A review of data preprocessing modules in digital image forensics methods using deep learning

Alexandre Berthet
Department of Digital Security
Eurecom
Email: berthet@eurecom.fr

Jean-Luc Dugelay
Department of Digital Security
Eurecom
Email: dugelay@eurecom.fr

***Abstract*—Access to technologies like mobile phones contributes to the significant increase in the volume of digital visual data (images and videos). In addition, photo editing software is becoming increasingly powerful and easy to use. In some cases, these tools can be utilized to produce forgeries with the objective to change the semantic meaning of a photo or a video (e.g. fake news). Digital image forensics (DIF) includes two main objectives: the detection (and localization) of forgery and the identification of the origin of the acquisition (i.e. sensor identification). Since 2005, many classical methods for DIF have been designed, implemented and tested on several databases. Meantime, innovative approaches based on deep learning have emerged in other fields and have surpassed traditional techniques. In the context of DIF, deep learning methods mainly use convolutional neural networks (CNN) associated with significant preprocessing modules. This is an active domain and two possible ways to operate preprocessing have been studied: prior to the network or incorporated into it. None of the various studies on the digital image forensics provide a comprehensive overview of the preprocessing techniques used with deep learning methods. Therefore, the core objective of this article is to review the preprocessing modules associated with CNN models.**

I. Introduction

Today, images and videos play a key role in digital communication and whether they are of personal (social network), legal (trial) or security (surveillance, police investigation) origin, they can be employed as evidence. Therefore, the confirmation of their origin and authenticity is a crucial aspect to avoid any malicious use. However, since editing software is easy to access and use, forged content is becoming more common and increasingly difficult for humans to distinguish. Digital Image Forensics (DIF [40]) provides tools for blindly analysing images and gives information about their authenticity, whether is to detect forgeries or to identify the camera model. This is achieved through the analysis of the artifacts that remain in the digital image during the creation process, which consists of three stages: acquisition, post-processing and storage.

These traces are caused either by the camera that captured the photo or by modifications performed on the picture. They can be grouped into four various classes. Camera-based techniques, which exploit the artifacts introduced during the acquisition stages: the camera lens [1], [2], the sensor [3], [4] or the colour filter array (CFA) [5], [6]. Each of the elements in this pipeline plays a key role in digital image acquisition. The camera lens transmits the light from the scene to the sensor at a unique point and transforms it into pixels. The CFA assigns a specific colour to each pixel, in the first place through a colour mosaic and then through an RGB representation by interpolation. This thorough process produces some artifacts due to imperfections in the camera model that captures the image. Therefore, these techniques are principally exploited to identify the camera model as in [2], [3], [4]. They can also detect falsifications applied to the content of an image as in [1], [5], [6], [7]. Pixel-based techniques, which detect changes in the picture at the pixel level. The main manipulations studied are: splicing, which merges part of an image A into an image B; cloning also named copy-move [8], [9], which copies part of a picture on itself; resampling [10], which is frequently used to match (resize, rotate, etc.) a tampered region to an image. These falsifications provide artifacts that can be used to detect altered images. However, these artifacts can be hidden by applying specific techniques, either to mask the forgeries or to enhance the image. Therefore, some detection methods are focused on manipulations like in [11] where noise inconsistencies are exploited. Techniques based on geometry and physics, which capture the inconsistencies that could be created in a forgery. When an image is altered, by adding or removing an element, real-life characteristics are rarely maintained. Indeed, light (2-D, 3-D, environmental) or geometric parameters are generally neglected in falsifications, and this can be exploited to detect them: [12], [13]. In addition, lighting inconsistencies can help to detect forged images as in [14]. Format-based techniques, which use information from a specific compression. For example, during the quantization step, blocks of pixels are converted in frequency space by the discrete cosine transform (DCT). Anomalies can be introduced in the DCT coefficients [15] and also in the JPEG block [16], [17]. After a forgery, the image can be recompressed and some inconsistencies may appear (e.g., in the JPEG block or quantization matrix) [18], [19], [20].

