LOSSLESS IMAGE COMPRESSION AND SELECTIVE ENCRYPTION USING A DISCRETE RADON TRANSFORM

A. Kingston†, S. Colosimo†‡, P. Campisi‡, F. Autrusseau†

† Polytech' Nantes, IRCCyN Lab.
Rue Christian Pauc, BP 50609, 44306 Nantes Cedex 3, France
‡ Dip. Elettronica Applicata
Universitá degli Studi di Roma Tre, via Della Vasca Navale 84, I-00146 Roma, Italy

ABSTRACT

In this paper we propose a new joint encryption and lossless compression technique designed for large images. The proposed technique takes advantage of the Mojette transform properties, and can easily be included in a distributed storage architecture. The basic crypto-compression scheme presented is based on a cascade of Radon projection which enables fast encryption of a large amount of digital data. Standard encryption techniques, such as AES, DES, 3DES, or IDEA can be applied to encrypt very small percentages of high resolution images. As the proposed scheme uses standard encryption, and only transmits uncorrelated data along with the encrypted part, this technique takes benefit of the security related to the chosen encryption standard, here, we assess its performances in terms of processing time and compression ratio.

Index Terms— Lossless compression, Selective encryption, High payload images

1. INTRODUCTION

When dealing with very large quantities of data, (such as that from high definition scans of paintings, 3D laser scans of sculptures, or video files), directly applying standard encryption techniques, such as 3DES and AES [1], becomes prohibitive due to the processing time.

This work is motivated by a French project[1] which aims to secure the digital database of the Louvre museum. The Research lab in the Louvre Museum (C2RMF) has commenced the digitisation of about 180000 images. Besides the use of a lossless compression algorithm, the Louvre Museum wants this whole database to be secured by both encryption techniques (for full resolution images both stored in the database, and distributed for research purposes) and digital watermarking (for low resolution thumbnails to be widely distributed). Very accurate scans are performed on the paintings of up to 800 Megapixels. An encryption technique applied directly to such images would certainly be incredibly slow.

[1] http://www.lirmm.fr/tsar/

Joint compression and encryption have been extensively studied over the past decade (see [2] for an overview). However, there are few papers in the literatre combining lossless compression and selective encryption (SE) [3]. One of the main goals of SE is to reduce the intensive processing time of most encryption algorithms [4]. Authors in [4] give an overview of selective encryption, and explain that for quadtree image compression, 13 to 27% of the compressed data is encrypted, whereas, for zero-tree based compression, less than 2% of the data is encrypted for 512×512 images. Here we present a technique able to encrypt as little as 0.02% of the data for high payload images. Similar to the work in [4], although only a minor portion of the data is encrypted, the remaining data (left unencrypted, but highly de-correlated) is useless in cryptanalysis. The technique proposed in [3] presents effective compression ratios, but processing time can still be improved. In this paper we propose a fast encryption technique for high payload images based on a discrete Radon transform (DRT). The DRT exploited here is known as the Mojette transform [5] and it is predominantly used in a data transmission context. The transform has a tunable redundancy and distributes the data over a predefined projection set, with applications in distributed storage, forward error correction codes, quality of Service, and ad hoc networking. The results section shows how efficient the proposed technique is in this respect. In [5] it has been demonstrated that applying the inverse Mojette transform on erroneous bins leads to a quick propagation of errors, providing encrypted images. The present work goes further and proposes an adaptation of standard encryption techniques for large images. We will demonstrate that one can take advantage of both the security inherent to standard encryption techniques, (e.g., AES, 3DES and even RSA), and the speed of the Mojette transform. The technique presented is perfectly suitable for joint SE-lossless compression as required in the TSAR project or in secure Medical imaging storage, where a secure fast encryption is required along with efficient lossless compression.

This paper is structured as follows: Section 2 defines the Mojette transform, both the forward and inverse algorithms.

In section 3 the proposed method to reduce the proportion of sensitive data that has to be encrypted, enabling a fast SE, is presented. Finally, section 4 gives experimental results for processing time and compression attained.

