Geometric Shape Effects in Redundant Keys used to Encrypt Data Transformed by Finite Discrete Radon Projections

Andrew Kingston and Imants Svalbe
School of Physics
Monash University, VIC 3800, Australia
{Andrew.Kingston, Imants.Svalbe}@sci.monash.edu.au

Abstract

The Finite discrete Radon Transform (FRT) represents digital data exactly and without redundancy. Redundancy can however be injected into the FRT by reserving part of the image area to be replaced by a key that contains pixels of known, fixed values. The resulting image redundancy can be used to watermark values into the image, or as an encryption key that must be known if the image data is to be recoverable from a subset of transmitted projections. This paper looks at the affect the geometry of the selected key areas has on the interaction between the FRT projections of the key area and those of the data area. A method is proposed to measure this interaction of projected values. Results for simple key geometries are obtained. These give some insight into the design of key shapes that optimise the coupling of projected key and image values.

Keywords: discrete image processing, discrete Radon transform, data encryption, error correcting code.

1 Introduction

A discretisation of the Radon transform known as the Finite Radon Transform (FRT), defined by Matus and Flusser [15], enables the exact representation of digital data as projections, with no redundancy. 2D data on a $p \times p$ array can be mapped exactly and invertibly using just $p^2$ FRT projection elements.

This paper seeks to investigate the effect of injecting redundancy into the FRT projection set. This is done by selecting a pattern of pixel locations in the original image, $I(x, y)$, that are each set to some known value to act as a key for an encryption process. The FRT projection process mixes the key and the image data, making it very difficult to recover the original image values (which now occupy only some portion of a $p \times p$ square array) (i) – from a sub-set of the projections, or (ii) – after noisy data transmission, without knowledge of the pre-defined key [13]. Thus redundancy can be used for encryption or robust data transmission and storage as shown for the Mojette transform [1, 9] (another discrete form of the Radon transform).

In a 2D image, the design of the key has a large number of degrees of freedom. A wide diversity of options is necessary to enable a high level of robustness and security in any encryption scheme. The aim of this paper is to examine the effect the geometry of the selected key area has on the intertwining of key and image data. The objective is to specify the key shapes that spread the key and projection data uniformly into all projections, so that any one projection is not more valuable than others. Then any subset of the full set of projections can, with equal efficiency, use the injected redundancy to extract the original data, given knowledge of the selected encryption key.

In 1948, Shannon derived a formula governing the limit to the rate or capacity of information that can be reliably transmitted for a given signal to noise ratio [17]. Although Shannon’s formula shows the optimal capacity and he proves it is possible to achieve rates arbitrarily close to this limit, his work gives no indication as to how to reach this limit. Recently techniques have been developed that approach this limit. There are two main methods to encode data for robust transmission; Turbo codes, invented in 1993 [2], and Low Density Parity-Check (LDPC) codes, originally invented by Gallager in 1963 [6], that were rediscovered toward the end of last decade.

FRT projections are highly robust, however, due to the large summed values which must be stored, requires an additional $p^2 \log p$ bits to represent the data. An XOR FRT projection (Eq. 3) and reconstruction (Eq. 4) requires only an additional $pn$ bits to represent the $n$-bit greylevel data, i.e., an inherent redundancy of $O(1/p)$. The XOR FRT may prove useful as a form of error correcting code similar to the LDPC for robust data transmission. To optimise this scheme, the minimal key geometry which maximises redundancy and removes all bias to specific projections is
required; this is the subject of investigation in this paper.

All of the FRT projection angles and translates are automatically determined by just one parameter, the size of the data array, which is chosen to be square and of prime length, \( p \). The advantage of the prime length periodic FRT is that both projection and reconstruction from projections are implemented using simple addition of data element values and neither requires any pre-filtering or data interpolation. The projection angles are automatically pre-selected from the set of relative prime rational fractions given by the Farey sequence [20]. The discretely sampled FRT projection rays (separated by integer pixel translates) closely mimic the continuous Radon integrals for large array sizes, rather like the linogram form of the traditional sinogram.

Other discrete projection mappings such as the Mojette transform [8] are based on similar principles to the FRT. They also employ irreducible rational fractions for projection angles, but select an arbitrary set of projections that satisfy the Katz criterion [10] to ensure the exact reconstructability of the data. Image reconstruction is done using simple iterative algorithms for the noise free case [7] or more complex algorithms when using real projection data (such as in [16]).