In recent years, many image processing tasks have made use of deep learning methods, including CNN models. Notably, the performance achieved for classification challenge like ILSVRC [41] has proved the efficiency of such approaches. Therefore, some domains of image processing like face recognition [42] or steganalysis [43] have adopted deep learning methods. However, there are differences between both examples. Notably, for face recognition, digital images are directly transmitted to the network that learns the pixel features. In the case of steganalysis, a preprocessing step based on the SRM filters is applied [43]. Digital image forensics is closer

to this domain than face recognition. In a preliminary study, Chen *et al.* attempted to directly authenticate raw pictures with a deep learning method [22]. However, CNN models do not learn the key statistical properties relevant to image forensics. This means that the localization of forgeries or any other type of image forensics analysis cannot be carried out with traditional deep learning techniques. In fact, classical methods (i.e. without deep learning) are always based on relevant artifacts to detect tampering. Consequently, the equivalent process for CNN models is the extraction of the traces left by alterations. This preprocessing step is crucial because without it, the network only learns features from the image content. This process leads to disappointing performance in forgery detection. To correctly authenticate images, it must learn about hidden artifacts, i.e. those that are overshadowed by the image content. Preprocessing is therefore a required step in deep learning methods. According to existing surveys on DIF, only one deals with deep learning methods. However, it is restricted to copy-move operation and only one single subsection. This paper is the first review on preprocessing applied to deep learning-based methods for authenticating camera or detecting falsifications. The following sections will present two ways to apply this crucial step.

II. Handcrafted techniques

Handcrafted preprocessing is used prior to the CNN, without self-learned features extraction. In fact, this process is close to classical algorithms (i.e. without deep learning) that use handcrafted features to detect some forgeries. Various techniques are employed in the main state-of-art publications as residuals (noise or median filtering) or DCT coefficients histograms.

Noise residuals are one of the main artifacts extracted during the preprocessing phase. Each image has a specific noise due to the camera that captured it and the operations applied to the content. Indeed, an alteration frequently produces noise, whether for hiding a previous operation or modifying the image. These residuals can therefore be used as an element for any process (e.g. forgery detection, camera identification). However, these traces are often overshadowed by the image content. Regardless the type of denoising filter, the method to obtain noise residuals is similar. It consists in subtracting the denoised image $F(I)$ from the original image I to get the desired artifact $\tilde{I}$ (Eq. 1).

$$\tilde{I}_n = I_n - F(I_n) \tag{1}$$

Chen *et al.* implemented the first preprocessing approach for DIF with deep learning [22]. This technique is also based on filtering (median filtering residuals). It aims to remove interference from irrelevant information, which are the edges and textures of the image. The process is almost the same as for the application of a denoising filter. The residuals $d(i,j)$ are the results of the difference between the output $y(i,j)$, obtained by applying a $w \times w$ median filtering window on the image $x(i,j)$, and the image (Eq. 2).

$$d(i,j) = med_w(x(i,j)) - x(i,j) = y(i,j) - x(i,j) \tag{2}$$

Applying a high-pass filter (HPF) [31] represents a dual way to isolate the noise from the image. Different HPF have been used in the state-of-art articles. Pengpeng *et al.* [32] applied a Laplacian filter (3×3), usually used for edge detection, on small size patches (64×64) to detect recaptured images. Indeed, the Laplacian filter is dedicated to the identification of regions with rapid changes in intensity. Therefore, this technique is sensitive to noise as it causes a wave effect on the image. The steganalysis rich model (SRM) [33] is based on 30 basic high-pass filters, with non-linear operations, from seven groups ($1^{st}, 2^{nd}, 3^{rd}$ orders, EDGE and SQUARE 3×3 and 5×5). They are employed in the calculation of residual maps, and their results can be considered as a local noise descriptor. In [25], Kim *et al.* exploit one of them (SQUARE 5×5, eq. 3) as the input was on a single channel. In comparison, Zhou *et al.* use three of them [23] as their input was in RGB (2^{nd} order, SQUARE 3×3 and 5×5). In both cases, they used as few filters as possible to reduce the computing time. The same HPF (SQUARE 5×5, eq. 3) is compared, in [29], to a wavelet-based filter [34]. Tuama *et al.* proved through their experiments that the SRM filter performs better than the wavelet one.

