New Trends in Intelligent Software Methodologies, Tools and Techniques
H. Fujita and H. Perez-Meana (Eds.)
IOS Press, 2021

doi:10.3233/FAIA210010

Protecting the Sharing and Distribution of Color Images Hosted in Cloud Storage Services

Manuel CEDILLO-HERNANDEZ[a] [1], David MATA-MENDOZA[a], Diana NUÑEZ-RAMIREZ[a], Elizabeth CAMPOS-PONCE[a], Eduardo FRAGOSO-NAVARRO[a], Mariko NAKANO-MIYATAKE[a], Hector PEREZ-MEANA[a]
[a] Instituto Politecnico Nacional SEPI ESIME Culhuacan, Av. Santa Ana 1000 Culhuacan CTM V, 04440 CDMX, Mexico

Abstract. In recent years, the reversible data hiding techniques also known as lossless or invertible data hiding, has gradually become a very active research area. The reversibility of these schemes makes possible to extract the embedded data without errors, as well as to restore the cover medium to its original state. Furthermore, to guarantee the security and confidentiality of the hidden data and the image, reversible data hiding schemes over encrypted domain are presented as a promising solution to solve several issues of information security. This paper presents a study case of reversible data hiding schemes over encrypted domain oriented to the protection of the sharing and distribution of color images hosted in cloud storage services. The experimental results are presented in terms of imperceptibility, capacity, confidentiality, and visual quality, respectively.

Keywords. reversible data hiding in encrypted domain, information security, digital image processing, advanced encryption standard.

1. Introduction

In recent years, the reversible data hiding (RDH) techniques (also known as lossless or invertible data hiding) has gradually become a very active research area. The reversibility of RHD scemes makes possible to extract the embedded data without errors, as well as to restore the cover medium to its original state [1]. Over time, the proposals have been applied for digital media such as color and grayscale natural images, as well as digital audio and video. In this way, during the last two decades several RDH techniques have been reported in the scientific literature [1], where the main efforts, in a digital image context, are focused on: a) improving capacity of the methods, b) obtaining robustness against JPEG compression, c) concealing information meanwhile the contrast enhancement of the images is performed and d) hiding data before or after images encryption. In this way, to guarantee the security and confidentiality of the hidden data and the image respectively, reversible data hiding schemes over encrypted domain (RDH-ED) are presented as a promising solution to solve several issues of information security. In general terms, RDH-ED refers to embed

[1] Corresponding Author, Instituto Politecnico Nacional SEPI ESIME Culhuacan, Mexico; E-mail: mcedilloh@ipn.mx

additional data into encrypted images, with the ability to recover both the data and the original content of the image, respectively, which is expected to have wide application in the cloud computation into the real world, and the research in this attractive field will continue to move ahead [1-16]. Thus, RDH-ED is an emerging topic and according to Shi et al. in [1], has been: "*primarily driven by the needs from Cloud computing platforms and various privacy preserving applications"*, therefore, it has gained increasing attention. In this way, the conjunction of data hiding techniques and encryption of digital images focuses on embedding additional data in the encrypted domain in a reversible manner. In the scientific literature, several RDH-ED works have been reported [1-20] in Vacating Room Before Encryption (VRBE) and Vacating Room After Encryption (VRAE) modalities, respectively. At current, the efforts by the scientific community have been oriented to accomplish the following requirements: a) Obtain high capacity, measured in bits per pixel (bpp), b) Improve the confidentiality of the encrypted image with the secret message, c) Improve the visual quality of the approximate version of the original image, and d) Obtain the completely separability to be capable of extract the secret message either plaintext or encrypted domain, respectively.

According to the applications, these requirements will be satisfied to a greater or lesser extent possible [1-20]. In the following paragraphs, we describe an application scenario oriented to protect the sharing and distribution of color images hosted in cloud storage services.

2. Study case

To improve the information security in cloud storage services, this study case shows the use of RDH-ED in the protection of the sharing and distribution of color images collections. Considering an application scenario where a photographer stores its color images in a cloud storage service, before upload the image files to the cloud, he applies an RDH-ED method to each image.. Thus, the image is encrypted and visually unrecognized to unauthorized persons, and at the same time, control information is embedded into the same encrypted image. In this way, according to the managing of encrypted and data-hiding keys, the authorized persons can perform the tasks shown in Fig. 1.

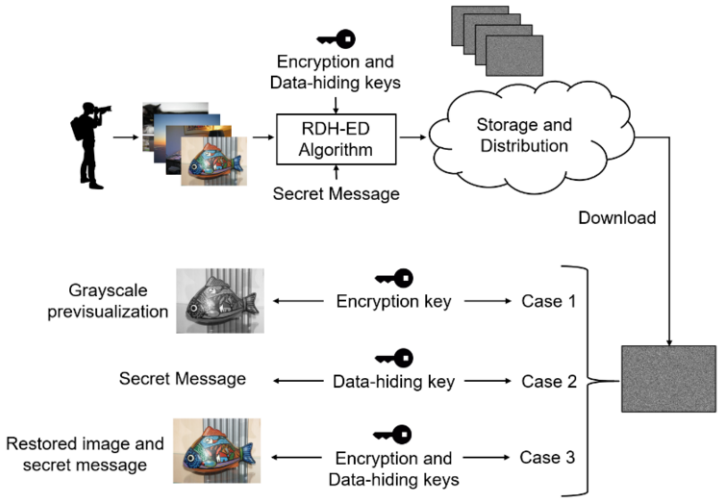

Figure 1. General diagram of the RDH-ED to protect the sharing and distribution of color images hosted in cloud storage services.

