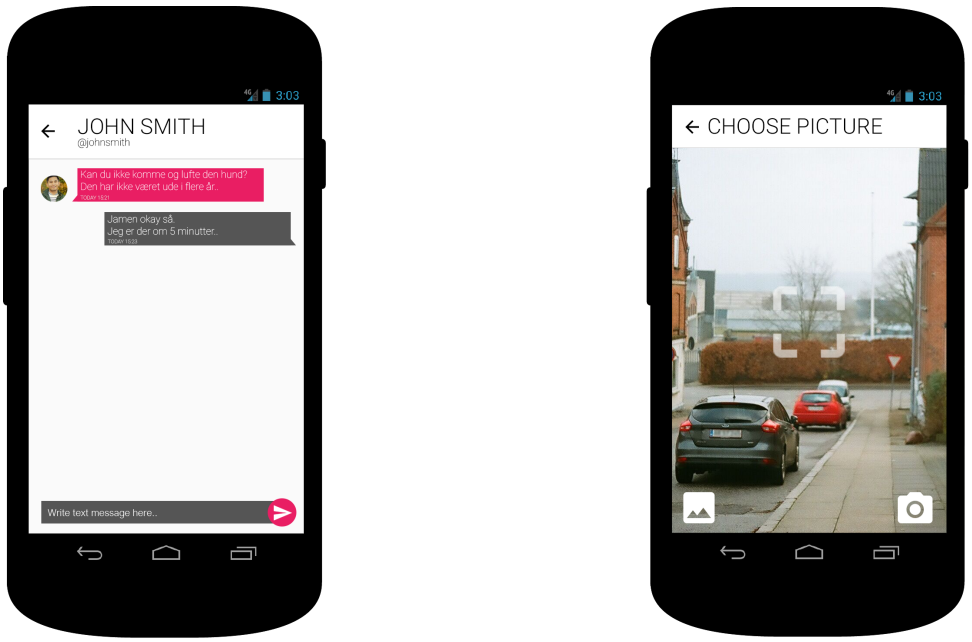


Figure 6.1

They were confused with where to input/write the hidden text. So to solve this problem and any similar problems where inputs are confusing, we have upgraded the test. So that it looks like a real phone and not a drawing. If we look at figure(6.2a), we can easily see where the text is supposed to be written.
If we take another look at 5.3, number 7 "final picture", here the testusers are having lots of problems(6.3). Our "goal 2", is to standardize the icons, so that the user understands what he or she is pressing.



(a) Function: Write hidden text

(b) Function: take picture

Figure 6.2

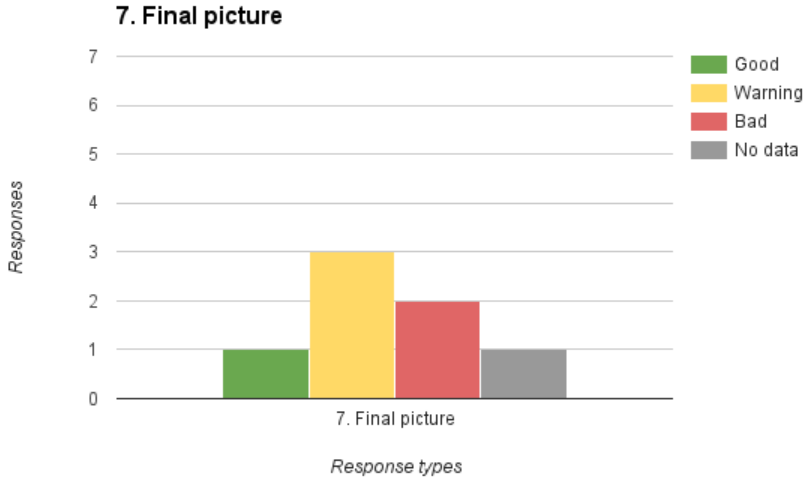


Figure 6.3

If we look at figure 6.2b, we can see that the icons now are standards and hopefully will make sense to the users.
For goal 1 "the warning", there has also been an upgrade. Even though it hasn't been a problem for the users to understand it. However, for one of the users it was very confusing. He thought that it was an error, even tough it says warning! To make sure that this doesn't happen to any other user, we have decided to call the function "Publish info". By doing this the user can not think of it as an error or warning(figure6.4).

