https://doi.org/10.2352/ISSN.2470-1173.2018.07.MWSF-120

Privacy Preserving Forensics for JPEG Images

Huajian Liu, Martin Steinebach, Richard Stein, Felix Mayer; Fraunhofer SIT; Darmstadt, Germany

Abstract

Visual content like digital images and videos are helpful in forensic investigation, which usually provides direct evidence. However, the privacy issues arising therefrom are rarely addressed. In this paper a partial encryption based scheme is proposed to enable privacy-preserving forensics for JPEG images. Viewing sensitive regions, e.g. human faces, is only granted by the trusty party when the content is proved to be of potential relevance to the investigation. A key management protocol is defined for access authorization, which ensures access to the restricted content only possible under agreement by pre-defined parties. A fully reversible partial encryption approach is applied to ensure that the encrypted regions can be perfectly recovered after the decryption is approved. Evaluation results demonstrate the applicability and effectiveness of the proposed scheme.

Introduction

A forensic investigation always holds the conflict of violating privacy rights versus ignoring relevant evidence. This is for example discussed by Aminnezhad et al. [1]. Research calls in the EU regularly address forensics under the limitations of privacy concerns to find a trade-off between interests. In Germany, the Federal Ministry of the Interior regularly stresses that privacy must be considered in all forensic activities. In Germany, filtering and removal of private data is required when forensic investigations are executed. [1]

Still, technical solutions enabling a fair trade-off between the interests of the investigator and the target of the investigation are rare. They should on the one hand enable access to relevant data, but on the other hand protect private information, if they are not necessary for the case. This may seem to further complicate already complex investigations, but at the end will increase acceptance and security of the forensic process.

In this work, we focus on the protection of digital images, considering human faces as privacy-sensitive regions because they contain identifiable personal information. Our scenario is the following: a person is accused for committing a crime, e.g. dealing drugs. His smart phone is searched for evidence. One potential evidence is the photos on the smart-phone showing locations of illegal activities or known criminals. They could confirm that the accused has been at these places and met criminals. However, during the investigation also photos of his family, his children and other children playing together with them, or other innocent persons would be subject to inspection. The access to these photos containing faces of innocent persons should be limited.

Our approach limits the risk of unnecessary loss of privacy by automatically encrypting all faces found in an image. Figure 1 shows a simplified example. An investigator is able to estimate if the partially encrypted image is of relevance and sends a request to access the image information of individual faces to a trusty third party, e.g. a prosecutor. If this party agrees upon the relevance, it can enable the decryption of the faces. For instance, it could allow to access all faces of armed persons in an image, but refuse access to faces of children.

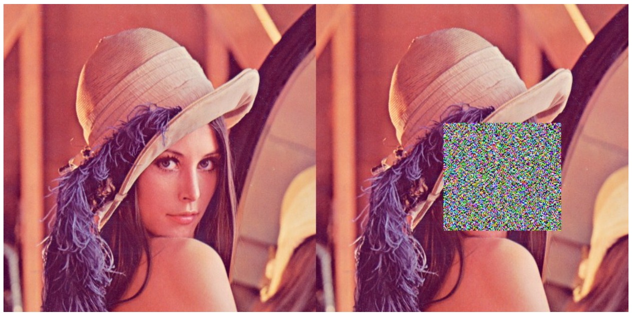

Figure 1. *Left: Image with visible face, Right: The face has been detected and encrypted.*

In the following sections, we describe how this concept is realized by an asymmetric multiparty key access protocol combining face detection and partial encryption. Although human faces are taken as an example of privacy critical regions in this paper, the proposed scheme can be straightforwardly applied to any other kind of regions containing privacy-sensitive information.

The paper is organized as follows. In Section 2, related works regarding privacy-preserving forensics are briefly summarized. Section 3 introduces the proposed scheme including the key management protocol, the local partial encryption and the integrity verification. Test results are presented in Section 4. We conclude the paper in Section 5.

Related Work

The idea to execute a forensic investigation in a privacy-preserving manner is not new. In this section we provide a brief overview on approaches discussed in the literature. A short introduction of partial encryption is also given as it is an important component of the proposed scheme.