$$F_{sqrt5} = \frac{1}{12} * \begin{bmatrix} -1 & 2 & -2 & 2 & -1 \\ 2 & -6 & 8 & -6 & 2 \\ -2 & 8 & \textbf{-12} & 8 & -2 \\ 2 & -6 & 8 & -6 & 2 \\ -1 & 2 & -2 & 2 & -1 \end{bmatrix} \tag{3}$$

In the article [27], the method of Wang *et al.* is based on histograms of DCT coefficients, mainly used to detect recompressed images. In fact, after a forgery, the tampered image is usually stored again by applying another compression with a different quality factor. This affects the distribution of DCT coefficient histograms. The histograms follow approximately a generalized Gaussian distribution (regardless of the quality factor). This phenomenon occurs for single compression whereas the histograms reveal some inconsistencies for double compression. These anomalies depend on the quality factors used for the two steps: if QF1 (1^{st} compression quality factor) is greater than QF2 (2^{nd} compression quality factor) there will be peaks and valleys in the histogram and missing values for the opposite (i.e. QF2 greater than QF1). These differences illustrate the application of a recompression and the consequence of a potential alteration. In the article, Wang *et al.* detail the different steps of this process and explain the advantages of their method. In fact, they specify a fixed interval that solves the problem of the variable size of the DCT histograms and reduces the calculation with a negligible loss of information. This technique is also exploited in [30], but with a different interval size (vectors of size 909×1 and 9×11 for [27]). Barni *et al.* detail a "CNN Embedding DCT Histograms" [36] that includes a first step devoted to preprocessing and also based on DCT coefficients histograms. The network is fed with small raw patches (64×64) that are then handled in a preprocessing phase. This preprocessing step extracts self-learned artifacts without accessing to pixel values. Even if the network can be considered as end-to-end, the preprocessing is somewhat equivalent to handcrafted technique as it is not impacted by the training phase. It is therefore an intermediate step between the techniques carried out prior to the network and those incorporated into it.

III. Network incorporated techniques

The second type of techniques is implemented in the network and is subject to the training phase. Unlike the previous

ones, these methods automatically extract features within the model. The extraction is applied in the first convolutional layer by modifying its weights. Therefore, the first layer is considered as a preprocessing layer. In fact, the network is forced to learn particular artifacts that cause the difference with standard models.

In [39], Cozzolino *et al.* explain how to recast a residual-based local descriptor into a CNN. Foremost, the processing chain of a residual-based local descriptor consists of several steps. Only the first, dedicated to the extraction of noise residuals, is interesting for preprocessing. This phase is usually performed with a high-pass filter to spotlight the relevant artifacts. The conversion of this model into a CNN was in two phases: from local features to a Bag-of-Features paradigm and then to a CNN. However, only the extraction of artifacts is related to preprocessing. In fact, the noise residuals R are obtained by a group of shifted filters. It corresponds to a bank of *N* filters in the case of the Bag-of-Features and then to a convolutional layer in the case of the CNN. The *N* filters corresponds to zero windows with non-zero weights ($[\ 1 \quad -3 \quad 3 \quad -1\ ]$) on the *n*-row. Finally, they replaced these filters by a convolutional layer that calculate the residuals with the same filter coefficients.

Rao *et al.* described in [38] another technique, influenced by steganalysis [33], using the weights of the first convolutional layer of the network. The filters used in the calculation of the residual maps were also applied in the handcrafted preprocessing method [23]. Instead of only three, this technique exploits 30 basic high-pass filters, from seven classes c_i, to initialise the weight of the convolutional layer. The output of this first layer is a set of 30 feature maps. In the case of an RGB input (three color channels), the outputs are obtained with three filters (from SRM). Rao *et al.* explain that for optimal results, the three filters used for the feature maps must be of the same class but not identical. Therefore, the initialization strategy consists in associating a set of three filters to each feature map. The application of SRM filters, even for weight initialization, spotlights sharp edges that are introduced by tampering operations like splicing. In addition, Rao *et al.* stated that this initialization accelerates the convergence of the network.

