Photo Encryption in Medicine

Georg Bernold (1325845), Gabor Szivos (1227443)

Index Terms—Photo Encryption, Image, Encryption, Medicine

1 Problem Description

PRIVACY is one of the key issues of the information age. Especially in the post-Snowden era this fact has become clear to the most individuals around the globe. Numerous regulations and laws require it across all kinds of use cases and industries. A well known way to achieve privacy is through encryption, which means encoding an information in such a way that only authorized parties can access it. Hardly any efforts on implementing encryption can be found in photography, which is a remarkable finding, keeping in mind that photographs are generally among the most private media. This statement becomes even more astonishing considering the year, when the first patent for such a solution was registered: 1999. [7] To fulfill the requirements of privacy in photography without a gap it might be necessary to encrypt photographs right after they are taken.

Especially in the context of medicine this is very important as health data is considered the most private data [8]. Medical photographs show a patients body, they are used to document visual properties of the skin, the state of a wound or the progress of a plastic surgery. All of the above mentioned photographs document very private information about an individual, which is only to be seen by authorized persons.

Another important application for encryption of photographs is journalism. Journalists are looking for possibilities to hide any traces of sensitive material on their devices, for obvious reasons. Journalists take big risks on them when taking sensitive pictures in countries with authoritarian governments, where such actions are considered as act of crime and punished with imprisonment or even death penalty [3]. So it could be possible that encryption would not be enough to keep the journalists safe, as a trace of encrypted images could already lead to punishments. Encryption is a first step to achieve this, this is why in December 2016, 150 journalists wrote an open letter to camera manufacturers, asking them to implement such a feature.[5]

So we can state that there is a demand for digital single-lens reflex (DSLR) photo encryption feature which is not (yet) satisfied by state of the art devices. This fact may lead physicians or journalists to take their private devices, which support encryption, for taking photographs, which is no real option for professional privacy. Privacy is strictly regulated by law, the most important regulations may be found in the general protected data regulation of the EU [6], the European convention of human rights [4] or the respective national law.

Another issue that may be stated here is that even if custom solutions for encryption do exist, they are not implemented to be turned on and off again easily. This leads to the conclusion that it is not possible to perform image encryption without a required amount of previous knowledge and expertise with such solutions.

A good example for this is the Magic Lantern encryption module, which will be explained

- *188.948 SE - Seminar aus Medizinischer Informatik*
- *Seminar*
- *Supervisor: Univ.Prof. Mag. Dr. Silvia Miksch*

April 6, 2017

in the next section. The weaknesses of this solution are as follows:

1) The usage of Magic Lantern is limited to less than 10 models of canon cameras.
2) The encryption algorithm used in this module is considered weak, even by the developer.
3) Plausible deniability is not assured, as the encrypted photos may be found on the SD card.

The goal of this project is to find a solution for the encryption of photographs on DSLR cameras. Additionally, the proposed solution should represent a best practice solution for the introduced problem. This enables a solid base for further research on this topic.

2 Expected Results

Our goal is to evaluate different possibilities, to make on-the fly encryption for DSLR cameras possible. To ensure comparability between the introduced possibilities it is inevitable to define measurable parameters.

As encryption requires computational resources, its performance is dependent on the platform it is used on. Considering this fact it is essential to be aware of the limited hardware resources of DSLRs that can be used for encryption. So we can state that the performance of the implemented algorithm may be measured by the time, the encryption process takes ($t_{encryption}$). Furthermore, a threshold must be found that determines the critical time ($t_{critical}$) for the duration of the encryption process.

Additionally, it must be assured that the encrypted information may only be decrypted by authorized persons. For this reason, the used encryption algorithm must be considered safe, according to a definition which needs to be defined in the course of the project.

To ensure a specific degree of performance it is necessary that the evaluated solution does rely on as little proprietary soft- and hardware as possible. An important information which is not known to us for now: whether or not it is better to perform encryption on DSLRs with software or hardware. In the first place, this is a performance related topic, but it has big impact on portability.

Another parameter worth mentioning is, whether the proposed solution supports plausible deniability. Plausible deniability, according to the Oxford dictionary, is "the possibility of denying a fact, especially a discreditable action without arousing suspicion".[1] It worth mentioning, that the plausible deniability, is not really important in the medical context, however it might help for the journalist community.

Our final goal is to create a method which can evolve to a best practice, which gives the medical and journalist community the possibility to protect their data with the help of encryption. A best practice solution should fulfill the following requirements in the best possible way.