The proposed RDH-ED in this paper is an example of Vacating Room Before Encryption (VRBE) with data extraction and image recovery in encrypted domain, as shown in Fig. 2. In general terms, VRBE framework preserves an embedding room in the plaintext domain, i.e., vacating embedding room before encryption [1], [17-20]. In this way, the content-owner performs additional preprocessing before the image is ciphered. Some frequently used terms in RDH-ED are: *original content* which refer to the multimedia in plaintext format, the *encrypted content* which is obtained by applying ciphering to the original content, the *secret message* in binary format, the *marked encrypted content* which refer to the encrypted content with the secret message embedded in its data, the *approximate content* obtained by applying directly deciphering to the marked encrypted content and is a version close to the original content, the *restored content* which is the perfect version of the original content restored without any embedded data; and three entities called content-owner, data-hider and receiver.

2.1. Embedding stage

Preprocessing (Content-Owner). Given a color original image I, convert its red-green-blue (RGB) color model representation to luminance-chrominance (YCbCr) color model. Isolate the luminance information Y and chrominances Cb, Cr, respectively. One of the major issues in color image processing is to find the appropriate color model for the problem being addressed [21]. Whereas the application context often defines the original color model, particularly RGB model for color images; the color model used for data-hiding must be discussed according to the application scenario. According to [22], [23], the RGB color model has the most correlated components while the YCbCr color model components are the less correlated. Based on this fact, YCbCr is adopted as suitable color model in this RDH-ED method.

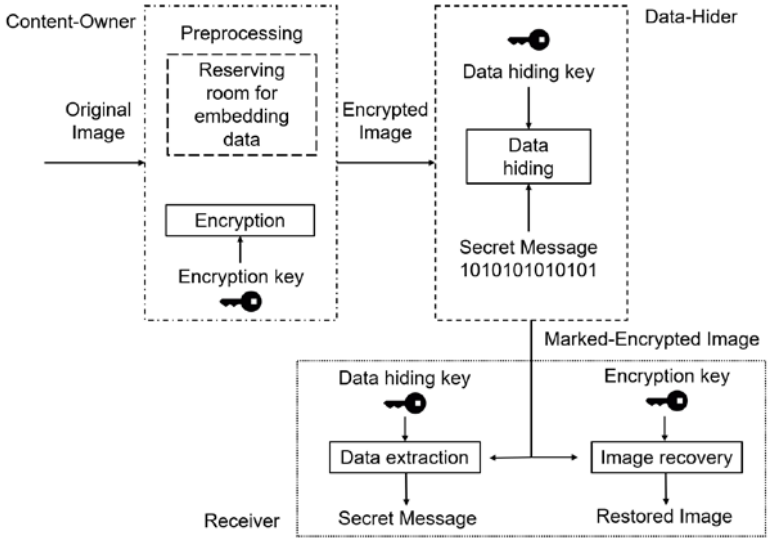

Figure 2. General diagram of VRBE framework.

Once the color information has been processed, from the luminance information Y select a region of interesting (ROI) composed by the 50% of the pixels in Y, for that RDH-ED algorithm be able to perform the reversibility and restoration of the color image. The rest of luminance information Y composes the region of non-interest (RONI). Once the ROI is selected, obtain its message digest denoted as H_{ROI} using the hash function SHA-1 [24], store the least significant bit (LSB) of each pixel of the ROI into LSB_{ROI} variable, store the first and last pixels of ROI into IND_{ROI} variable, and re-arrange the luminance information Y in a stack form, as shown in Fig. 3.

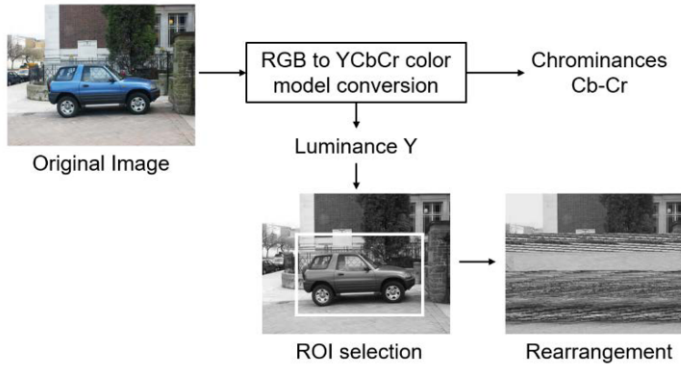

Fig. 3 Image preprocessing stage.