Privacy Preserving Forensics

Srinivasan et al. [2] describe various policies for preserving privacy during an investigation. They do not focus on technical solutions, but rather on correct behavior of investigators and acceptance of evidence by the court. Adams [3] discusses the requirements of a forensics tool to be compliant with the laws of the United States. One aspect addressed is logging the actions of investigators, allowing to trace privacy breaches.

Hou et al. [4] present a technique to search encrypted data for multiple search words. In the scenario presented, there are

[1] https://www.datenschutz-praxis.de/fachartikel/computer-forensik provides a discussion on the topic in German.

two roles. An investigator who performs an investigation and only has access to relevant data and an administrator who manages the data. A similar approach is taken by Armknecht and Dewald [5]. Here a third party is investigating emails of a company. All emails are encrypted, and only if a sufficient number of keywords within the emails are found, the full text of these individual emails can be decrypted. Peter et al. [6] discuss the need for protecting privacy when using robust images hashes in forensic investigations by adding encryption to the hash scheme. Stahlberg et al. [7] explore the threat to privacy imposed by unintended data retention in the database systems.

Partial Encryption

Partial encryption is a family of algorithms for various applications, also known as selective encryption. An overview on partial encryption techniques is provided by Mondal et al. [8], with concepts ranging from early RGB pixel encryption to complex chaotic and wavelet-based approaches.

In general partial encryption falls into two categories. (A) only a subset of all elements of an image is encrypted [9, 10], for example the most significant bits of a raw image or low frequency coefficients of an JPEG file [11]. As a result, the whole image looks encrypted while only a fraction of the data representing the image is actually encrypted. (B) only a subsection of the image is encrypted, usually a selected region [12, 13]. A typical partial encryption algorithm combines a selector and an encryption algorithm. The selector decides what to encrypt and the encryption algorithm performs the actual encryption.

For our privacy-preserving forensics scenario, the partial encryption techniques in the second category are required which must meet the following requirements.

- **Cryptographic security**: The encrypted content shall not be able to be reconstructed without the knowledge of the proper secret key.
- **Visual security**: The encrypted content shall be visually unrecognizable.
- **Reversibility**: The encryption must be reversible without causing loss or modification of the original information.
- **Partiality**: The encryption shall not hinder the normal usage of the unencrypted parts for investigation.

Proposed Scheme

In this section, the proposed scheme is introduced, including the key management protocol, the applied partial encryption approach for JPEG images and the integrity verification of protected faces.

Role Definition

To simplify the description, the involved parties are classified into three roles according to their functionality, which are defined as follows.

- **The technician** obtains and anonymizes the images to be inspected. He detects, signs and encrypts all the faces in images. Then the partially encrypted images will be transmitted to *the investigator*. In practice, the image anonymization process shall be automatically accomplished, i.e. to prevent a human technician from having access to the unencrypted images, *the technician* is a smart device or software.
- **The investigator** receives the encrypted images and inspects them for potentially suspicious persons. If one or more suspects shall be identified, he chooses the faces of the suspects and submits a request together with the encrypted image to *the prosecutor* for approval.
- **The prosecutor** determines if a face shall be decrypted for free view or not. Upon receiving a request from the *the investigator*, *the prosecutor* inspects the requests and grants the access to faces if they are necessary for the investigation. However, *the prosecutor* has no access to the faces by himself. If the request is approved, a *release-answer* will be sent back to *the investigator*, with which the faces can be decrypted.

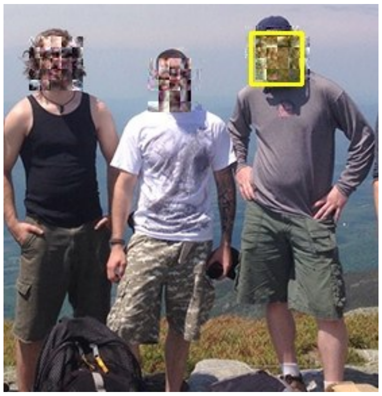

Figure 2. An image showing three persons. The investigator requests to decrypt the face surrounded by the yellow box.