The Katz criterion prescribes conditions to choose a minimum set of projections that will guarantee exact reconstruction and so always generates a degree of redundancy in the data representation. The Mojette approach gives more flexibility in the shape of the data array on which projections are made, as the projection set can be asymmetric. In contrast, the FRT is restricted to a square, prime sized array, however, by design, has zero inherent redundancy.

The Mojette transform makes great use of its inherent redundant projection information. Redundant data schemes have been used to embed watermarks, encrypt data [1] and for robust data communications and storage [9]. The redundancy ensures any subset of the received projection data can still reconstruct the original data exactly even when multiple projections may be lost in transmission, or are inaccessible in storage.

These advantages of the FRT (or its near relatives) have been exploited in other applications such as CT image reconstruction [21], data compression [4], feature extraction [5], object tracking [3] and blind deconvolution [14]. The 2D FRT extends neatly from 2D to higher dimensions by projecting discrete hyper-volumes to discrete hyper-planes [11]. A simple form of embedding data in FRT projections was presented in [18].

In section 2, the FRT is reviewed briefly. Section 3 gives an example of redundancy injected into an image as a geometric key and shows the recovery of the image from a sub-sample of the projected key plus image data. Then the properties of the FRT for planar areas and their complements are presented in section 4. A method to estimate the interaction of a key with the remaining part of the image array is given in section 5. Some example key shapes and the results obtained for these shapes are presented in section 6, with a summary and some options for future work being outlined in section 7.

2 Overview of the FRT

The FRT, \( R_m(t) \), of an image, \( I(x,y) \), sums the contents of image pixels as sampled at selected locations along digital straight lines according to

\[
R_m(t) = \begin{cases} 
\sum_{y=0}^{p-1} I((my+t)_p, y) & \text{for } 0 \leq m < p, \\
\sum_{x=0}^{p-1} I(x, t) & \text{for } m = p.
\end{cases}
\]

Each projection, \( R_m \), of an image \( I \) is indexed by an integer \( m \) which defines the slope of the lines of integration as \( x \equiv my + t (mod p) \) for \( 0 \leq m < p \) (see Fig. 1) and \( y \equiv t (mod p) \) for \( m = p \), with translations \( 0 \leq t < p \). The modular arithmetic implies that the rays wrap, under periodic boundary conditions, around from the right to the left image boundary.

![Figure 1. An example of a discrete line of projection in an 11 x 11 array. (a) The values of the grey pixels in \( I(x, y) \) which lie on the line \( x \equiv 5y + 2 \ (mod \ 11) \) sum to give the value of projection bin shaded grey in (b) at \( t = 2 \) and \( m = 5 \), i.e., \( R_5(2) \).](image)

Owing to this modular nature, these lines which have slopes, \( m \), can be expressed as the ratio of two relatively prime integers \( i/j \) (such that \( i \neq j \) (mod \( p \)) where \( j \) is the multiplicative inverse of \( j \mod p \)) The image is sampled at regular intervals \( \sqrt{i^2 + j^2} \) along these lines, as shown in Fig. 1. The values \( (i, j) \) are chosen to minimise the distance between line projection samples in the image and \( i/j \).
is always a member of the set of Farey fractions [20]. A digital projection is a parallel array of such lines, separated by integer translations (usually taken as the unit pixel spacing along the x-axis direction).

The image can be recovered from its FRT projections exactly using a discrete form of back-projection as

$$I(x, y) = \frac{1}{p} \left( \sum_{m=0}^{p-1} R_m(x - my)_p + R_p(y) - I_{\text{sum}} \right),$$

where $I_{\text{sum}}$ is the sum of all pixel values in $I$, found as $I_{\text{sum}} = \sum_{j=0}^{p-1} R_j(t)$, for any $j \in [0, p]$. This reconstruction is achieved in $O(p^2)$ operations. Inversion via the frequency domain is also possible in $O(p^2 \log p)$ operations. Algorithms for efficient FRT projection and reconstruction can be found in [11].

3 Injecting redundancy into FRT projections

The projections of the FRT are designed to minimise redundancy. When the square array size is prime, $p$, the transform can be presented in a form with no redundancy as the only common information between projections is $I_{\text{sum}}$ (or the DC term). Redundancy can however be injected into the projections by creating deliberate redundancy in the image prior to transformation. If the image is padded with zeroes, (or any known integer values), to a larger prime array size $p'$ and transformed, knowledge of where these zeroes occur in the original image enables the $p \times p$ data to be reconstructed from a subset of the $p'/p$ + 1 projections. Thus, when redundancy is injected into FRT projections, the proportion of zeros (or known numbers) to image data gives the ratio of redundancy and determines the number of projections which are non-essential in the reconstruction process. This region of zeroes or known values within the image will be termed the key, since knowledge of the key is required to reconstruct the image from a subset of projections.