Finally, the last preprocessing technique introduced in the litterature is also a modification of the first convolutional layer. Bayar *et al.* proposed an innovative approach [37], the constrained convolutional layer. The CNN is forced to learn features for detection of manipulations through the first layer that has been modified. The key of this process is still the same as presented previously with other preprocessing techniques: isolating the artifacts that are overshadowed by the image content. Therefore, the task of this constrained convolutional layer is to remove irrelevant information, which is achieved by updating the weights. The precise artifacts retained by this preprocessing layer are prediction error filters that provides the value of the central pixel of the filter window. The weights w of each filter K are forced as follows: the center value is fixed to -1 while the sum of the remaining pixels is set to 1 (Eq 4).

$$\begin{cases} w_k(0,0) = -1 \\ \sum_{l,m \neq 0} w_k(l,m) = 1 \end{cases} \tag{4}$$

This constraint is applied during the training part of the network with a particular sequence. The weights of each filter are initialized randomly as it is usually the case. Then, a two-step iterative process is started with the back-propagation until the value of the loss function is reached: the weights are first forced by the constraint and then updated according to the stochastic gradient descent (SGD). Bayar *et al.* have published a series of articles, based on this new layer, improving continuously their model. One of them [35] represents an innovation of the preprocessing layer. It exploits a dual-flow filtering layer to capture prediction error filters, as before, but also non-linear artifacts. The input image, of size $256 \times 256 \times 2$ is handled separately by each pre-processing step. It passes through the constrained convolutional layer and is processed in parallel first with a residual median filter and then with an identity convolutional layer. Both outputs are then merged with a concatenated layer. Therefore, this preprocessing technique provides more artifacts and so a more accurate extraction of features.

IV. Conclusion

Contrary to other domains as face recognition for example, DIF is at the early stages of the adoption of deep learning methods. Some preprocessing techniques are inspired by steganalysis like the use of the SRM filters. In fact, the goal is to put forward the artifacts dedicated to digital image forensics as it is done with classical methods. Therefore, the typical preprocessing techniques are based on noise residuals or compression traces. This review proves that preprocessing represents an essential step for authenticating cameras or detecting forged images, whatever applied prior to the network or embedded in it. However, techniques used inside the network benefit from the computing power of GPU that are used with deep learning methods. In addition, they are utilized in state-of-art articles, and it could be interesting to observe the impact of each preprocessing on the global performance of the models. The results could provide a comparison between deep learning and classical methods but also between several preprocessing techniques. Therefore, an upcoming work could consist in examining results of deep learning models for DIF to develop a comprehensive overview.

Acknowledgment

This work was supported by the DEFACTO (Automated detection of digital images falsifications) consortium (UTT, Eurecom and Surys) that participates to the French challenge DEFALS (DEtection of FALSifications in images and videos).

References

[1] Micah K. Johnson and Hany Farid. 2006. Exposing digital forgeries through chromatic aberration. In Proceedings of the 8th workshop on Multimedia and security. Association for Computing Machinery, New York, NY, USA, 48–55. doi:https://doi.org/10.1145/1161366.1161376

[2] L. T. Van, S. Emmanuel and M. S. Kankanhalli, "Identifying Source Cell Phone using Chromatic Aberration," 2007 IEEE International Conference on Multimedia and Expo, Beijing, 2007, pp. 883-886, doi: 10.1109/ICME.2007.4284792.

[3] J. Lukas, J. Fridrich and M. Goljan, "Digital camera identification from sensor pattern noise," in IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 205-214, June 2006, doi: 10.1109/TIFS.2006.873602.

[4] M. Chen, J. Fridrich, M. Goljan and J. Lukas, "Determining Image Origin and Integrity Using Sensor Noise," in IEEE Transactions on Information Forensics and Security, vol. 3, no. 1, pp. 74-90, March 2008, doi: 10.1109/TIFS.2007.916285.

[5] S. Bayram, H. Sencar, N. Memon and I. Avcibas, "Source camera identification based on CFA interpolation," IEEE International Conference on Image Processing 2005, Genova, 2005, pp. III-69, doi: 10.1109/ICIP.2005.1530330.

[6] A. C. Popescu and H. Farid, "Exposing digital forgeries in color filter array interpolated images," in IEEE Transactions on Signal Processing, vol. 53, no. 10, pp. 3948-3959, Oct. 2005, doi: 10.1109/TSP.2005.855406.

[7] B. Mahdian and S. Saic, "Blind Authentication Using Periodic Properties of Interpolation," in IEEE Transactions on Information Forensics and Security, vol. 3, no. 3, pp. 529-538, Sept. 2008, doi: 10.1109/TIFS.2004.924603.