Figure 2 illustrates the concept: it shows the state when *the investigator* has requested decryption from *the prosecutor* for one of the three faces in the image, which is indicated by a yellow box.

Key Management Protocol

Among the above-defined three roles, *the technician* encrypts and signs faces and *the prosecutor* examines decryption requests. Only *the investigator* may decrypt the faces with the approval of *the prosecutor*.

To fulfill the desired access control rules, four sets of keys are used in the encryption and decryption stages including

- Ke: the symmetric key for partial encryption,
- (PKt, SKt): the public and private key pair of *the technician*,
- (PKi, SKi): the public and private key pair of *the investigator*,
- (PKp, SKp): the private and public key pair of *the prosecutor*.

The technician signs the detected faces in a JPEG image F using his private key SKt and encrypts each face using a symmetric key Ke. The signing process is detailed in the following section of integrity verification. Each face is encrypted with a different Ke. Then each used Ke is encrypted using *the investigator*'s

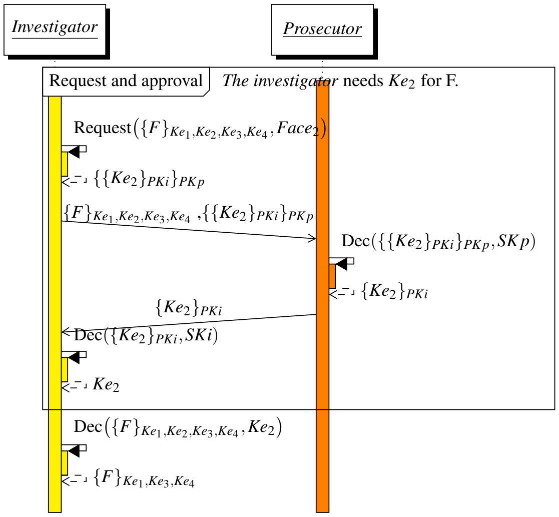
Investigator
Prosecutor
Request and approval
The investigator needs Ke_2 for F.
Request$(\{F\}_{Ke_1,Ke_2,Ke_3,Ke_4}, Face_2)$
$\{\{Ke_2\}_{PKi}\}_{PKp}$
$\{F\}_{Ke_1,Ke_2,Ke_3,Ke_4}, \{\{Ke_2\}_{PKi}\}_{PKp}$
Dec$(\{\{Ke_2\}_{PKi}\}_{PKp}, SKp)$
$\{Ke_2\}_{PKi}$
$\{Ke_2\}_{PKi}$
Dec$(\{Ke_2\}_{PKi}, SKi)$
Ke_2
Dec$(\{F\}_{Ke_1,Ke_2,Ke_3,Ke_4}, Ke_2)$
$\{F\}_{Ke_1,Ke_3,Ke_4}$

Figure 3. *Request and approval process*

public key PKi and *the prosecutor*'s public key PKp consecutively as follows:

$$Kee = \{\{Ke\}_{PKi}\}_{PKp} \tag{1}$$

where $\{D\}_K$ denotes the encryption function which encrypts the message D using the key K.

The encrypted key Kee together with the face signatures is then stored as metadata in F, more specifically, in the JPEG application segments, i.e. APP$_n$ marker segments of JPEG header. Depending on the quantity of faces and the involved investigator and prosecutors, the generated metadata vary in size and will lead to slight growth of the JPEG file size.

Figure 3 illustrates the request and approval process between *the investigator* and *the prosecutor*. Assume there are four faces in F which are encrypted using Ke_1, Ke_2, Ke_3 and Ke_4 respectively. *The investigator* observes that the second face encrypted with Ke_2 is suspicious and shall be decrypted for further inspection. Then he sends a request to *the prosecutor*, which includes the encrypted image F and the encrypted Ke_2 which is $Kee_2 = \{\{Ke_2\}_{PKi}\}_{PKp}$. If the request is approved, *the prosecutor* decrypts Kee_2 using his private key SKp and sends the partly decrypted key $\{Ke_2\}_{PKi}$ as *release-answer* to *the investigator*. Upon receiving the *release-answer*, *the investigator* decrypts Ke_2 using his private key SKi. With Ke_2 he then decrypts the second face, while other faces still remain encrypted. Finally the integrity of the decrypted face can be verified by the signed signature, which is stored as metadata in JPEG header, using PKt.

