“Private” JPEG Images for Earth Science Purposes

Bruno Carpentieri
Dipartimento di Informatica, Università di Salerno, 84084 Fisciano (SA) – Italy
bcarpentieri@unisa.it

Abstract. The 5G era that is about to come will exponentially increase the amount of digital data produced. Already, the giant amount of digital data that is produced every day by sensors, users and digital devices has called for scalable and efficient decentralized approaches to data storage and elaboration and to a Fog/Edge computing paradigm that requires efficient networking and storage for better services related to the compression and security of digital data. In this paper, we will explore a unified approach that merges compression and security in one step, by reviewing the current research in this field and by presenting new experimental evidence and new ideas for secure compression of two-dimensional data (for instance digital images). The purpose of our study is also the masking and unmasking of the sensitive biometric data, i.e. face and eyes, that are contained within a JPEG image that contains human faces.

1. Introduction
The huge amount of data, that today travels on the digital communication networks is certainly going to increase exponentially in size in the next few years. Already, the giant amount of digital data that is produced every day by sensors, users and digital devices has called for scalable and efficient decentralized approaches to data storage and elaboration and to a Fog/Edge computing paradigm: i.e. a decentralized model that transfers computing-intensive tasks from the cloud to intermediate nodes or to edge nodes.

The 5G era that is about to come will further increase the amount of digital data produced. It shall be a true revolution: the increase of speed in communication will boost today’s data traffic by involving new users and will lead to the development of new and futuristic applications that will need to produce and exchange digital data in a secure and efficient way. Telemedicine, body sensors, virtual and augmented reality applications, 3-d or hologram-based televisions or telephones, etc., they are all possible new frontiers for the computer scientists in the 5G era and all of them involve an enormous amount of digital data that shall be stored, transmitted or received by preserving privacy and transmission speed.

Data compression is always needed when digital data are transmitted or stored but the advent of the 5G communication speed and the new, huge, growth in the amount of digital traffic will make the use of data compression a strict requirement of any communication protocol.

On the other side, the need for privacy will increase the use of cryptology and encryption methods in the transmission or storage of data. Therefore, there will be a growing demand for compression combined with security, i.e. secure compression paradigms.
As has been demonstrated in the literature (see [1], [2]), a correct approach for compression combined with security should be to do first the data compression and then the data encryption. Most of the compression tools we use today include as an option the possibility of encrypting the compressed output by using a secret password provided by the user.

A disadvantage of this way of compression and encryption is the fact that data, after encryption, are now very hard to search and to process in compressed form and this is not acceptable in many applications. Another approach unifies compression and encryption in a single step, by modifying compression algorithms to provide also security.

In this paper, we will explore this approach, by reviewing the current research in this field and by presenting new experimental evidence and new ideas for the secure compression of one-dimensional digital data (for instance text) and two-dimensional digital data (for instance digital images).

The paper is organized as follows: in Section II we review the state of the art in privacy and compression of two-dimensional data (i.e. digital images) and present new approaches to AVQ encryption and to JPEG image scrambling. Section III presents our conclusions and possible future research directions.

2. Privacy and compression of two-dimensional data
Digital imaging and image sharing platforms are today one of the biggest sources for digital data traffic.

With the advent of 5G communication and of mobile edge and fog computing, this traffic will dramatically increase, and the public concerns regarding security and visual privacy protection of image data shall proportionally grow.

Because of their intrinsic digital nature, digital images can be easily and inexpensively manipulated, copied, and distributed. When communicating digital images there is therefore an obvious need for content protection, authentication, data integrity, and privacy protection.

There have been many approaches to secure the transmission of digital images. The JPEG committee in 2006 created Secure JPEG 2000 (JPSEC) which is now an International Standard that provides a secure framework for image compression in JPEG 2000.

Other approaches, like [3] and [6] for JPEG, aims to secure other compression algorithms or (see [4] and [5]) to apply watermarking techniques to ensure privacy and property of the digital data.

Here we will concentrate on the security of AVQ based image compression algorithms and on preserving privacy when images are for example transmitted on social networks by using image scrambling techniques.