[8] S. Bayram, H. Taha Sencar and N. Memon, "An efficient and robust method for detecting copy-move forgery," 2009 IEEE International Conference on Acoustics, Speech and Signal Processing, Taipei, 2009, pp. 1053-1056, doi: 10.1109/ICASSP.2009.4959768.

[9] Popescu, Alin C. and Hany Farid. "Exposing Digital Forgeries by Detecting Duplicated Image Regions."

[10] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," in IEEE Transactions on Signal Processing, vol. 53, no. 2, pp. 758-767, Feb. 2005, doi: 10.1109/TSP.2004.839932.

[11] Babak Mahdian, Stanislav Saic, "Using noise inconsistencies for blind image forensics", in Image and Vision Computing,Volume 27, Issue 10, 2009, Pages 1497-1503, ISSN 0262-8856, https://doi.org/10.1016/j.imavis.2009.02.001.

[12] Micah K. Johnson and Hany Farid. 2005. Exposing digital forgeries by detecting inconsistencies in lighting. In Proceedings of the 7th workshop on Multimedia and security. Association for Computing Machinery, New York, NY, USA, 1–10. DOI:https://doi.org/10.1145/1073170.1073171

[13] M. K. Johnson and H. Farid, "Exposing Digital Forgeries in Complex Lighting Environments," in IEEE Transactions on Information Forensics and Security, vol. 2, no. 3, pp. 450-461, Sept. 2007, doi: 10.1109/TIFS.2007.903848.

[14] Asati, Shraddha and Pardhi, P.R. (2014). Exposing Digital Image Forgeries by Illumination Color Classification. International Journal of Engineering Trends and Technology. 18. 269-271. 10.14445/22315381/IJETT-V18P255.

[15] Zhouchen Lin, Junfeng He, Xiaoou Tang, Chi-Keung Tang, "Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis", in Pattern Recognition, Volume 42, Issue 11, 2009, Pages 2492-2501, ISSN 0031-3203, https://doi.org/10.1016/j.patcog.2009.03.019.

[16] S. Ye, Q. Sun and E. Chang, "Detecting Digital Image Forgeries by Measuring Inconsistencies of Blocking Artifact," 2007 IEEE International Conference on Multimedia and Expo, Beijing, 2007, pp. 12-15, doi: 10.1109/ICME.2007.4284574.

[17] H. Farid, "Exposing Digital Forgeries From JPEG Ghosts," in IEEE Transactions on Information Forensics and Security, vol. 4, no. 1, pp. 154-160, March 2009, doi: 10.1109/TIFS.2008.2012215.

[18] F. Huang, J. Huang and Y. Q. Shi, "Detecting Double JPEG Compression With the Same Quantization Matrix," in IEEE Transactions on Information Forensics and Security, vol. 5, no. 4, pp. 848-856, Dec. 2010, doi: 10.1109/TIFS.2010.2072921.

[19] W. Luo, Z. Qu, J. Huang and G. Qiu, "A Novel Method for Detecting Cropped and Recompressed Image Block," 2007 IEEE International Conference on Acoustics, Speech and Signal Processing - ICASSP '07, Honolulu, HI, 2007, pp. II-217-II-220, doi: 10.1109/ICASSP.2007.366211.

[20] M. Kirchner and T. Gloe, "On resampling detection in re-compressed images," 2009 First IEEE International Workshop on Information Forensics and Security (WIFS), London, 2009, pp. 21-25, doi: 10.1109/WIFS.2009.5386489.

[21] Tan, Weijin et al. "A Survey on Digital Image Copy-Move Forgery Localization Using Passive Techniques." (2019).

[22] J. Chen, X. Kang, Y. Liu and Z. J. Wang, "Median Filtering Forensics Based on Convolutional Neural Networks," in IEEE Signal Processing Letters, vol. 22, no. 11, pp. 1849-1853, Nov. 2015, doi: 10.1109/LSP.2015.2438008.

[23] Zhou, Peng et al. "Learning Rich Features for Image Manipulation Detection." 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (2018).

[24] Zhang, Ying et al. "Image Region Forgery Detection: A Deep Learning Approach." SG-CRC (2016).