Image encryption (Content-Owner). This RDH-ED study case presented in this chapter employs the cryptography symmetric key method called stream cipher, which, operates on each pixel of the image bit to bit using the Boolean function or-exclusive. In this way, we configurate a block cipher to operates in a stream cipher mode, mainly OFB (Output Feedback) or CTR (Counter Mode). The most popular block cipher using in

several information security applications is the Rijndael [24], [25], contained in the Advanced Encryption Standard (AES) [26], which is not Feistel cipher and, in general terms, processes 128-bit blocks of plaintext with keys of 128, 192 or 256 bits, length that defines the number of rounds that executes the algorithm. In this way, once the luminance information Y is pre-processed, we apply the Rijndael algorithm to obtain the encrypted domain in which it will be concealed the secret message. To improve the confidentiality of the encrypted image E_{IMG}, in this step we perform a pixel permutation in a pseudorandom form using a secret key K_1, which, in conjunction with the block cipher key K_2 and the indexes into IND_{ROI}, compose the encryption key denoted as EK. An example of the output of this step is shown in Fig. 4.

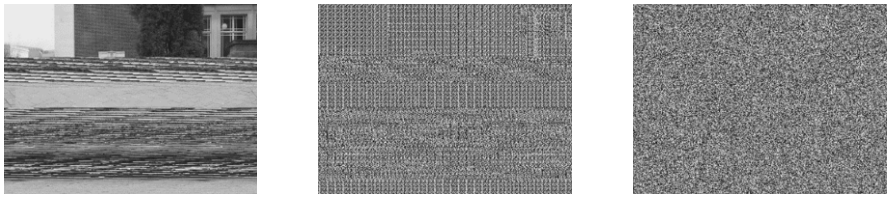

Fig. 4. (a) Luminance information pre-processed. (b) Result of apply Rijndael algorithm to (a) in CTR mode. (c) Result of apply pixel permutation to (b).

Data hiding (Data-Hider). Once the encrypted image E_{IMG} is obtained, the secret message will be embedded into E_{IMG}. To accomplish the ability of the algorithm to perform the tasks shown in Fig. 1, the secret message SM is composed by two binary strings denoted as SM_{ROI} (that contains the message digest denoted as H_{ROI} to verify the integrity of the ROI after the image restoration, as well as ownership information with authentication purposes) and SM_{RONI} (which contain LSB_{ROI} to recover the original ROI, and the chrominance data CD to restore the color information of the image.) respectively.

Note that this RDH-ED study case is ROI-based, this fact indicates that the reversibility is only performed in the ROI region, the RONI area preserves data hidden in its content, even when the color image has been restored. However, considering that the ROI is most relevant that the RONI, the visual distortions are considered imperceptible by a naked eye and the contextual content of the color image is preserved. To obtain the binary chrominance data CD, the chrominances Cb and Cr are rescaled to a predefined size m x m, and its decimal values are converted to a binary representation. Finally, to embed the secret message SM into the encrypted image E_{IMG}, Least Significant Bit (LSB) substitution technique is used, which has been widely used in data hiding schemes, due to its high capacity to embed data into images without affecting its visual quality. A pseudo-random walk generated by a pseudo-random number generator (PRNG) is used to embed SM into the encrypted image E_{IMG}, and this compose the data hiding key denoted as DHK.

2.2. Recovery data and image restoration stage

An authorized receiver, and according to the managing of the encrypted and data-hiding keys *EK* and *DHK* respectively, can perform the following tasks:

Case 1 (Receiver). Having only the encryption key *EK*, the receiver can obtain an approximate version of the original image *I* in grayscale resolution, executing the follow steps:

a) Decrypt directly the encrypted image E_{IMG} using the block cipher key K_2.
b) Reorder the pixel's locations using the key permutation K_1.
c) Re-arrange the ROI and RONI to its original form using the IND_{ROI} data.

Case 2 (Receiver). Having only the data hiding key *DHK*, the receiver can obtain the secret message *SM*. However, in this case, the receiver can only perform the ownership authentication and not is able to see the image content.

Case 3 (Receiver). Having the encryption key *EK* and the data hiding key *DHK*, the receiver can recover the secret message *SM* and restore the color image with its ROI area with error-free.

In the next section, some experimental results are shown to analyze the performance of the proposed RDH-ED in VRBE modality with data extraction and image recovery in encrypted domain.

3. Experimental results

Considering 100 color images from Microsoft © COCO dataset [27] and the proposed RDH-ED, in this section we show the experimental results in terms of imperceptibility, capacity, confidentiality and visual quality, respectively.

Imperceptibility. Considering the *Case 1* of the receiver stage, the encryption key *EK*, the AES algorithm in OFB mode, an embedding data in each bit-plane of the encrypted image E_{IMG}, i.e., from the LSB (plane-0) to the most significant bit (MSB) (plane-7); and using the peak signal to noise ratio (PSNR) in decibels (dB), which measure the imperceptibility between original luminance and decrypted luminance with data hidden, the Fig. 5 shows the average PSNR obtained in this testing. From Fig. 5 we show that the imperceptibility decreases when the bit-plane is nearer to the plane-7 (MSB). According to this behavior, the most suitable bit-planes that can be used to conceal the secret message are the planes 0, 1 and 2, where the PSNR is greater than 38dB.