An example has been given in Fig. 2 for $47 \times 47$ data. The key is the redundant region of zeros with a geometry shown in Fig. 2a, and the valid data fills the remainder of the array, as shown in Fig. 2b. The key/data ratio is approximately $(1 - \pi)/4$, so up to 10 projections can be lost and the original data can still be recovered if the key is known. Ten projections, (those with $\theta_m \approx k\pi/10$ for $0 \leq k < 10$), have been removed. Figure 2c shows the reconstruction achieved (without using the key) with these 10 projections missing. Knowledge of the key enables exact data recovery from the remaining 37 projections as shown in Fig. 2d by finding the solution to a set of linear algebraic equations as described in [11].

An alternative representation of the FRT projections is to sum the image data bitwise using the XOR operation [1]. The invertible XOR FRT data maintains the same number of bits as the original data, is computationally more efficient (being a bitwise operation) and requires no division by $p$.

Label the bitwise XOR summation data, $\eta$, as $\eta^X$, and let $\oplus$ denote bitwise XOR summation of data. The XOR projected value, $R_m^X(t)$, are then defined as

$$R_m^X(t) = \left\{ \begin{array}{ll} \left( \sum_{y=0}^{p-1} I \left( (my + t)_p, y \right) \right) & \text{for } 0 \leq m < p, \\ \left( \sum_{x=0}^{p-1} I(x, t) \right) & \text{for } m = p. \end{array} \right. \ (3)$$

and the original image is recovered from discrete XOR projection data, $R^X$, as

$$I(x, y) \equiv \sum_{m=0}^{p-1} R_m^X(t - x + my)_p \oplus I_{\text{parity}}. \ (4)$$

where $I_{\text{parity}}$ is the parity of $I_{\text{sum}}$ or $\langle I_{\text{sum}} \rangle_2$, found as

$$I_{\text{parity}} = \left( \sum_{j=0}^{p-1} R_j^X(t) \right), \text{ for any } j \in [0, p].$$

Therefore, each projection serves as a parity-check since they all should sum modulo 2 to $I_{\text{parity}}$. The projections with parity errors are easily isolated and the precise bins from these projections that must be corrected can be determined using the artifacts in the reconstructed key. Once all projections with parity errors are corrected, any remaining artifacts in the key arise due to multiple errors in a projection. These are more easily located once the other projections have been corrected. Figure 3 shows a $47 \times 47$ image with the key comprised of the
last two columns and rows of the array set to zero. This has
a redundancy of O(1/p), in this case \((5p – 2)/p^2 \approx 0.105\).
The example given in Fig. 3 has been successfully corrected
after insertion of 12 random bit errors. The robustness in-
creases with decreasing array size, \(p\), and the amount of in-
jected redundancy, so the array size and key used to encode
the data prior to transmission can be selected according to
the expected transmission bit error rate.

To ensure that no one projection is more crucial than any
other for exact recovery of \(I\), certain criteria are required of
the key. The remainder of this paper investigates the distri-
bution of various key geometries within the FRT projec-
tions, in a search for the optimal robust key which (i) – dis-
tributes itself evenly amongst all projections and (ii) – gives
enough redundancy to locate the projection bins from which
artifacts originate.

4 FRT projection of key shapes

The FRT is a linear transform. It preserves the Fourier
slice property of the continuous Radon transform and, as
a consequence, also retains the convolution property (en-
abling 2D image convolutions to be done through 1D con-
volutions in the projection domain). Because the FRT has
the property that the projection basis functions are identical
in form to the Fourier transform of the basis functions [12],
the results described below could be obtained by operating
in either the frequency or spatial domain. Simple spatial op-
érations such as image translation and rotation can also be
implemented by direct operations performed in the projec-
tion domain [19].

The shape of an encryption key area will be examined
here in relation to the remaining area of the image. This
remaining area is defined here by the complement of the
key shape.