This key management protocol can be easily extended in case there is more than one investigator or prosecutor involved in the process. If there is more than one investigator, the symmetric key of each face will be encrypted by each investigator's public key separately. To identify each investigator, all encrypted keys of an investigator will be grouped and labeled with the fingerprint of his public key. In case of decryption request, his keys can be identified with the help of his public key before extracted for approval and decryption.

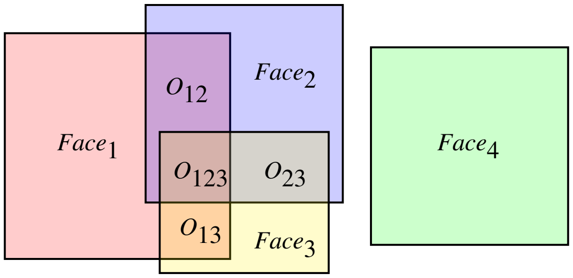

Figure 4. *Overlapping faces*

Handling Overlapping

Since each face is separately encrypted, if there is overlapping between detected faces, the overlapped areas will be encrypted multiple times. In this case, the decryption of an overlapped area is only possible when all the overlapped faces are decrypted. However, the decryption of each single should be independent of other faces. Furthermore, an overlapped area belongs to more than one face and has to be included in the decryption of any overlapped faces to render a complete face view. Therefore, overlapping areas have to be identified and each overlapping area shall be encrypted by a separate symmetric key Ko instead of using any key belonging to faces.

Figure 4 illustrates an example of face overlapping, in which each box represents a detected face. $Face_1$, $Face_2$ and $Face_3$ are overlapped with each other. O_{12} represents the overlapping area of $Face_1$ and $Face_2$, O_{13} the overlapping area of $Face_1$ and $Face_3$ and O_{23} the overlapping area of $Face_2$ and $Face_3$. In addition, O_{12}, O_{13} and O_{23} share a further overlapping area of O_{123}. $Face_4$ is not overlapped with other faces.

To avoid multiple encryption and ensure independent decryption of each face, $Face_1$, $Face_2$ and $Face_3$ must be encrypted excluding the overlapping areas. Each overlapping area O_{12}, O_{13} and O_{23} must be encrypted respectively excluding the area O_{123} which shall be separately encrypted. Thus, each area is encrypted only once and each face can be decrypted alone. For instance, when $Face_1$ shall be decrypted, the overlapping areas O_{12}, O_{13} and O_{123} will be decrypted together to render a complete view of $Face_1$.

To ensure the overlapping areas belonging to a face can be decrypted together with the face, in the key management the symmetric key Ke of each face shall be first concatenated with the keys of overlapping areas before encrypted using Equation 1 as follows:

$$Kee = \{\{Ke \| Ko_1 \| Ko_2 \| ... \| Ko_n\}_{PKi}\}_{PKp} \tag{2}$$

where Ko_n represents the symmetric key of the nth involved overlapping area. Thus, after approved by *the prosecutor*, *the investigator* obtains all necessary keys to decrypt the whole face region. An example of concatenated keys for the overlapping case in Figure 4 is shown in Table 1.

Table 2 lists two encrypted versions of the concatenated keys in Table 1 for two investigators. Every concatenated key is first encrypted by each investigator's public key respectively and then encrypted by *the prosecutor*'s public key. If the request of the first investigator to observe the first and the third faces is approved by *the prosecutor*, the corresponding encrypted keys of the first in-

Table 1. Example of concatenated keys

Face	Key of Face	Key of Overlapping Area	Concatenated Key
Face_1	Ke_1	$Ko_{12}, Ko_{13}, Ko_{123}$	$Ke_1 \| Ko_{12} \| Ko_{13} \| Ko_{123}$
Face_2	Ke_2	$Ko_{12}, Ko_{23}, Ko_{123}$	$Ke_2 \| Ko_{12} \| Ko_{23} \| Ko_{123}$
Face_3	Ke_3	$Ko_{13}, Ko_{23}, Ko_{123}$	$Ke_3 \| Ko_{13} \| Ko_{23} \| Ko_{123}$
Face_4	Ke_4	—	Ke_4