Capacity. Considering the *Case 1* of the receiver stage, the encryption key *EK*, the AES algorithm in OFB mode, an embedding data in the bit-planes 0, 1 and 2 of the encrypted image E_{IMG}, and varying the capacity of the secret message from 0.1 to 1 bpp (bits per pixel), the Fig. 6 shows the average PSNR obtained in each bit-plane. From Fig. 6 we show that the bit-plane 0 (LSB) offers PSNR values from 66dB to 52dB when the capacity rate from 0.1 to 1 bpp. On the other hand, if we use the bit-plane 1 to

conceal the secret message, this offers PSNR values from 55dB to 45dB when the capacity rate is from 0.1 to 1 bpp. Finally, using the bit-plane 2, the PSNR values obtained are from 49dB to 39dB when the capacity rate is from 0.1 to 1 bpp. Considering this behavior, the *Data-Hider* can embed the secret message only in the bit-plane 0 to increase the imperceptibility, or well, can conceal the bits of the secret message in a permuted form into the bit-planes 0, 1 and 2 to increase the security in the data extraction of the secret message. This implementation of the embedding data is dependent of the application scenario.

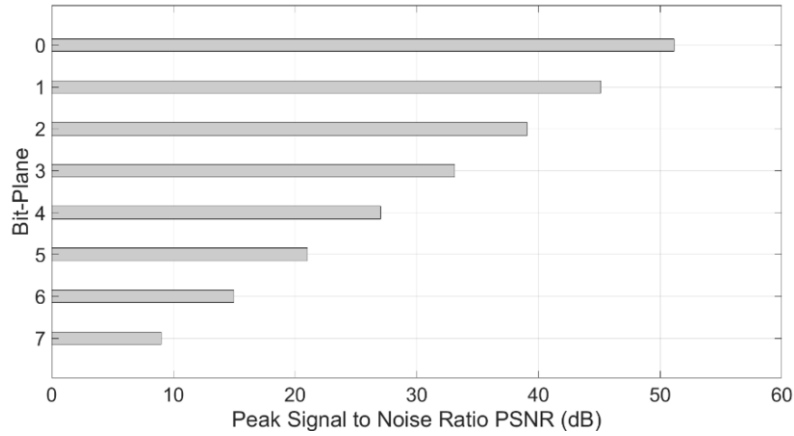

Fig. 5. Average PSNR (dB) obtained for the bit-planes 0 to 7 using AES in OFB mode.

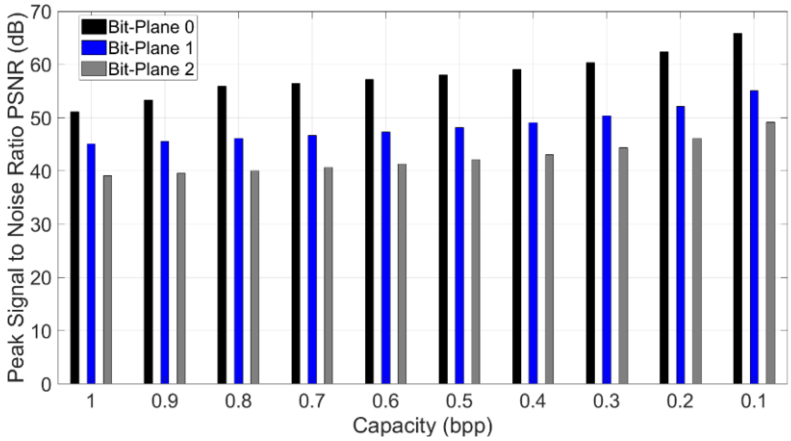

Fig. 6. Data hiding capacity with several embedding rates.

Confidentiality. In the context of RDH-ED, the confidentiality is related with the visual artifacts that can be perceived by a naked eye in the encrypted image and as consequence, the security of an RDH-ED scheme could be compromised. For illustrative purposes, considering five images with 8 bit/pixel of grayscale resolution

obtained from the USC-SIPI image database available on [28], and implementing the state-of-the-art methods reported in [9], [29], in Table 1 shows the PSNR measured between the original and encrypted versions. From Table 1 we show in a quantitative manner that the methods in [9], [29] and the proposed in this study case obtains PSNR values under 10 dB, which indicates that the encrypted version does not contain visible details of the original images that could compromises its confidentiality. To visualize this effect, Fig 7 shows the encrypted version of Lena image from methods in [9], [29] and the proposed, respectively.

Table 1. PSNR between original and encrypted versions.

Image	Method in [9]	Method in [29]	Proposed method
Lena 	8.50 dB	8.21 dB	7.85 dB
Baboon 	8.01 dB	9.00 dB	7.17 dB
Man 	8.25 dB	8.66 dB	7.23 dB
Boats 	7.19 dB	7.59 dB	7.17 dB
Peppers 	7.28 dB	7.48 dB	7.56 dB

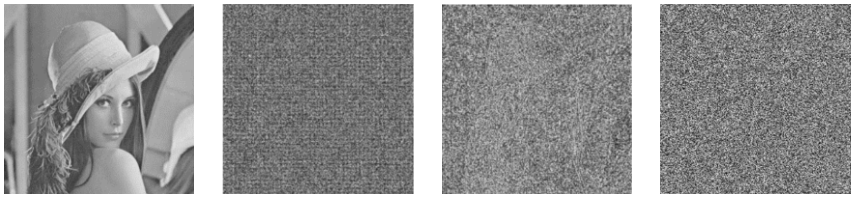

Fig. 7. Encrypted versions of Lena image. (a) Original, (b) Method in [9], (c) Method in [29] and (d) Proposed method.