An image \(I\) with greyscale \(g\) at pixel location \((x, y)\)
added pointwise to the complement of the same image \(\tilde{I}\)
(with \(\tilde{g} = g_{\text{max}} - g\) at \((x, y)\) where \(g_{\text{max}}\) is the maximum
possible greylevel for the image data) produces an image
with a constant value \(g_{\text{max}}\). Similarly, the FRT, \(R\), of
an image added to the FRT of the complement of the image, \(\tilde{R}\),
will sum to a constant value. In this paper, the projections
of a key will be compared to the projections of the comple-
ment of the key as a means to gauge the interaction between
the key and the encoded image for each projection translate
and angle.

5 Characterising the interaction between key
and image areas

To compare the key and key-complement (or anti-key)
shapes, we take the ratio of the FRT values for the original
image containing just the key and that of the key’s comple-
ment. The value of the ratio obtained is then normalised
to facilitate an equal comparison over all projections. At
each bin, \(\overline{\Pi}_m(t)\), the value \(a/b\) is stored where \(a\) and \(b\)
are the projected values from either \(I\) or \(\tilde{I}\) according to
\[ \frac{a}{b} = \min \left\{ R_m(t), \tilde{R}_m(t) \right\} \quad \text{and} \quad \frac{b}{a} = \max \left\{ R_m(t), \tilde{R}_m(t) \right\}. \]

If \(a\) or \(b\) is zero, then the value stored will be zero, indicat-
ing that the key and key complement are totally uncoupled.
This is summarised as
\[
\overline{\Pi}_m(t) = \begin{cases} 
0 & \text{if } \tilde{R}_m(t) = 0 \text{ or } R_m(t) = 0 \\
R_m(t)/\tilde{R}_m(t) & \text{if } \tilde{R}_m(t) \geq R_m(t) \\
\tilde{R}_m(t)/R_m(t) & \text{otherwise},
\end{cases}
\]

for \(0 \leq t < p\).

The maximum value of the ratio will be 1 when \(R_m(t) =
\tilde{R}_m(t)\), i.e., the projection key area is maximally coupled
to the data. A measure, \(S_m\), of how a given key interacts with
the balance of the image for any slope \(m\) is given by the sum
of projection values over all translates for that \(m\), i.e.,
\[
S_m = \sum_{t=0}^{p-1} \overline{\Pi}_m(t). \tag{6}
\]

\(S_m\) is analogous to \(I_{\text{sum}}\) in the original FRT, however its
value is no longer constant for each projection. The maxi-
mum interaction value for a given \(m\) value will then be \(p\),
the minimum will be zero. This has been demonstrated for
the circle quadrant key used in Fig. 2 where the variation of
$S_m/p$ has been plotted with $m$. The mean value of $S_m/p$ is 0.2599 with a maximum value of 0.3116 and a minimum value of 0.2511 and a standard deviation of 0.0057.

Figure 4. (a) The binary image of the key from Fig. 2. White pixels give the position of known data (key), Black pixels represent unknown data to be recovered. (b) The greyscale image reconstructed from $\mathbf{f}$ for this key. (c) A plot of the variation of $S_m$ with $m$ for this key.

Only the value of a projection sum is changed by forming the ratio of the projected values from $I$ and $\mathbf{f}$. As the location of each entry in $\mathbf{f}$ is preserved, the spatial image reconstructed from the ratio values is faithful to the form of the original key geometry, as can be seen for the circle quadrant key in Fig. 4b. The weight of each projected value is scaled in proportion to the overlap between the projected image and the projection of its complement for each projected ray.

Reconstructing the ratio FRT values will give a spatial image of the relative interaction strengths, overlaid onto the underlying key shape. Normalisation of the ratio in (Eq. 5) means that the darker of the image or its complement will be the numerator in the ratio. The reconstructed image will thus mimic the spatial form of the darker component of $I$ and $\mathbf{f}$. Examples for several keys are given in the next section.

Taking the ratio of projected sums will not preserve the consistency of each projection (meaning the row sums, $S_m$, of the ratio projections, $\mathbf{R}_m$, will vary with projection angle. To ensure uniform spread of the injected redundancy for all angles, the $S_m$ values should also be as consistent as possible for a good key geometry.

6 Results for simple key shapes

We first examine simple binary spatial keys. This produces a uniform foreground versus background comparison. Simple shapes turn out to have a very selective effect on mixing the FRT projections.

Using a key comprised of two pixels in $I$ produces very little interaction, as the FRT projections are largely orthogonal. The collection of discrete FRT lines passing through any given point all have the property of crossing just once at that point. Back-projecting a single pixel mixes only a small proportion of the $p(p+1)$ back-projected values used to reconstruct the image. Keys thus need to comprise a more significant fraction of the image area to inject a useful level of redundancy as well as create significant interaction between projected areas.