Table 2. Encryption and decryption of keys

	Face	Encrypted Key	After Approval
Investigator_1	Face_1	$\{\{Ke_1 \| Ko_{12} \| Ko_{13} \| Ko_{123}\}_{PKi_1}\}_{PKp}$	$\{Ke_1 \| Ko_{12} \| Ko_{13} \| Ko_{123}\}_{PKi_1}$
	Face_2	$\{\{Ke_2 \| Ko_{12} \| Ko_{23} \| Ko_{123}\}_{PKi_1}\}_{PKp}$	$\{\{Ke_2 \| Ko_{12} \| Ko_{23} \| Ko_{123}\}_{PKi_1}\}_{PKp}$
	Face_3	$\{\{Ke_3 \| Ko_{13} \| Ko_{23} \| Ko_{123}\}_{PKi_1}\}_{PKp}$	$\{Ke_3 \| Ko_{13} \| Ko_{23} \| Ko_{123}\}_{PKi_1}$
	Face_4	$\{\{Ke_4\}_{PKi_1}\}_{PKp}$	$\{\{Ke_4\}_{PKi_1}\}_{PKp}$
Investigator_2	Face_1	$\{\{Ke_1 \| Ko_{12} \| Ko_{13} \| Ko_{123}\}_{PKi_2}\}_{PKp}$	$\{\{Ke_1 \| Ko_{12} \| Ko_{13} \| Ko_{123}\}_{PKi_2}\}_{PKp}$
	Face_2	$\{\{Ke_2 \| Ko_{12} \| Ko_{23} \| Ko_{123}\}_{PKi_2}\}_{PKp}$	$\{\{Ke_2 \| Ko_{12} \| Ko_{23} \| Ko_{123}\}_{PKi_2}\}_{PKp}$
	Face_3	$\{\{Ke_3 \| Ko_{13} \| Ko_{23} \| Ko_{123}\}_{PKi_2}\}_{PKp}$	$\{\{Ke_3 \| Ko_{13} \| Ko_{23} \| Ko_{123}\}_{PKi_2}\}_{PKp}$
	Face_4	$\{\{Ke_4\}_{PKi_2}\}_{PKp}$	$\{\{Ke_4\}_{PKi_2}\}_{PKp}$

vestigator for these two faces are partly decrypted by *the prosecutor*, while other keys of the first investigator and all keys of the second investigator remain encrypted by *the prosecutor*'s public key, as shown in the right column of Table 2. Subsequently, the first investigator can decrypt the keys completely with his private key SKi_1 and extract the symmetric keys for the first face (Ke_1), the third face (Ke_3), and the involved overlapping areas (Ko_{12}, Ko_{13}, Ko_{23} and Ko_{123}). Finally he can decrypt $Face_1$, $Face_3$ and the overlapping areas O_{12}, O_{13}, O_{23} and O_{123} to obtain a complete view of the first and the third faces.

Local Partial Encryption

Partial encryption plays an important role in the proposed scheme, which has to meet the requirements listed in Section 2. In this work, the partial encryption approach in [14] is applied to encrypt detected faces locally, which is compatible with JPEG compression standard [15].

The faces in JPEG images are assumed to be given by a surrounding rectangle which can be determined by face detection technology. Face detection is beyond the scope of this paper and the following will focus on the partial encryption of the regions containing faces.

The partial encryption approach in [14] encrypts the quantized DCT coefficients of selected JPEG blocks before entropy encoding. The DCT coefficients are extracted from the JPEG blocks inside the rectangle surrounding a face and encrypted in full length p, i.e. the upper bound of the quantized DCT coefficient precision. In baseline JPEG [15], for instance, the corresponding maximal precision of quantized DCT coefficients is 11 bits, i.e. $p = 11$, which is determined by the sample precision of 8 bits. Each coefficient is first represented with a p-bit stream. Then the coefficient bit stream is aligned in a byte array, which is subsequently encrypted with Ke using a symmetric encryption method, e.g. `AES`. From the encrypted byte array every p bits are extracted and assigned to each coefficient sequentially. Finally, these encrypted coefficients replace their original counterparts in the JPEG stream, such that the faces become irrecognizable.

