Image Analysis and Processing in the Encrypted Domain

Pauline Puteaux, William Puech

IMAGE ANALYSIS AND PROCESSING IN THE ENCRYPTED DOMAIN

Pauline Puteaux, Ph.D. thesis directed by William Puech

LIRMM, CNRS, Univ. Montpellier, France

ABSTRACT

In this research project, we are interested by finding solutions to the problem of image analysis and processing in the encrypted domain. For security reasons, more and more digital data are transferred or stored in the encrypted domain. However, during the transmission or the archiving of encrypted images, it is often necessary to analyze or process them, without knowing the original content or the secret key used during the encryption phase. We propose to work on this problem, by associating theoretical aspects with numerous applications. Our main contributions concern: data hiding in encrypted images, correction of noisy encrypted images, recompression of crypto-compressed images and secret image sharing.

***Index Terms*—** Multimedia security, image encryption, signal processing in the encrypted domain.

1. INTRODUCTION

Digital image security plays a significant role in all fields, especially in highly confidential applications such as in the military and medical fields. With the development of cloud computing, the growth in information technology has led to serious security problems. The aim of encryption methods is to guarantee data privacy and confidentiality by fully or partially randomizing the content of original images. During the transmission or the archiving of encrypted images, it is often necessary to analyze or to process them without knowing the original content, or the secret key used during the encryption phase. Many applications exist, such as secret image sharing (SIS), research and indexing in encrypted databases, reversible data hiding in encrypted images (RDHEI), correction of noisy encrypted images, or recompression of crypto-compressed images.

In this paper, we present the results obtained during the two first years of this Ph.D. thesis. In Section 2, we describe our new method of RDHEI based on MSB-prediction. Then, we explain how to perform a significant Shannon entropy measurement in a pixel block of small size and give two possible applications using this statistical metric in Section 3. In Section 4, we propose a solution to recompress JPEG crypto-compressed images, without knowing the secret key used during encryption. Section 5 presents our privacy protection for social media based on a hierarchical secret image sharing scheme. Finally, the conclusion is drawn and future work is proposed in Section 6.

2. MSB-BASED REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES

Reversible data hiding in encrypted images (RDHEI) is an effective technique to embed data in the encrypted domain. An original image is encrypted with a secret key and during or after its transmission, it is possible to embed additional information in the encrypted image, without knowing the encryption key or the original content of the image. During the decoding process, the secret message can be extracted and the original image can be reconstructed.

We have proposed a new method based on MSB prediction with a very high embedding capacity. This is one of the first methods which proposes to use MSB instead of LSB for RDHEI. Due to the fact that MSB prediction is easier than LSB prediction in original domain and because image quality deterioration is not a problem in the encrypted domain, we are then able to have a very high capacity. By analyzing the original content of the image, the prediction errors are highlighted and an error location binary map is built. In a first approch, the original image is slightly modified in order to avoid all the prediction errors. After that, by substituting all MSB in the image, it is possible to hide one bit per pixel. In addition to this maximal payload equal to 1 bpp, the reconstructed image quality is high (SSIM close to 1 and PSNR $= 57.4\ dB$ on the average). Moreover, in a second approach, information about the location of the prediction errors is stored in the encrypted image according to the error location binary map. Note that using overhead such an additional map is not necessary for this proposed approach. Rather than that, we used some MSB values instead of embedding bits from the hidden message. Thus, by substituting most of the MSB values in the encrypted image, a large message can be hidden (payload close to 1 bpp) and during the decoding phase, the original image can be recovered losslessly (PSNR $\rightarrow +\infty$). This work has been presented in a conference paper [1] first and then, in an extended journal version [2].

Recently, we have improved the approach based on the storage of the prediction error location information by using recursively other bit-planes, from MSB to LSB as long as it is possible. Indeed, depending on the image content, bit-planes can easily be predicted, and so most of them can be substituted by bits of a secret message. According to the obtained results, the payload can be much higher than 1 bpp (median equal to 1.749 bpp, on average 1.836 bpp, and 5.408 bpp in the best case), while preserving perfect reversibility [3].

3. SHANNON ENTROPY MEASUREMENT IN PIXEL BLOCKS OF VERY SMALL SIZE

Introduced by Shannon in 1948, entropy measures the expected value of the information contained in a message. If we consider a block B of k pixels in an image of l grey-levels, local entropy is increased by the minimal value between its block-size k and the number of grey-levels l.

We have designed another method of RDHEI, where a local Shannon entropy analysis is performed in order to reconstruct the original image without error from the marked encrypted image. As zero-order entropy value in a block of pixels in a clear image is generally smaller than the value in the encrypted domain, it is possible to know if a block has been correctly decrypted or not during the decoding phase. However, there are some misconfigurations when blocks in the clear domain are highly textured. In this case, entropy value in the clear domain can be close to the values measured for badly decrypted configurations (and even higher), in particular when we consider very small block-sizes. A first idea to reduce the number of misconfigurations is to adapt the number of grey-levels by image quantization. Moreover, using distance map entropy, results are significantly improved, since we exploit the natural correlation between neighboring pixels in the clear domain. This work has been published in [4].