Visual quality. It refers to the visual quality obtained after the color image is processed by the RDH-ED proposed in this section. Considering the 100 color images from Microsoft © COCO dataset [27] with a spatial resolution of 640x480 pixels in size, and m = {8,16,32,64,128}, which is the parameter used for obtaining the binary chrominance data *CD*, the PSNR, the Structural Similarity Index (SSIM) [30], and the Normalized Color Difference (NCD) [31-32], in Table 2 we show the average visual quality results. The range of SSIM values is [0, 1], and the closer value to 1 represents a better-quality respect to the original image, a value of 1 corresponds to the case when

the original and the reference image are the same. The normalized color difference NCD [31], [32] is based on the CIELAB color space and it is applied to measure the difference of color between two images. A value closer to 0 represents a better quality with respect to the original image. A value of 0 indicates that the original and reference image are the same.

Table 2. Average visual quality results in terms of PSNR, SSIM and NCD for several chrominance resizing.

Chrominance resizing	PSNR	SSIM	NCD
128x128	42.1399 dB	0.9947	0.0287
64x64	36.8705 dB	0.9852	0.0518
32x32	33.5713 dB	0.9684	0.0772
16x16	31.2624 dB	0.9445	0.1037
8x8	29.4018 dB	0.9147	0.1326

In Table 2, we show that resizing the chrominance to 8x8 pixels in size, is not the best choice because the color in the restored image is affected and perceived by a naked eye, as shown in Fig. 8. On the other hand, as shown in Fig. 8, resizing the chrominance to 128x128 pixels in size offers the best visual quality results, however, the total capacity C (taking into consideration 1 bpp) in the encrypted luminance information is C = 640x480= 307,200 bits, on the other hand, the bits that composes the binary chrominance data CD are 128x128x8x2 = 262,144 bits, this amount reduces the dimensions of the ROI area, and as consequence, dicreases the ability of the RDH-ED to perform the reversibility. This is a tradeoff between visual quality and reversibility.

From Figs. 8 and Table 2 we show that a suitable value for the parameter m is 64, obtaining average values of PSNR, SSIM and NCD of 36.87dB, 0.9852 and 0.0518, respectively. In this way, having a spatial resolution of 640x480 and considering 1 bpp, the capacity C available in the encrypted luminance information is 640x480 = 307,200 bits. If the value of m is 64 then the capacity needed is 64x64x8x2 = 65,536 bits. This ratio allows delimiting each one of the RONI and ROI regions in approximately 50% of the encrypted luminance information, allowing the restoration of luminance information into the ROI with error-free, remembering that this RDH-ED study case is ROI-based, this fact indicates that the reversibility is only performed in the ROI region, the RONI area preserves data hidden in its content, even when the color image has been restored. However, considering that the ROI is most relevant that the RONI, the visual distortions are considered imperceptible by a naked eye and the contextual content of the color image is preserved. With illustrative purposes, Fig. 9 shows the output in each stage of this RDH-ED study case.