Using a purely row or column oriented key can be shown to affect just one projection ($R_{tp}$ or $R_{t0}$, corresponding to the row or column projection). Because the values within the key are mixed with the complementary values in the complemented area, all other projected values will be unaffected and the row and column values themselves do not interact (because the translate direction $t$ is taken in the same direction). Using a triangular key, as shown in Fig. 5a in a $101 \times 101$ array, produces changes only in the 0, 45 and 90 degree projections with a value $S_{m}/p = 0.3862$ as shown in Fig. 5c. The key is distributed equally through all other projections which have $S_{m}/p = 0.9629$ giving a total standard deviation of 0.1004. The interaction between key and background area for this geometry is biased towards the 0, 45 and 90 degree projections. This is demonstrated by the line artifacts that arise when $\mathbf{f}$ is transformed back into the spatial domain (as shown in Fig. 5b).
A trapezoidal key, as shown in Fig. 6a in a 101 × 101 array, has a large variation of \( S_m/p \) amongst the projections, as shown in Fig. 6c. It has a mean value of \( S_m/p \) of 0.9210 and a standard deviation of 0.0929. The \( S_m/p \) values range from a maximum of 0.9804 to a minimum of 0.3862. As for the triangular key, the structure of the trapezoidal key is lost due to the biased interaction between the key and background area amongst the projections. Many artifacts are produced when \( R \) is transformed back into the spatial domain (as shown in Fig. 6b).

We are interested in circular key shapes, as shown in Fig. 2a and Fig. 7a. Such apertures arise naturally in the conversion of real CT data (where the projected imaging domain is circular as shown in Fig. 8a) onto a p × p image space where the region of compact image support is square, as shown in Fig. 8b. The redundant region of zeros provides information that can be used to improve the consistency of the reconstructed image.

The circular key, as shown in Fig. 7a in a 101 × 101 array, has very little variation of \( S_m/p \) amongst the projections, as shown in Fig. 7c. It has a mean value of \( S_m/p \) of 0.3043 and a standard deviation of 0.0072. The \( S_m/p \) values range from a maximum of 0.3335 to a minimum of 0.2623. The structure of the circular key is maintained since the interaction between the key and background area is very evenly spread amongst the projections. Very few artifacts are introduced when \( R \) is transformed back into the spatial domain (as shown in Fig. 7b).

Figure 7b gives an indication of the spatial interaction pattern for this key. This key shape has exhibited a remarkable robustness that enables reconstruction of the encrypted image [13] using an arbitrary subset of projections whose relative size is commensurate with the level of injected redundancy (given by the ratio of key area to image area). Figure 2 shows an example of this approach for the equally robust circle quadrant key analysed in Fig. 4.

Figure 9a and 9b show that a random key in a 101 × 101 array (here with approximately 50% of the image area) maintains a high level of interaction between projections yet maintains the spatial integrity of the keyed area. Figure 9c shows that the scaled row sums, \( S_m/p \), for the ratio values are very consistent for all projection angles with a mean value of 0.8582, a maximum of 0.8816, a minimum of 0.8227, and a standard deviation of 0.0099.

The same approach can be extended to evaluate the util-
Figure 9. (a) Random key. (b) Reconstruction from $\overline{R}_m(t)$. (c) A plot of $S_m/p$.

Figure 10. (a) Key based on the complement of the Lena image. (b) Reconstruction from $\overline{R}_m(t)$.

7 Conclusions and further work

The outcome of this work confirms the intuitive idea that keys that are random or have a geometry that mixes tangent angles across the projection directions (such as the circular aperture or its variants) provide the best opportunity for encrypting values that do not rely on any special projections to be recoverable. The variance in the ratio of key and key complement projected values enables a quantitative measure of the evenness with which redundancy is injected across the projection space.

The recovery of images from keyed projections was done here using linear algebra at present [11]. One aim of this work is to find a direct computational approach to unpack image data from any set of commensurate redundant projections.

8 Acknowledgments

Thanks are due to Jean-Pierre Guédon and members of the Mojette group at the University of Nantes in France who drew our attention to the use of redundancy in projections, as well as the XOR and modulo $2^n$ methods for storing summed projection values.

This work is supported by the School of Physics and the Faculty of Science at Monash University. AK acknowledges support from an Australian Postgraduate Award PhD scholarship, provided through the Australian government.

References