2. THE MOJETTE TRANSFORM

2.1. Forward Mojette transform

The Mojette transform is an exact and finite, discrete form of the Radon transform defined for specific "rational" projection angles. Like the classical Radon transform, the Mojette transform represents the image as a set of projections, however, there is a finite number of discrete projections with an exact inverse. The projection angles, θ_i, defined by a set of vectors (p_i, q_i) as $\theta_i = \tan^{-1}(q_i/p_i)$. To avoid redundancy p_i and q_i are selected such that $\gcd(p_i, q_i) = 1$ and q_i is restricted to be non-negative. The transformed domain of an image is a set of projections where each element (called a bin as in tomography) corresponds to the sum of the pixels centered on the line of projection. This is a linear transform defined for each projection angle as:

$$\mathrm{proj}_{p_i,q_i}(b) = \sum_{k=-\infty}^{+\infty} \sum_{l=-\infty}^{+\infty} f(k,l)\,\Delta(b + kq_i - lp_i), \quad (1)$$

where(k, l) defines the position of an image pixel and $\Delta(b)$ is the Kronecker delta function which is 1 when $b = 0$ and zero otherwise.The Mojette transform $M_I f(k, l)$ corresponds to the set of I projections $M_I f(k, l) = \{\mathrm{proj}_{p_i,q_i}, i \in [1...I]\}$. Each bin value equals the sum of the pixels crossed by the appropriate line $b = lp_i - kq_i$ as demonstrated for the example image in the top panel of Fig.1. The principal difference from the classical Radon transform is the sampling rate on each projection, which is no longer constant but depends on the chosen angle as $1/\sqrt{p_i^2 + q_i^2}$. Figure 1 (top panel) demonstrates the Mojette transform for the directions set $S = \{(0,-1)\,(-1,1)\,\text{and}\,(1,1)\}$. The number of bins for each projection depends on the chosen discrete angle. The algorithmic complexity of the Mojette transform for a $P \times Q$ image with I projections is O(PQI).

2.2. Inverse Mojette transform and the notion of reconstructibility

Since the set of projection directions is selected arbitrarily, the original data cannot necessarily be recovered from the set of projections chosen. A criterion is required to determine if a set of projections is sufficient to uniquely reconstruct the data.

The first result on the conditions for the existence of a unique reconstruction from a given set of I projections came from Katz [6] in a very similar context. He showed that if the following criterion is satisfied, any rectangular $P \times Q$ data-set can be uniquely reconstructed:

$$P \le P_I = \sum_{i=1}^{I} |p_i| \quad or \quad Q \le Q_I = \sum_{i=1}^{I} q_i. \quad (2)$$

The inverse Mojette transform is a fast and simple algorithm. Searching for and updating 1-1 pixel-bin correspondence enables a simple iterative procedure to recover the image. The bin value is back-projected into the pixel and subtracted from the corresponding bins in all other projections. The number of pixels belonging to the corresponding bins is also decremented. The algorithmic complexity of the inverse Mojette transform for a $P \times Q$ image with I projections is O(PQI). Figure 1 (bottom panel) shows an example of the first three steps of the inverse Mojette transform.

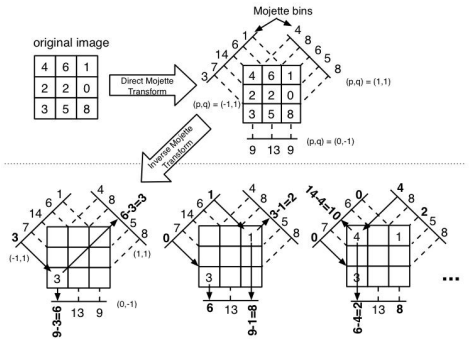

Fig. 1. Both forward Mojette transform (upper panel) and three steps of the inverse Mojette transform (lower panel).

3. SELECTIVE ENCRYPTION USING CASCADED RADON PROJECTIONS

A recent study [7] showed that the correlation between Mojette projections at similar angles can be exploited in a lossless compression algorithm. Both an intra-projection and inter-projection compression method were designed. Figure 2 shows two projections with (p_i, q_i) of (1,102) and (1,103) for the 256×205 flowers image [2]. It was noted in [7] that the projections are periodic with q_i, in fact, the projection data can be displayed as an image, r, of width q_i as demonstrated for the two projections in the example. Autrusseau et al in [7] employed a differential pulse code modulation of order 1 (DPCM-1) prediction method to compress the data with prediction $\widetilde{r}(k, l) = r(k, l-1)$. Here we use DPCM-3 with prediction $\widetilde{r}(k, l) = 0.9r(k, l-1) + 0.9r(k-1, l) - 0.8r(k-1, l-1)$ as it significantly improves the compression ratio with only a marginal increase in computation time. The strong

[2]"Fleurs et fruits", Paul Cézanne, Musée de l'Orangerie, Ref C2RMF F11714, oil painting

correlation remaining between these prediction error Mojette projections at similar angles (as demonstrated in the example) can also be removed (again through DPCM-1) from all but one projection, the 'basis' projection. An entropy coder (Golomb-Rice) is applied to the prediction error data to realise the compression. These techniques will be referred to as intra-projection and inter-projection coding respectively. The so-obtained compression rates are less efficient than standard techniques such as JPEG2000, however, the proposed Mojette based compression offers an interesting tunable redundancy and thus application in a distributed storage framework.