Compared to encryption approaches based on encoded coefficients [11] [12], which reduces the encryption space of coefficients in order to keep the encoding size, encrypting quantized coefficients directly achieves a full encryption of each coefficient. This ensures the fulfillment of the *cryptographic security* and *visual security* requirements.

However, full encryption also results in bigger JPEG files, because the encrypted coefficients are pseudo-randomized bits and hence they are compressed less efficiently in the subsequent RLE and entropy encoding. Therefore, in addition to *full encryption*, two variants have been proposed in [14] to alleviate the increase of JPEG file size: *encoding-friendly encryption* and *hybrid encryption*. *Encoding-friendly encryption* behaves as if the encryption would be executed on the quantized and encoded coefficients, while *hybrid encryption* encrypts the significant coefficients containing the majority of the visual content fully and the other coefficients encoding-friendly for a good trade-off between security and compression. In all these three variant encryption approaches, the encrypted faces can be perfectly recovered by decryption with the corresponding key Ke, which fulfills the *reversibility* requirement.

Furthermore, as the encryption occurs locally and is totally compatible with JPEG standard, it will not prevent the partially encrypted JPEG image from decoding and viewing the unencrypted portions. All JPEG blocks outside face regions are kept intact during the encryption and can be decoded as usual. The encrypted blocks are re-encoded as standard JPEG stream after encryption and therefore are fully compatible with compliant JPEG decoders, only rendering an encrypted representation of the corresponding regions after decompression. Thus, the *partiality* requirement is met.

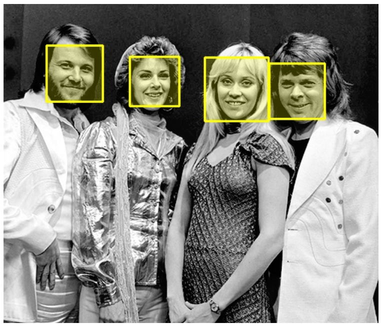

Figure 5. *Face detection with proper parameters. (Image CC/AVRO)*

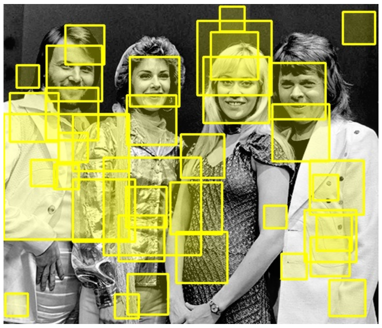

Figure 6. *Face detection with improper parameters. (Image CC/AVRO)*

Integrity Verification

To verify the integrity of faces, all faces are signed by *the technician* with his private key SKt. After decryption, the decrypted faces can be verified using his public key. Each face is signed separately so that it can be verified individually. In addition, the background, where no face appears, is also signed. To ensure the linkage between faces and background, the signature should become invalid after a face is moved or exchanged in the image or into other images. To achieve this, the face content, its size and position and the background are all taken into account in the signature generation as follows:

$$Sig_f = sign(C_f, W_f, H_f, x_f, y_f, Sig_{bg}) \tag{3}$$

where Sig_f is the face signature, C_f is the DCT coefficients of the JPEG blocks inside a face region, W_f and H_f are the face width and height, x_f and y_f are the face position and Sig_{bg} is the signature of the background which is generated by the DCT coefficients of the JPEG blocks outside the face regions.

Results

As human faces are defined as as privacy critical regions in this paper, the accuracy of face detection becomes vital for the scheme. It should be noted that face detection requires suitable parameter setting for the given case. Figures 5 and 6 show the results of face detection using OpenCV with different parameter sets. As shown in Figure 6 an improper set of parameters leads to a multitude of falsely detected face regions. Falsely detected faces will result in unnecessary decryption effort and missing faces will lead to leak of privacy information.