2.1. AVQ encryption
The AVQ algorithm ([7], [8]) combines one-dimensional dictionary-based data compression schemes (often called Lempel-Ziv compression algorithms) and Vector Quantization. Compressor and decompressor employ each a consistent dictionary $D$ and they compress and communicate two-dimensional data, i.e. full color or grayscale images or generic binary images.
In [9] it is presented a secure lossy image compression method based on Adaptive Vector Quantization based on the Entropy-restricted Semantic Security and the logical functioning of the Squeeze Cipher algorithm of [1], here we review and improve that approach by showing new experimental evidence of its efficiency. A secure, modified version of the AVQ algorithm can be denoted as AVQs and in [9] it is proved to be secure, according to the Entropy-restricted Semantic Security definition in [1].

In AVQs it is built a uniform distribution of the entries in both the compressor’s and the decompressor’s dictionaries.

Every time a dictionary element is used then this entry is randomly swapped with another entry, pseudo-randomly selected (when possible, an empty entry is preferred).

When a new item is added to $D$, then the index of this item it is pseudo-randomly generated by randomly searching an empty dictionary entry.

The initialization of the compressor’s dictionary it is driven by a new initialization dictionary heuristic: the secure initialization dictionary heuristic ($SIDH$) that assigns the initial entries for the 256 pixels to pseudo-random locations that are randomly selected by using a secret key that is known only to the compressor and decompressor.

AVQs transmits (or stores) at each step index $i$, i.e. the index in the dictionary of the matched block $b$.

The entry at $i$ is randomly swapped with an empty entry in the dictionary $D$, selected by using a pseudo random generator based on the secret key. A new update heuristic is then used to insert new elements in the dictionary (secure dictionary update heuristic).

**Figure 1.** Coverings of “Lena”
Table 1. AVQ encryption

| Image        | Compression Ratio | PSNR   |
|--------------|-------------------|--------|
| Lena (standard) | 1.5277            | 36.76  |
| Lena (encrypted) | 1.5255            | 36.81  |
| Board (standard)  | 1.1159            | 39.16  |
| Board (encrypted) | 1.1158            | 39.16  |
| Peppers (standard) | 1.2113           | 37.15  |
| Peppers (encrypted) | 1.2111           | 37.18  |
| Balloon (standard)  | 1.6778            | 36.14  |
| Balloon (encrypted) | 1.6780            | 36.12  |

In [9] a preliminary implementation of AVQs is tested. Here we have improved that implementation and we have tested the new AVQs on a standard test data set.

We have included in this new implementation of AVQs a better dictionary management strategy that fully replicates the choices that the standard algorithm does in terms of matching and updating, so to have a similar covering of the original image.

In [9] a preliminary implementation of AVQs is tested. Here we have improved that implementation and we have tested the new AVQs on a standard test data set.

We have included in this new implementation of AVQs a better dictionary management strategy that fully replicates the choices that the standard algorithm does in terms of matching and updating, so to have a similar covering of the original image.

Figure 1 shows a representation of the compression of the Lena image (upper left) by the standard AVQ compressor (upper right) and AVQs (lower left).

Each block shown in the figure is related to a match and it is represented by a random colour that visually indicates the size of the corresponding block found in the local dictionary by the Matching Heuristic.

By looking at the image it is clear that AVQs behaves in the same way AVQ does, and that the small differences in compression or quality are only due to the different “naming” of the indices.

Table II shows the experimental results we have obtained on the standard images Lena, Board, Peppers and Balloon by using a dictionary with at most 1024 entries, with a match heuristic MSE with threshold 9.0 and with the Deletion Heuristic Freeze.

The results are almost identical for standard AVQ and for encrypted AVQ (our implementation of AVQs), as said before the very small differences depend only on the fact that AVQs use different numbers to indicate the same indices.

2.2. “Private” JPEG images
Cryptography has nowadays created systems and protocols that guarantee confidentiality, authenticity and integrity of digital data communication.

However, cryptographic techniques do not always solve the problem of the reliable and safe diffusion of digital data and the problem of privacy.