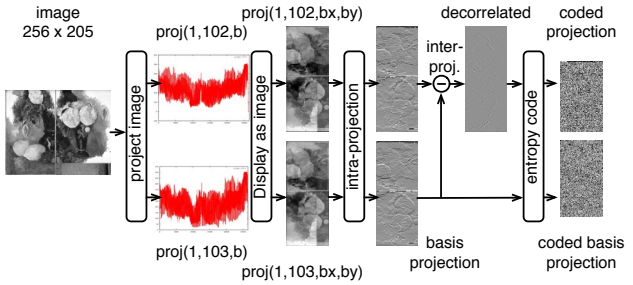

Fig. 2. Mojette projection respectively displayed as 1D sequences, and as images. The right column represent both the intra- and inter-encoded projections.

As a simple form of SE, the basis projection (approximately $100/I\%$ of the data) can be encrypted and transmitted along with the $I-1$ inter-coded projections which alone are useless since they have been decorrelated from the basis; A hacker must decipher the encrypted part. However, this compression technique can be exploited for a more efficient SE by using a cascade of Mojette projections. The output of this image compression scheme can be viewed as $I-1$ coded projections (essentially resembling noise that is useless without the basis projection) and the prediction error basis projection which itself is an image. This basis 'image' can be reprojected with a new projection set to obtain a second set of $I-1$ coded projections and a new smaller basis 'image' (approximately $100/I^2\%$ of the data). This can be repeated n times to any desired level with n sets of $I-1$ coded projections and 1 basis projection that is approximately $100/I^n\%$ of the data as depicted in Fig. 3. This final basis projection, which contains the sensitive data, can be encrypted with 3DES, AES, or even RSA. Similar to the work presented in [4], the encrypted data (the final basis projection) is transmitted along with the unencrypted part (the coded projections). The unencrypted part does not give any useful information on the original data, as the coded projections are strongly de-correlated from the basis projections.

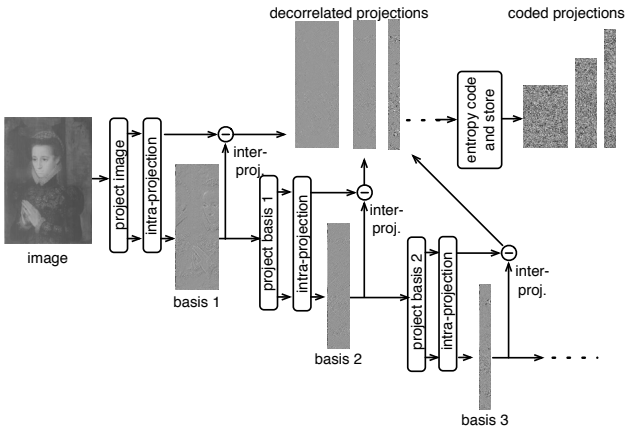

Fig. 3. Cascaded projections principle, each projection is intra-coded, the inter coding is then performed, this process is recursively repeated on inter coded projections.

4. EXPERIMENTAL RESULTS

One of the main advantages of using SE is that the amount of data to be encrypted is significantly reduced, and as a result, the processing time is also reduced. Evidently, with the cascaded Mojette projections scheme presented in section 3, the more loops we use, the less data need to be encrypted, but the compression ratio increases. Besides security and processing time, one of the main requirements of joint encryption and compression is to maintain the same compression performance when encryption is taken into account. In the presented technique, as the Mojette transform is extremely tunable, determine the number of loops of the cascade that provides the best trade-off between processing time and compression ratio. It's main asset is the processing time, as it only computes successive Mojette transforms, which are not computationally expensive, and only the final basis projection is encrypted, which indeed can be very small. Figure 3 shows the first three projections of a cascade on a Museum image[3]. $I = 2$ is used here, using $I = 3$ or more would reduce the projection sizes even more drastically, but would also degrade the compression ratio. A comparison of the processing time for either AES, 3DES, or the proposed technique is given in Figure 4 for different images size. In this plot, the Mojette SE is performed using either AES or DES as the encryption tool. For the larger tested image (7738×11146 pixels), the processing time of the Mojette+AES encoding is less than the time required for AES to encrypt the data, while for 3DES based Mojette encryption, the proposed technique present a processing time of approximately 30% of the full 3DES encryption. The ratios remain identical when both encoding and decoding are taken into account.