Figure 7 shows examples for encrypted Lena images using different encryption schemes. Both full encryption and hybrid encryption result in huge visual impact on the face region, while the impact of the encoding-friendly encryption is much smaller, although the quantity of the encrypted DCT coefficients is doubled. In case of full and hybrid encryption, the face region becomes totally unrecognizable by human eyes.

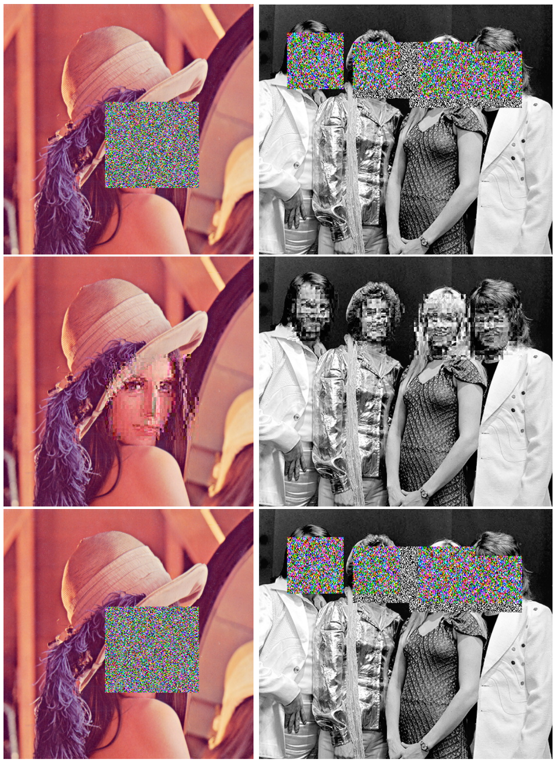

Figure 7. *Visual security. Top: full encryption with 32 coefficients, Middle: coding-friendly encryption with 64 coefficients, Bottom: hybrid encryption with 32 coefficients.*

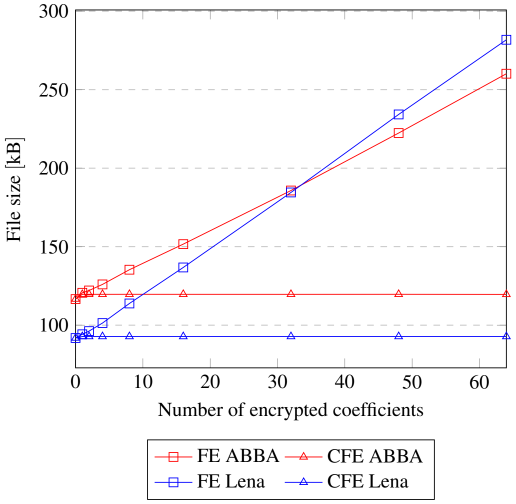

Figure 8. *JPEG file size after encryption. FE: full encryption, CFE: code-friendly encryption.*

Figure 8 shows the JPEG file sizes after encrypting different number of DCT coefficients. When the coefficients are fully encrypted, the file size rise linearly with the number of encrypted coefficients increasing. When all 64 coefficients in a JPEG block are encrypted fully, the file size increases up to 2.5 times of the original file size approximately. The larger the face regions are, the larger the increasing factor is. When the coefficients are coding-friendly encrypted, the file size remains nearly constant as expected.

Conclusion

In this paper a privacy-preserving forensic scheme for JPEG images is proposed. A key management protocol is proposed based on three predefined roles, which ensures that the privacy critical regions can only be accessed by certain parties under the approval of trusty parties. Partial encryption technology is applied to encrypt the privacy critical regions locally and individually. The proposed scheme allows privacy-preserving access to images with a fair trade-off between interests of investigators and subjects of investigations. It places a third party, *the prosecutor*, between *the investigator* and the encrypted image and thereby enforces the widely accepted four-eye-principle.

Acknowledgments

This work was supported by the German Federal Ministry of Education and Research (BMBF) as well as by the Hessen State Ministry for Higher Education, Research and the Arts (HMWK) within CRISP.

References

[1] A. Aminnezhad, A. Dehghantanha, and M. T. Abdullah. A survey on privacy issues in digital forensics. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 1(4):311–323, 2012.