Figure 6.4: Function: Warning

6.2 Discussion of the test results in proportion to interaction design theory

When it comes to understand the metaphor "writing with invisible ink" concept of the application, the test shows that a mental model of the concept was generally percieved in the way we wanted, however the indroduction to the test was a relatively detailed explanation of the application, which might have forced the matter in the mind of the user. It's worth noting that, generally, the user fully understood, what it had accomplished when it was done with the test, which indicates that the concept of the application isn't too complex. The interaction design of the application was made with human cognition in mind, prioritizing attention; perception, and recognizion; memory, and the test results indicate that the attention of the user turns to the recognizable icons in the application, and it is generally percieved in the right way. The user sometimes get confused by an icon, and the consensus is, that it is the somewhat shaky unrecognizable icons, that causes the confusion, such as the gallery icon, that might not look like anything the user has seen before, when it comes to taking a picture, with an application like SnapChat or other applications utilizing the camera function of the smartphone or tablet.

Chapter 7

Conclusion

Overall, the conceptual model in this project seemed to work. The users generally understood what they were doing and how to do it.
One of the most important lessons learned in this mini-project is the fact that testing is hard! Much of the feedback on the Lo-Fi prototype test was caused by unclear drawings and icons. You can say the prototype was a bit too Lo-Fi. Given more time, it would be beneficial to re-run a second revision of the Lo-Fi prototype test. A second run could provide more clear data on the actual product, and remove noise in the form of feedback on the test. When all that is said, the data from the first Lo-Fi test is still usable.
The Lo-Fi test showed that users were able to follow common smartphone design conventions. Straying away from the conventions quickly made the users unsure about what to do. This is where we need to improve the design for the Hi-Fi prototype by not trying to re-invent the wheel and instead reuse existing conventions where possible. This will be done by using standardized icons, because most of our design problems was caused by custom icons.
The Lo-Fi test also showed that the warning message worked and it conveyed the intended message to the users.
Summing up, the project is on the right track but still needs some work before it is ready for the world.

Bibliography

[1] statestikbanken. *statestikbanken.dk*. 2015. URL: http://www.statistikbanken.dk/VARFORBR (visited on 04/22/2016).

[2] socailstats. *socailstats.dk*. 2015. URL: http://socialstats.dk/ (visited on 04/22/2016).

[3] Amnesty. *Amnesty mass surveillance*. 2015. URL: http://amnesty.dk/nyhedsliste/2015/global-modstand-mod-usa-s-masseovervaagning (visited on 04/22/2016).

[4] ITCB370. *Transcribed test recordings*. 2016. URL: https://goo.gl/DCPWGV (visited on 05/04/2016).

[5] ITCB370. *Dataset of processed tests*. 2016. URL: https://goo.gl/zw5aYD (visited on 05/04/2016).

Appendix A

Test introduction

A.1 Introduktion til Lo-Fi prototype

Dette scenarie går ud på at teste basis funktionaliteten af en chat app til android. App'en er skabt med henblik på beskyttelse af privatlivet, og er i stand til at sende og modtage hemmelige beskeder. App'en benytter en teknik kaldet steganografi, der går ud på at gemme tekst i billeder. Det forventes ikke at brugeren har kendskab til steganografi. Derfor vil app'en i store træk fungere som en almindelig chat app. En hemmelig besked afsendes ved at brugeren tager et billede og skriver en besked. App'en gemmer derpå beskeden i billedet. Billederne med hemmelige beskeder sendes aldrig direkte til modtageren. De postes i stedet til Twitter hvor modtageren henter dem. Det gøres for at afsender og modtager aldrig er i direkte kontakt. Mens du bruger appen må du gerne tænke højt og sige hvis der mangler noget. Sig gerne til hvis du føler dig forvirret, da det er vigtig feedback. Har du forslag til at gøre noget anderledes, eller noget som ikke giver mening skal du bare sige til.