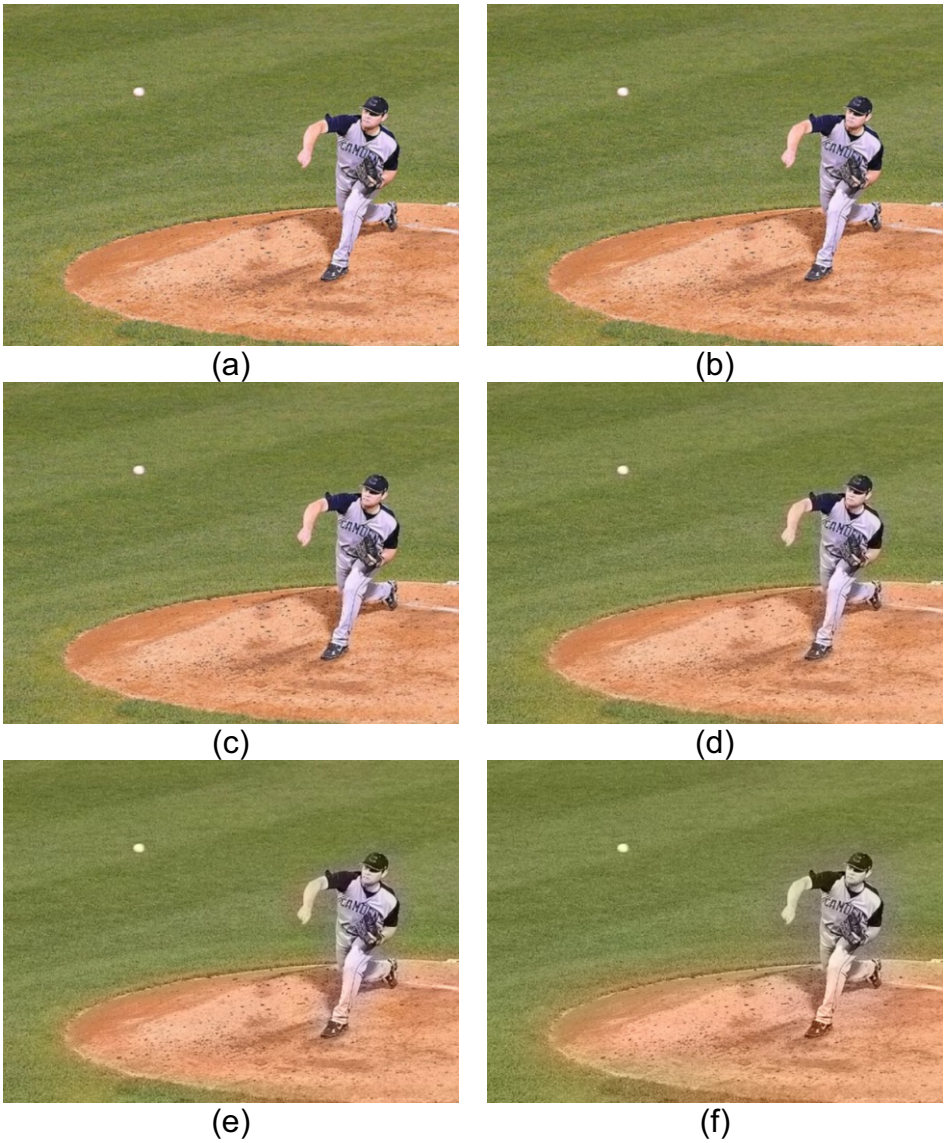

Fig. 8. (a) Original image. Recovered color image with chrominances resized to (b) 128x128, (c) 64x64, (d) 32x32, (e) 16x16 and (f) 8x8.

On the other hand, if the decrypted grayscale image (approximated version) is colorized using colorizing algorithms such as [33], to try obtaining a color version close to the original one, the effectiveness of the strategy proposed in this RDH-ED study case outperforms the synthetic colorizing, ensuring the privacy protection of the color images. In Fig. 10 we show a comprehensive result about this behavior.

4. Conclusions and future work

RDH-ED is a new research topic and emerging technology, illustrated by the study case presented in this paper and supported by the scientific literature in [1-20], [29]. According to Shi et al. in [1], "… *the research on theory, framework, methodology and applications on RDH-ED should be deeply developed. Firstly, we need new theory about RDH-ED to give the achievable rate-distortion performance suitable for the statistical properties of plaintext data and the usability of cryptographic key. Secondly, a generalized framework is desired. Thirdly, we need more methods on RDH-ED to improve actual rate-distortion performance.*" In this way, it is needed to develop novel algorithms to be implemented in specific application scenarios such as the privacy protection and security management of massive data (e.g., color images), both illustrated in a brief manner by the study case presented in this paper.

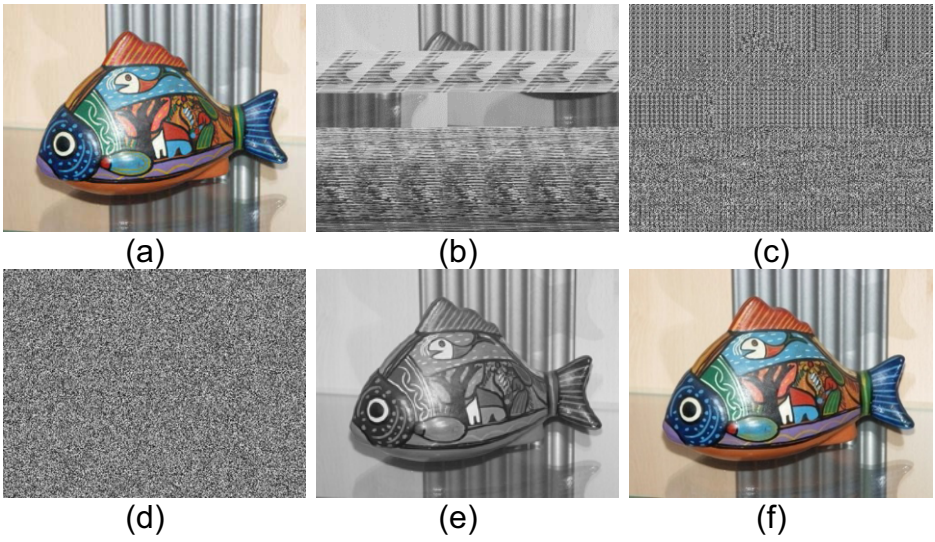

Fig. 9. (a) Original image, (b) Re-arranged image, (c) Encrypted version of image (b) using AES CTR mode, (d) Permuted version of image (c), (e) Approximate version in grayscale resolution with data hidden in its content, (f) Restored color image with ROI luminance error-free.