[25] Kim, Dong-Hyun and Hae-Yeoun Lee. "Image Manipulation Detection using Convolutional Neural Network." (2017).

[26] Yifeng Zhan, Yifang Chen, Qiong Zhang, and Xiangui Kang. 2017. "Image Forensics Based on Transfer Learning and Convolutional Neural Network". In Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security. Association for Computing Machinery, New York, NY, USA, 165–170. doi:https://doi.org/10.1145/3082031.3083250

[27] Wang, Qing and Zhang, Rong. (2016). Double JPEG compression forensics based on a convolutional neural network. EURASIP Journal on Information Security. 2016. 10.1186/s13635-016-0047-y.

[28] J. Bunk et al., "Detection and Localization of Image Forgeries Using Resampling Features and Deep Learning," 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Honolulu, HI, 2017, pp. 1881-1889, doi: 10.1109/CVPRW.2017.235.

[29] A. Tuama, F. Comby and M. Chaumont, "Camera model identification with the use of deep convolutional neural networks," 2016 IEEE International Workshop on Information Forensics and Security (WIFS), Abu Dhabi, 2016, pp. 1-6, doi: 10.1109/WIFS.2016.7823908.

[30] Amerini, Irene et al. "Localization of JPEG Double Compression Through Multi-Domain Convolutional Neural Networks." 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2017).

[31] Yinlong Qian, Jing Dong, Wei Wang, Tieniu Tan, "Deep learning for steganalysis via convolutional neural networks," Proc. SPIE 9409, Media Watermarking, Security, and Forensics 2015, 94090J (4 March 2015); https://doi.org/10.1117/12.2083479

[32] Pengpeng, Yang Ni, Rongrong Zhao, Yao, "Recapture Image Forensics Based on Laplacian Convolutional Neural Networks", Lecture Notes in Computer Science. 10082. 119-128.(2017).

[33] J. Fridrich and J. Kodovsky, "Rich Models for Steganalysis of Digital Images," in IEEE Transactions on Information Forensics and Security, vol. 7, no. 3, pp. 868-882, June 2012, doi: 10.1109/TIFS.2012.2190402.

[34] Fridrich, J. "Digital Image Forensics Using Sensor Noise."

[35] B. Bayar and M. C. Stamm, "Augmented convolutional feature maps for robust CNN-based camera model identification," 2017 IEEE International Conference on Image Processing (ICIP), Beijing, 2017, pp. 4098-4102, doi: 10.1109/ICIP.2017.8297053.

[36] Barni, M. et al. "Aligned and Non-Aligned Double JPEG Detection Using Convolutional Neural Networks." Journal of Visual Communication and Image Representation 49 (2017): 153–163.

[37] Belhassen Bayar and Matthew C. Stamm. 2016. A Deep Learning Approach to Universal Image Manipulation Detection Using a New Convolutional Layer. In Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security. Association for Computing Machinery, New York, NY, USA, 5–10. doi:https://doi.org/10.1145/2909827.2930786

[38] Y. Rao and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images," 2016 IEEE International Workshop on Information Forensics and Security (WIFS), Abu Dhabi, 2016, pp. 1-6, doi: 10.1109/WIFS.2016.7823911.

[39] Cozzolino, Davide, Giovanni Poggi, and Luisa Verdoliva. "Recasting Residual-Based Local Descriptors as Convolutional Neural Networks." Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security (2017).

[40] Redi, J.A., Taktak, W. Dugelay, J. Digital image forensics: a booklet for beginners. Multimed Tools Appl 51, 133–162 (2011). https://doi.org/10.1007/s11042-010-0620-1

[41] Russakovsky, O., Deng, J., Su, H. et al. ImageNet Large Scale Visual Recognition Challenge. Int J Comput Vis 115, 211–252 (2015). https://doi.org/10.1007/s11263-015-0816-y

[42] Guodong Guo, Na Zhang, "A survey on deep learning based face recognition", Computer Vision and Image Understanding, Volume 189, 2019, 102805, ISSN 1077-3142, https://doi.org/10.1016/j.cviu.2019.102805.

[43] Marc Chaumont, "Deep Learning in steganography and steganalysis from 2015 to 2018", 2019, 1904.01444.