With the advent of smartphones and social networks, the flow of multimedia traffic has increased dramatically.

More precisely, referring to the images uploaded every day on the main social networks, according to the evaluations of November 2017, we have: 300,000,000 images uploaded on Facebook; 95,000,000 on Instagram; 25,000,000 on Twitter. The forthcoming 5G era will probably increase exponentially these numbers.
The other side of the medals is the amount of information that passes through the images. Each image, for example, could reveal the identity of the people who are depicted in the photo, the location and the time in which the photo was taken. The photos on social networks can be viewed by anyone and often by combining multiple photos it is possible to identify a person and to watch and spy on them.

The main techniques for protecting information within an image are basically four. The first is image filtering that allows applying a filter to an image in such a way as not to make certain areas within it recognizable. The main limitation of this technique is that it does not allow the reconstruction of the original image, thus leading to the definitive loss of the modified information; The second technique is encryption that allows encrypting an image by using a special encryption algorithm (AES, RSA, etc.).

As a result, only those in possession of the decryption key will have the right to view the original image. The disadvantage of this is its complexity and the fact that images might have a relatively low commercial value which does not always justify the overhead.

The third is pixel replacement that allows replacing the pixels in an image by using masks, distortions or patterns. These changes and the information to perform the reverse operation are saved within the metadata. This technique is resistant to image processing actions but it introduces overhead and can significantly increase the size of the modified image.

The last technique is data manipulation. Unlike pixel replacement, data manipulation does not replace the pixels but applies a change that is reversible, provided that the decoder has the associated secret key. It is simple to implement and it does not have a decisive influence on the size of the file because it is not necessary to keep a large amount of information (for example, the original pixels must not be saved).

A special case of this technique is scrambling. This is an encryption technique that includes the methods that rearrange and deletes original image contents to make it impossible for an unauthorized observer to obtain information out of it. Image scrambling, therefore, transform the original image or parts of it, into random patterns that are meaningless and carry no information.

Only the authorized users will be able to reconstruct the original image by replacing the random patterns with the original information.

We have tested and implemented a scrambling strategy for JPEG images based on the Viola-Jones face detection algorithm.

The main phases of our strategy are the following:

1. A number of regions of interest (ROI) within an image is identified (by Viola-Jones) and selected. An ID is assigned to each ROI;

2. For each ROI a secret scrambling key $K_n$ is defined;

3. The DCT coefficients corresponding to the selected regions are modified by a complete scrambling on all the DCT coefficients of the three image matrices $Y$, $I$ and $Q$ through a bitwise XOR between each DCT coefficient (both AC and DC coefficients) and a pseudo-random value;

4. Once the image has been scrambled, all the scrambling information used and necessary to perform the descrambling operation are stored in the image metadata (IDs, ROIs, etc.).
Figure 2. “Alex” scrambled

Figure 3. “People” scrambled

Figure 2 and Figure 3 show two examples of the scrambling obtained.

In Figure 2 the ROI is a single face. In Figure 3 the ROIs are the four faces.

A way to compare scrambling algorithms for digital images in the case of face detection is to run the face detection algorithm after the scrambling.

We have experimentally compared our approach to the approach presented in [10] (in the case where the ROIs are human faces) by implementing it with the Viola-Jones face detection algorithm (the same we use in our approach). We have also implemented it by using the OpenCV face detection tool.

The experiments use a standard dataset (Group4a) and they are targeted to see how many faces are detected after scrambling.

The results are shown in Table 2.

The first column in Table 2 refers to the approach presented in [10] with face detection by the Viola-Jones algorithm.

The second column in Table 2 refers to the approach presented in [10] with face detection obtained by using the OpenCV tool.

The third column shows the results obtained with our approach.
Table 2. Results

|                | [10] and (Viola-Jones) | [10] and (OpenCV) | Our algorithm |
|----------------|------------------------|-------------------|---------------|
|                | 4334 / 234             | 4116 / 252        | 4334 / 16     |

Our algorithm has clearly the best performance. Security, therefore, derives from the fact that every pixel of the ROIs (faces) is modified and therefore the extensive modification of the DCT coefficients within the ROIs makes it difficult for the face detection algorithm to operate. Scrambling is total, making it impossible (or nearly so) to automatically identify a face and even to detect it.