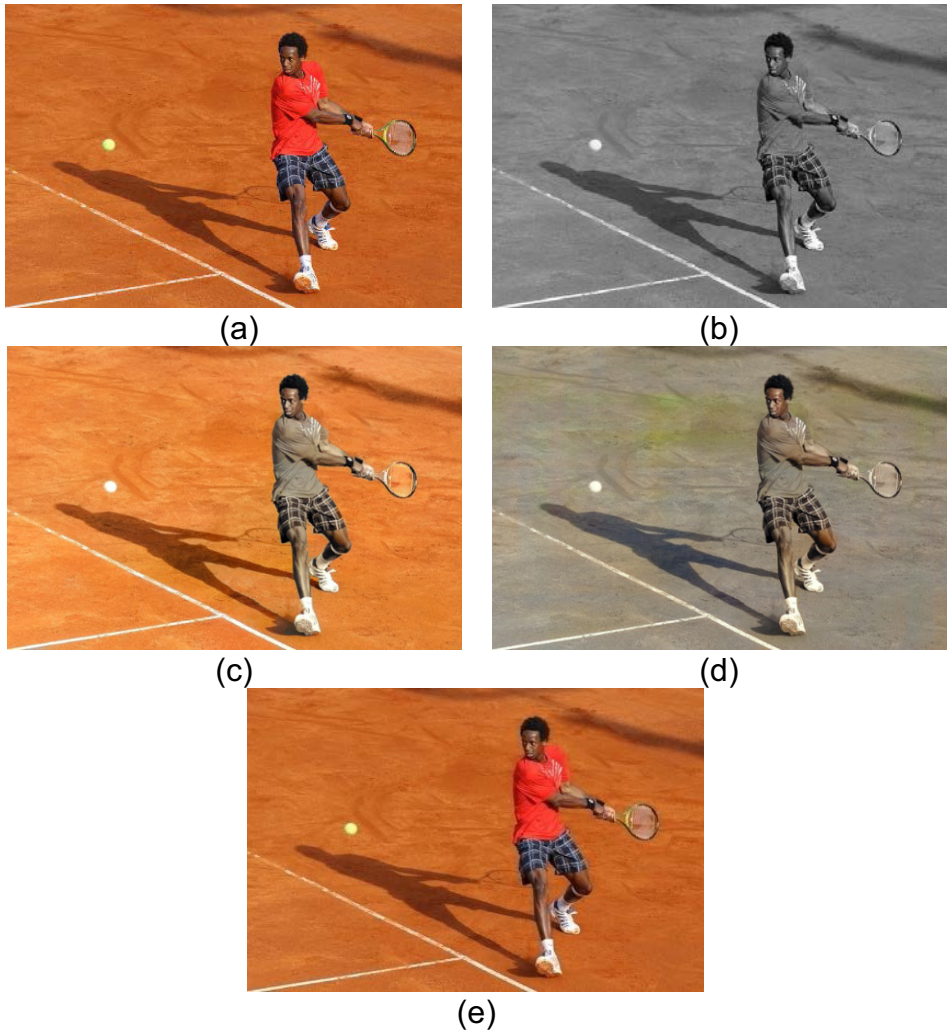

Fig. 10. (a) Original image, (b) Approximate version in grayscale resolution with data hidden in its content, (c) Colorized version of (b) using [33] in manual-mode, (d) Colorized version of (b) using [33] in auto-mode, (e) Recovered color image using the proposed RDH-ED.

References

[1] Y. Shi, X. Li, X. Zhang, H. Wu and B. Ma. Reversible data hiding: Advances in the past two decades. IEEE Access, vol. 4; 2016. pp. 3210-3237, https://doi.org/10.1109/ACCESS.2016.2573308

[2] X.P. Zhang. Reversible data hiding in encrypted images. IEEE Signal Process, vol. 18; 2011. pp. 255–258, https://doi.org/10.1109/LSP.2011.2114651

[3] W. Hong, T. Chen, H. Wu. An improved reversible data hiding in encrypted images using side match. IEEE Signal Process. vol. 19; 2012. pp. 199–202, https://doi.org/10.1109/LSP.2012.2187334

[4] Zhang, X. Separable reversible data hiding in encrypted image. IEEE Transactions on Information Forensics and Security, vol. 7; 2012. pp. 826–832, https://doi.org/10.1109/tifs.2011.2176120

[5] A. Lavanya, V. Natarajan. Watermarking patient data in encrypted medical images. Sadhana-Acad. Proc. Eng. Sci., vol 37; 2012. pp. 723–729, https://doi.org/10.1007/s12046-012-0107-z