[3]"Dame en prière", unknown artist, Musée du Louvre, Ref C2RMF F11823, oil painting

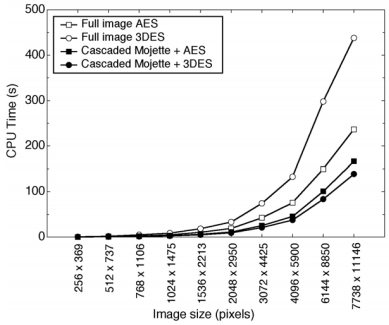

Fig. 4. Encoding processing time of the Mojette SE with $I = 2$ compared with two Encryption standards (3DES, AES) for a range of scales of the 'Dame' image.

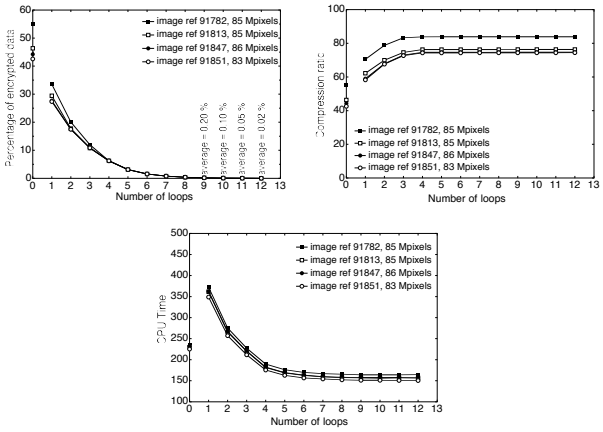

Fig. 5. Evolution of (a) the ratio of encrypted data, (b) the compression ratio, and (c) the processing time, as a function of the number of cascaded Mojette loops applied to 4 C2RMF images of size 83 to 86 Mega pixels with $I = 2$.

Figure 5 summarizes the performances in terms of processing time, compression ratios, and percentage of encrypted data for several number of loops. It clearly appears on these plots that the optimum trade-off both in terms of compression ratio and processing time is located at 8 loops. The results for lossless JPG2K encoding combined with AES encryption are given on the Y-axis. Although the compression ratios provided by the proposed technique can not compete with lossless JPG2K, it is interesting to notice that the percentage of encrypted data can very strongly be reduced allowing the use of public key encryption algorithms, such as RSA. The average percentage of encrypted data (4 test images) is given for the loops number 9 to 12 in Fig. 5(a). Furthermore, as shown in Fig. 5(c) the CPU time of the proposed technique is about 60 % of the CPU time needed by JPG2K encoding combined with AES. Such improvement would be very advantageous when processing a full image database. Besides the improved computation time, one of the main advantages of using this "all in one" compression and encryption technique, is to allow an open distribution of the error projections, as these ones are useless without the encrypted basis one, and a secure transmission of the final basis projection only.

5. CONCLUSION

We have proposed a fast selective encryption technique based on standard encryption algorithms. The original input data is split onto several Mojette projections, a cascade of projections leads to a small final basis projection, which contains all the sensitive data and can easily be encrypted by using either, AES, 3DES or even RSA. All additional coded projections are decorrelated from the basis, as specified in the Mojette compression technique, so little useful information about the image can be obtained from these projections without the (decrypted) final basis projection. Considering this point, and the fact that the basis projection is securely encrypted with appropriate standards algorithms, one can assume that the proposed technique is secure. Future works will be devoted to a best evaluation of the security aspects as well as the use of RSA to encrypt the basis projection.

6. REFERENCES

[1] J. Daemen and V. Rijmen, "AES proposal, rijndael," in *The First Advanced Encryption Standard Candidate Conference, N.I.S.T.*, 1998.

[2] X. Liu and A. M. Eskicioglu, "Selective encryption of multimedia content in distribution networks: Challenges and new directions," in *Int. Conf. on Communications, Internet, and Information Technology*, 2003, pp. 527–533.

[3] S. S. Maniccam and N. G. Bourbakis, "Lossless image compression and encryption using scan," in *Pattern Recognition*, 2001, vol. 34, pp. 1229–1245.

[4] H. Cheng and Xiaobo Li, "Partial encryption of compressed images and videos," in *IEEE Trans. Signal Processing*, 2000, vol. 48, pp. 2439–2451.

[5] F. Autrusseau, JP. Guedon, and Y. Bizais, "Watermarking and cryptographic schemes for medical imaging," in *SPIE Medical Imaging*, 2003, pp. 532–105.

[6] M. Katz, "Questions of uniqueness and resolution in reconstruction from projections," in *Lect. Notes in Biomath., Springer Verlag*, 1979.

[7] F. Autrusseau, B. Parrein, and M. Servieres, "Lossless compression based on a discrete and exact radon transform: A preliminary study," in *ICASSP*, 2006.