A.1.1 Test: Afsendelse af besked

Opgaven er at vælge en kontaktperson og sende en skjult besked til kontakten.
Det første billede du ser er dine kontaktpersoner. Hvis der er mulighed for at indskrive oplysninger på et skærmbillede skal du udfylde felterne. Når du udfylder et felt må du gerne tænke højt og fortælle hvad du vil skrive. Testen afsluttes når du når sidste slide eller giver op.

A.2 Lo-Fi prototype

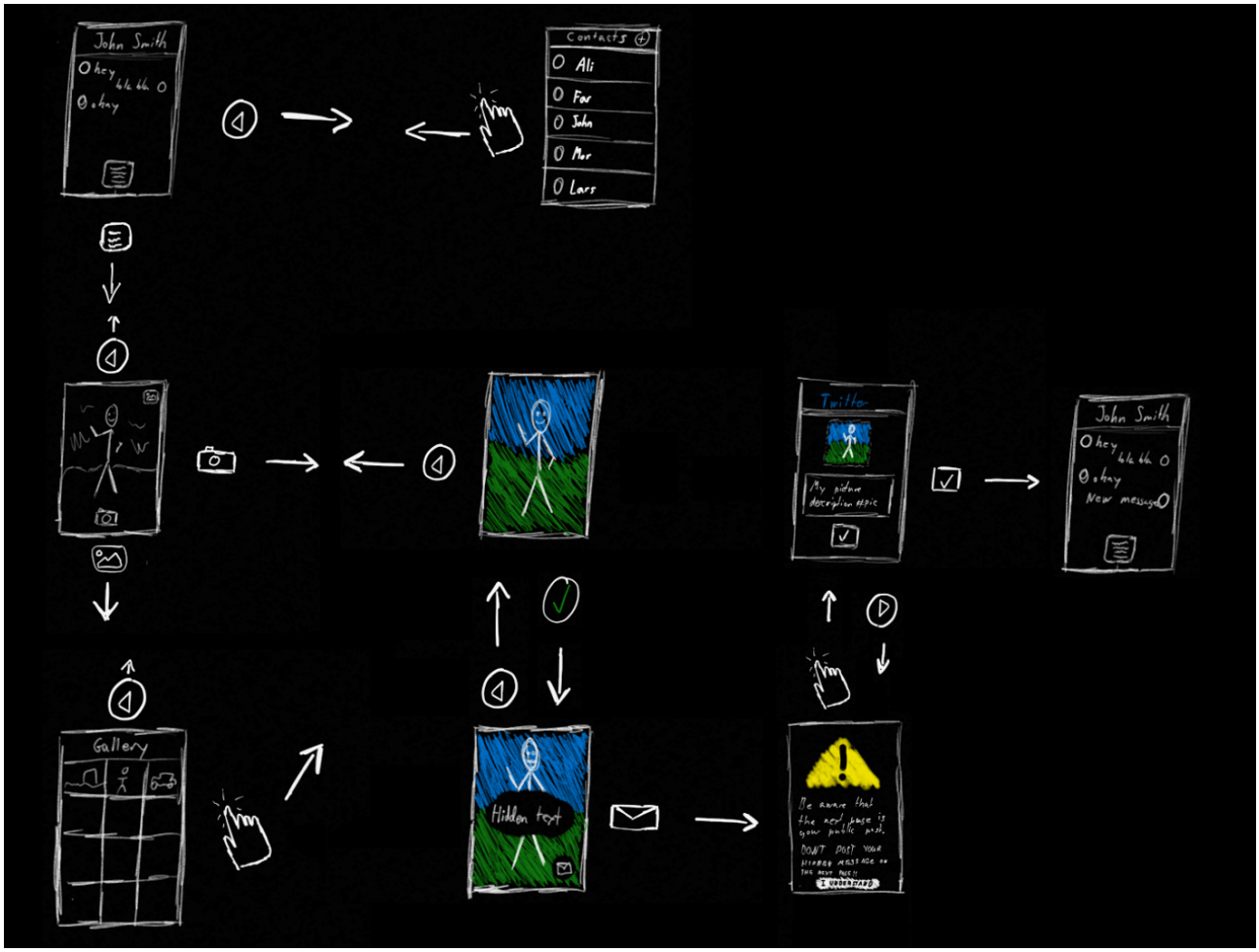


Figure A.1: The full version of the Lo-Fi prototype