[6] Liu, Yuling, Xinxin Qu and Guojiang Xin. A ROI-based reversible data hiding scheme in encrypted medical images. J. Visual Communication and Image Representation, vol 39; 2016, pp. 51-57, https://doi.org/10.1016/j.jvcir.2016.05.008.
[7] Z. Yin, H. Wang, H. Zhao, B. Luo, and X. Zhang. Complete separable reversible data hiding in encrypted image. Proc. 1st Int. Conf. Cloud Comput. Secur.; 2015. pp. 101-110, https://doi.org/10.1007/978-3-319-27051-7_9
[8] J. Zhou, W. Sun, L. Dong, X. Liu, O. C. Au and Y. Y. Tang. Secure Reversible Image Data Hiding Over Encrypted Domain via Key Modulation. IEEE Transactions on Circuits and Systems for Video Technology, vol. 26, no. 3; 2016. pp. 441-452, https://doi.org/10.1109/TCSVT.2015.2416591
[9] Li, Q., Yan, B., Li, H. et al. Separable reversible data hiding in encrypted images with improved security and capacity. Multimed Tools Appl 77, 30749–30768 (2018). https://doi.org/10.1007/s11042-018-6187-y
[10] Yu, M., Liu, Y., Sun, H. et al. Adaptive and separable multiary reversible data hiding in encryption domain. J Image Video Proc. 2020, 16 (2020). https://doi.org/10.1186/s13640-020-00502-w
[11] Min Long, Yu Zhao, Xiang Zhang, Fei Peng, A separable reversible data hiding scheme for encrypted images based on Tromino scrambling and adaptive pixel value ordering, Signal Processing, Volume 176, 2020, 107703, https://doi.org/10.1016/j.sigpro.2020.107703.
[12] L. Liu, A. Wang and C. Chang, "Separable Reversible Data Hiding in Encrypted Images With High Capacity Based on Median-Edge Detector Prediction," in IEEE Access, vol. 8, pp. 29639-29647, 2020, https://doi.org/10.1109/ACCESS.2020.2972736.
[13] N. Zhou, M. Zhang, H. Wang, Y. Ke and F. Di, "Separable Reversible Data Hiding Scheme in Homomorphic Encrypted Domain Based on NTRU," in IEEE Access, vol. 8, pp. 81412-81424, 2020, https://doi.org/10.1109/ACCESS.2020.2990903.
[14] Chen, K., Chang, CC. Error-free separable reversible data hiding in encrypted images using linear regression and prediction error map. Multimed Tools Appl 78, 31441–31465 (2019). https://doi.org/10.1007/s11042-019-07946-x
[15] Yu C, Ye C, Zhang X, Tang Z, Zhan S. Separable Reversible Data Hiding in Encrypted Image Based on Two-Dimensional Permutation and Exploiting Modification Direction. Mathematics. 2019; 7(10):976. https://doi.org/10.3390/math7100976
[16] Wu, H., Li, F., Qin, C. et al. Separable reversible data hiding in encrypted images based on scalable blocks. Multimed Tools Appl 78, 25349–25372 (2019). https://doi.org/10.1007/s11042-019-07769-w
[17] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted im-ages by reserving room before encryption", IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553-562, Mar. 2013. https://doi.org/10.1109/TIFS.2013.2248725
[18] W. Zhang, K. Ma, and N. Yu, "Reversibility improved data hiding in encrypted images", Signal Process., vol. 94, no. 1, pp. 118-127, Jan. 2014. https://doi.org/10.1016/j.sigpro.2013.06.023
[19] X. Cao, L. Du, X. Wei, D. Meng, and X. Guo, "High capacity reversible data hiding in encrypted images by patch-level sparse representation", IEEE Trans. Cybern., vol. 46, no. 5, pp. 1132-1143, May 2016. https://doi.org/10.1109/TCYB.2015.2423678
[20] C.-W. Shiu, Y.-C. Chen, and W. Hong, "Encrypted image-based reversible data hiding with public key cryptography from difference expansion", Signal Process., Image Commun., vol. 39, pp. 226-233, Nov. 2015. https://doi.org/10.1016/j.image.2015.09.014
[21] Lukac, R., Plataniotis, K.: Color Image Processing. CRC Press, London (2007)
[22] Chareyron, G., Da Rugna, J., Trémeau, A.: Color in image watermarking. In: Al-Haj, A. (ed.) Advanced Techniques in Multimedia Watermarking: Image, Video and Audio Ap-plications, IGI Global, pp. 36–56 (2010). https://doi.org/10.4018/978-1-61520-903-3.ch003
[23] Cedillo-Hernández, M., García-Ugalde, F., Nakano-Miyatake, M. et al. Robust hybrid color image watermarking method based on DFT domain and 2D histogram modification. SIViP 8, 49–63 (2014). https://doi.org/10.1007/s11760-013-0459-9
[24] C. Paar, J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, Springer-Verlag, Berlin Heidelberg, 2010, http://dx.doi.org/10.1007/978-3-642-04101-3.
[25] Schneier, B.: Applied Cryptography, 2nd edn. Wiley, New York (1996)
[26] Federal Information - Processing Standards Publications (FIPS PUBS). Announcing the Advanced Encryption Standard (AES), November 2001.
[27] Lin TY. et al. (2014) Microsoft COCO: Common Objects in Context. In: Fleet D., Pajdla T., Schiele B., Tuytelaars T. (eds) Computer Vision – ECCV 2014. ECCV 2014. Lecture Notes in Computer Science, vol 8693. Springer, Cham. https://doi.org/10.1007/978-3-319-10602-1_48
[28] USC-SIPI image database. Available at: http://sipi.usc.edu/database/
[29] Dawen Xu, Rangding Wang, Separable and error-free reversible data hiding in encrypt-ed images, Signal Processing, Vol. 123, 2016, pp. 9-21, https://doi.org/10.1016/j.sigpro.2015.12.012