Another application is noisy encrypted image correction. Indeed, encrypted data can be damaged during its transmission through a noisy channel. Even if the secret key is known during the decryption phase, it becomes difficult to reconstruct the original image without errors. In order to deal with this problem, for each block of a noisy encrypted image, we have explained how to define the set of the possible correct configurations in clear, using local entropy measurements [5].

4. RECOMPRESSION OF JPEG CRYPTO-COMPRESSED IMAGES

In the clear domain, JPEG images can be recompressed with the aim to be adapted to limited bandwidth or storage. The problem lies in applying recompression in the encrypted domain. In fact, direct JPEG recompression of crypto-compressed images does not allow decryption.

We have proposed a method allowing to recompress crypto-compressed JPEG images, which is efficient in the encrypted domain. From our knowledge, this is one of the first methods allowing recompression directly in the encrypted domain, without knowing the secret key. Recompression step consists mainly in dividing by two each quantized encrypted DCT coefficient. In fact, the least significant bit of the non-zero quantized encrypted coefficients are thus removed, and zero coefficients are then encoded in the run-length of the next non-zero coefficients. For the decoding, the coefficients of the quantization table are adapted in consequence, by multiplying them by two. In our experiments, we have seen that this recompression operation achieves a very good trade-off between the compression rate and the image quality. Moreover, unlike standard recompression with JPEG, the recompressed image with an estimated quality factor EQF^* is strongly similar to the JPEG image obtained with a direct JPEG compression with the equivalent quality factor QF. There are no artifacts, such as grainy effects or an important loss of sharpness. In order to make this recompression operation possible in the encrypted domain, the crypto-compression step is adapted. In fact, quantized DCT coefficients are encrypted according to their size, from the largest to the smallest, in order to avoid desynchronization during the decryption phase. Furthermore, in the crypto-compressed image, the main content of the original image is kept secret, as indicated by a PSNR close to $10\ dB$. Note that, after recompression, visual confidentiality is still preserved, because our recompression method does not introduce security leaks. Therefore, in addition to offering a strong level of security, the proposed used encryption procedure is format-compliant and does not introduce overhead. This work has been presented in a journal paper [6].

5. PRIVACY PROTECTION FOR SOCIAL MEDIA

Social network development raises many issues relating to privacy protection for images. In particular, multi-party privacy protection conflicts can take place when an image is published by only one of its owners. Indeed, privacy settings applied to this image are those of its owner and people on the image are not involved in the process.

We have proposed a new hierarchical secret image sharing scheme for social networks in order to answer this problem [7]. Based on the disjunctive multi-level approach of Belenkiy applied to images, this solution ensures user privacy. By mutual agreement, n users choose to allow clear visualization of all the regions of interest (ROI) when at least k of them allowed the entire reconstruction. If this threshold is not met, only the ROI associated to users who participate in the reconstruction are revealed, with the help of a public share. According to our experimental results, our approach is efficient in terms of uses in real situations and in terms of security.

6. CONCLUSION

In this paper, I have presented the main contributions of the two first years of my Ph.D. thesis focused on image analysis and processing in the encrypted domain. Four different related applications have been discussed: MSB-based RDHEI, entropy measurement in small blocks, recompression of JPEG crypto-compressed images and privacy protection for social media. In future work, we first aim to improve the obtained results. Furthermore, we will work on the use of homomorphic cryptography for data hiding and features extraction in the encrypted domain.

7. REFERENCES

[1] P. Puteaux, D. Trinel, and W. Puech, "High-capacity data hiding in encrypted images using MSB prediction," in *Image Processing Theory Tools and Applications (IPTA), 2016 International Conference on*. IEEE, 2016, pp. 1–6.

[2] P. Puteaux and W. Puech, "An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 7, pp. 1670–1681, 2018.

[3] P. Puteaux and W. Puech, "EPE-based huge-capacity reversible data hiding in encrypted images," in *2018 IEEE International Workshop on Information Forensics and Security (WIFS)*. IEEE, 2018, pp. 1–7.

[4] P. Puteaux and W. Puech, "Reversible data hiding in encrypted images based on adaptive local entropy analysis," in *Image Processing Theory, Tools and Applications (IPTA), 2017 International Conference on*. IEEE, 2017, pp. 1–6.

[5] P. Puteaux and W. Puech, "Noisy encrypted image correction based on shannon entropy measurement in pixel blocks of very small size," in *2018 European Signal Processing Conference (EUSIPCO)*, 2018, pp. 161–165.

[6] V. Itier, P. Puteaux, and W. Puech, "Recompression of JPEG crypto-compressed images without a key," *IEEE Transactions on Circuits and Systems for Video Technology*, 2019.

[7] S. Beugnon, P. Puteaux, and W. Puech, "Privacy protection for social media based on a hierarchical secret image sharing scheme," in *2019 IEEE International Conference on Image Processing (ICIP)*. IEEE, 2019.