The price we pay for greater security is a slight deterioration in the compression performance.

This deterioration is due to the fact that with our approach all DCT coefficients, including most of them with a value of 0 before scrambling, with the scrambling they are altered and not simply reversed.

Therefore, most of the values in the 8x8 blocks of the DCT for the ROIs will have a value other than zero, thus implying an increase in the file size.

3. Conclusions
The 5G era that is about to come will exponentially increase the amount of digital data produced.

The enormous amount of digital data produced every day by sensors, users and digital devices has already called for scalable and efficient decentralized approaches to data storage and elaboration and to a Fog/Edge computing paradigm that requires efficient networking and storage services. This implies a persistent and important need for better services related to the compression and security of digital data.

In this paper, we will explore a unified approach that merges compression and security, by reviewing current research in the field and by presenting new experimental evidence and new ideas for secure compression of one dimensional data (for instance text) and two dimensional data (for instance digital images).

We have discussed, implemented and experimentally tested new ideas connected to one-dimensional data (in particular the security of interactive data compression) and to two-dimensional data (in particular AVQ encryption and JPEG image scrambling).

Future work includes a deeper experimentation of the new ideas presented and also new approaches to compression and security for three-dimensional data, as for example digital video or three-dimensional medical images or hyperspectral images (see [11], [12]).

Acknowledgment(s)
Authors The author needs to thank his students C. De Blasio and M. Nilo for conducting preliminary experiments.

References
[1] J. Kelley and R. Tamassia, “Secure compression: Theory & Practice”, IACR Cryptology EPrint Archive, 2014.
[2] B. Carpentieri, “Efficient compression and encryption for digital data transmission”, Security and Communication Networks, Vol. 2018, 2018.
[3] R. Pizzolante, B. Carpentieri, “Copyright protection for images on mobile devices”, Proceedings of the 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2012, pp. 585-590, 2012.
[4] R. Pizzolante, A. Castiglione, B. Carpentieri, A. De Santis, F. Palmieri, A. Castiglione, “On the protection of consumer genomic data in the Internet of Living Things”. Computers and Security, 74, pp. 384-400, 2018.

[5] B. Carpentieri, A. Castiglione, A. De Santis, F. Palmieri, R. Pizzolante, “One-pass lossless data hiding and compression of remote sensing data”, Future Generation Computer Systems 90, pp. 222-239, 2019.

[6] S. Lian, J. Sun, and Z. Wang, “A novel image encryption scheme based-on JPEG encoding”, Proceedings of the Eighth International Conference on Information Visualisation, IEEE Pub., 2004.

[7] F. Rizzo, J. A. Storer, and B. Carpentieri. “LZ-based image compression”. Information Sciences 135, no. 1-2, pp. 107-122, 2001.

[8] R. Pizzolante, B. Carpentieri, A. Castiglione, G. De Maio, “The AVQ algorithm: watermarking and compression performances”. Proceedings of the Third International Conference on Intelligent Networking and Collaborative Systems (INCoS), pp. 698–702. IEEE Pub., November 2011.

[9] B. Carpentieri, F. Palmieri, R. Pizzolante, “Secure Lossy Image Compression via Adaptive Vector Quantization”. Lecture Notes in Computer Science, 10850 LNCS (Augmented Reality, Virtual Reality, and Computer Graphics), pp. 497-505, 2018.

[10] P. Korshunov and T. Ebrahimi, “Scrambling-based tool for secure protection of JPEG images”. Proceedings of IEEE International Conference on Image Processing (ICIP), 2014.

[11] R. Pizzolante and B. Carpentieri, “Lossless, low-complexity, compression of three-dimensional volumetric medical images via linear prediction”, Proceedings of 18th International Conference on Digital Signal Processing (DSP), 2013.

[12] R. Pizzolante and B. Carpentieri, “Visualization, band ordering and compression of hyperspectral images”, Algorithms, Volume 5, Issue 1, Pages 76-97, March 2012.