1) The duration of the encryption process must not extend the defined threshold ($t_{encryption} \leq t_{critical}$);
2) The used encryption algorithm must be considered safe.
3) The solution must not be limited to one DSLR manufacturer.
4) Plausible deniability must be assured.

To make this happen we found four different solutions which could be used to make DSLR camera encryption possible. For Canon cameras there is an open source project called Magic Lantern, which enables the extension of the stock firmware with new functionalities, like encryption or better autofocus. This project already has an encryption module, however this module uses relatively weak algorithms. It also makes possible the use of stronger algorithms (RSA), however these are very slow. Our plan is to create a new encryption module with better and faster encryption algorithm (like Chacha20 with Poly1305). During this task we are going to learn about how the encryption in Magic Lantern works, and how different kind of algorithms perform. Additionally we also going to test, if there is a possibility to implement this feature to enable the plausible deniability.

As a second method we found, that there is way to implement a special SD-Controller, which is connected to a field programmable gateway array (FPGA), which is again connected to a mass storage. In this setup the FPGA is responsible for the encryption process.

Our goal is to find out how such a special SD-FPGA interface performs in a DSLR camera. And how the encryption algorithm performs on an FPGA. And as in the previous setup we are going to try to evaluate if there is a possibility to implement such a system in a way, where the user has an option for plausible deniability.

The third option would be to use a special WiFi capable SD-Card which in turn would send the photos directly to the users smartphone (or other smart device), which would take care about the encryption. The questions we ask regarding this method, and try to answer is how to transform images from the DSLR camera to the smart device and how to securely delete the data after the transmission is completed. We are also going to evaluate the performance and the possibility to implement the option for plausible deniability.

The last method we will consider is to place a whole PC between the mass storage and the camera in the form of an Intel Edison, which a fully functional PC in the size of an SD-Card. As in the previous setups we will evaluate the performance and the option for plausible deniability.

3 Method

To be able to evaluate and compare the results, how the previously mentioned methods work, we are going to create for each of them a prototype. This means we are going to write a module for the Magic Lantern project, which will replace the current implementation with a stronger encryption algorithm. Based on the work of Davidsson et. al. [2] we are going to create a modified SD-Card which includes an FPGA module between the SD-Card controller and the mass storage. As what the smartphone setup concerns, we are going to write an android app, for handling the datatransfer between the DSLR and the smartphone, with the help of an SD-Card with on-board WiFi capabilities. For the Intel Edison solution, we plan to use the General Purpose Input Output (GPIO) ports to fake an SD-Card for the DSLR-Camera. And to implement the encryption feature we are going to write a hook for the GPIO ports, meaning if there is a request from the camera to save an image on the mass storage the interconnected Intel Edison will take the image and encrypt it, and on the other side it will send back a response for the camera, that the image has been successfully saved.

The decryption of the files, apart from the smartphone solution, where the smartphone takes care of the crypto, will be realized as an external program which is independently runs on a desktop PC, or any similar architecture. This means there will be no on-board solution for the decryption, because this would jeopardize the goal of the encryption.

The planned steps for realizing this project would be the following. First we are going to perform a state of the art analysis to get a better view about the current situation regarding the hardware and software solutions of encryption in the field of embedded systems. As the software solutions seem to be easier to accomplish, firstly we are going to implement the Magic Lantern module. Following that we will implement the smartphone solution with the WiFi-capable SD-Card. Next we will take care of the implementation of the Intel Edison solution. And last but not least we are going to implement the FPGA tweaked SD-Card.

4 References

References

[1] plausible deniability - oxford dictionaries. https://en.oxforddictionaries.com/definition/plausible_deniability. Online; Accessed: 30.03.2017.

[2] Alexander Davidsson and Torbjrn Rasmusson. A vhdl architecture for auto encrypting sd cards. Master's thesis, 2016. 36.

[3] Amnesty International. Egyptian photojournalist at risk of death penalty. https://www.amnesty.org/en/get-involved/take-action/journalism-is-not-a-crime-free-shawkan/, 2016. Online; Accessed: 06.04.2017.

[4] European Court of Human Rights. European convention on human rights, 2010.

[5] Freedom of the Press Foundation. Camera encryption letter. Open Letter to Camera Manufacturers, December 2016.

[6] European Parliament and European Council. General data protection regulation, 2016.

[7] E. Steinberg and V. Yeremenko. Method and apparatus for in-camera encryption, January 19 1999. US Patent 5,862,217.

[8] Patricia Williams and Emma Hossack. It will never happen to us: the likelihood and impact of privacy breaches on health data in australia. In *Health Informatics: Digital Health Service Delivery - The Future is Now*, pages 155–161, 2013.