[2] S. Srinivasan. Security and privacy in the computer forensics context. In *2006 International Conference on Communication Technology*, pages 1–3, Nov 2006.

[3] C. W. Adams. Legal issues pertaining to the development of digital forensic tools. In *2008 Third International Workshop on Systematic Approaches to Digital Forensic Engineering*, pages 123–132, May 2008.

[4] S. Hou, T. Uehara, S. M. Yiu, L. C. K. Hui, and K. P. Chow. Privacy preserving multiple keyword search for confidential investigation of remote forensics. In *2011 Third International Conference on Multimedia Information Networking and Security*, pages 595–599, Nov 2011.

[5] Frederik Armknecht and Andreas Dewald. Privacy-preserving email forensics. Technical Report CS-2015-03, Department Informatik, 2015.

[6] A. Peter, T. Hartmann, S. Mller, and S. Katzenbeisser. Privacy-preserving architecture for forensic image recognition. In *2012 IEEE International Workshop on Information Forensics and Security (WIFS)*, pages 79–84, Dec 2012.

[7] Patrick Stahlberg, Gerome Miklau, and Brian Neil Levine. Threats to privacy in the forensic analysis of database systems. In *Proceedings of the 2007 ACM SIGMOD International Conference on Management of Data*, SIGMOD '07, pages 91–102, New York, NY, USA, 2007. ACM.

[8] Jayanta Mondal and Debabala Swain. A contemplator on topical image encryption measures. In *Security Breaches and Threat Prevention in the Internet of Things*, pages 189–212. IGI Global, 2017.

[9] Akram Belazi, Ahmed A. Abd El-Latif, Adrian-Viorel Diaconu, Rhouma Rhouma, and Safya Belghith. Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. *Optics and Lasers in Engineering*, 88:37 – 50, 2017.

[10] A. Goel and K. Chaudhari. Median based pixel selection for partial image encryption. In *2016 Sixth International Conference on Image Processing Theory, Tools and Applications (IPTA)*, pages 1–5, Dec 2016.

[11] Marc Van Droogenbroeck and Raphael Benedett. Techniques For A Selective Encryption Of Uncompressed And Compressed images. In *Proceedings of Advanced Concepts for Intelligent Vision Systems (ACIVS)*, 2002.

[12] J. M. Rodrigues, W. Puech, and A. G. Bors. Selective Encryption of Human Skin in JPEG Images. In *2006 International Conference on Image Processing*, pages 1981–1984, October 2006.

[13] W. Wen, Y. Zhang, Y. Fang, and Z. Fang. A novel selective image encryption method based on saliency detection. In *2016 Visual Communications and Image Processing (VCIP)*, pages 1–4, Nov 2016.

[14] Martin Steinebach, Huajian Liu, Richard Stein, and Felix Mayer. Hybrid image encryption. *Electronic Imaging*, January 2018.

[15] William B. Pennebaker and Joan L. Mitchell. *JPEG Still Image Data Compression Standard*. Kluwer Academic Publishers, Norwell, MA, USA, 1st edition, 1992.

Author Biography

Huajian Liu *received his B.S. and M.S. degrees in electronic engineering from Dalian University of Technology, China, in 1999 and 2002, respectively, and his Ph.D. degree in computer science from Technische Universität Darmstadt, Germany, in 2008. He is currently a senior research scientist at Fraunhofer Institute for Secure Information Technology. His major research interests include information security, digital watermarking, robust hashing and digital forensics.*

Martin Steinebach *is the manager of the Media Security and IT Forensics division at Fraunhofer SIT. From 2003 to 2007 he was the manager of the Media Security in IT division at Fraunhofer IPSI. In 2003 he received his PhD at the Technische Universität Darmstadt for this work on digital audio watermarking. Since 2016 he is honorary professor of Technische Universität Darmstadt.*

Felix Mayer *received his master's degree in computer science from TU Darmstadt, Germany in 2016. Since then he has worked in the Media Security and IT Forensics department at Fraunhofer Institute for Secure Information Technology (SIT) in Darmstadt, Germany. His work has focused on object detection and data triage.*