Defence Science Journal, Vol. 62, No. 1, January 2012, pp. 46-50, DOI: 10.14429/dsj.62.1441

SHORT COMMUNICATION

Image Encryption with Space-filling Curves

V. Suresh and C.E. Veni Madhavan

Indian Institute of Science, Bengaluru – 560 012, India
E-mail: suresh.venkatasubramanian@gmail.com

ABSTRACT

Conventional encryption techniques are usually applicable for text data and often unsuited for encrypting multimedia objects for two reasons. Firstly, the huge sizes associated with multimedia objects make conventional encryption computationally costly. Secondly, multimedia objects come with massive redundancies which are useful in avoiding encryption of the objects in their entirety. Hence a class of encryption techniques devoted to encrypting multimedia objects like images have been developed. These techniques make use of the fact that the data comprising multimedia objects like images could in general be seggregated into two disjoint components, namely salient and non-salient. While the former component contributes to the perceptual quality of the object, the latter only adds minor details to it. In the context of images, the salient component is often much smaller in size than the non-salient component. Encryption effort is considerably reduced if only the salient component is encrypted while leaving the other component unencrypted. A key challenge is to find means to achieve a desirable seggregation so that the unencrypted component does not reveal any information about the object itself. In this study, an image encryption approach that uses fractal structures–known as space-filling curves- in order to reduce the encryption overload is presented. In addition, the approach also enables a high quality lossy compression of images.

Keywords: Space-filling curves, partial encryption, light-weight encryption, lossy compression

1. INTRODUCTION

Space-filling curves are fractal objects that arose from the fundamental works of Giuseppe Peano[1] and David Hilbert[2] in 1890's in which they formulated curves that visit every point in a unit square. Their constructions raised some fundamental questions about the understanding of dimensions of objects– that a space-filling curve, a one-dimensional object, fills a two dimensional object was paradoxical - which culminated in the founding of the field of fractals. The historical development of fractals and the contribution of Peano and Hilbert[3] are covered. Interestingly, space-filling curves comprise an important design pattern in some fundamental building blocks of life wherein reaching every part in a given volume is an important design motif – for example, vascular, renal, and respiratory systems.

Author introduces space-filling curves in the context of image encryption and compression. First, they demonstrated its usefulness in achieving a correlation preserving linear reordering of image pixels. Then uses this property of space-filling curves to arrive at a light-weight and partial encryption approach for image encryption. Light-weight implies that the encryption requires lesser effort–this is usually realised by encrypting only the perceptually sensitive regions of the image, a process also known as partial encryption. In addition to encryption, their approach also realises a lossy compression scheme for images.

2. IMAGE ENCRYPTION

Conventional encryption methods like DES, AES, etc. which are commonly used for encrypting text and binary data are not usually suited for the encryption of multimedia data primarily due to their massive volumes. This has necessitated in the study of encryption approaches that are specifically suited for multimedia content and are commonly referred to as multimedia encryption techniques. Also, multimedia objects typically have more redundancies than text and binary data which are not exploited by a direct application of the conventional approaches. In addition to their large sizes, they often require real-time processing operations such as transmission, display, etc. These properties and requirements make traditional encryption techniques inefficient from the multimedia encryption point of view and hence the need for new and efficient encryption techniques that are specific to multimedia data.

Partial encryption of multimedia content aims at reducing the encryption load given that the input sizes are much larger than what is encountered usually with text and binary encryption. Here the information is categorised into two parts. Sensitive or salient part is encrypted with regular encryption techniques while the other part is either left unencrypted or encrypted using milder encryption techniques. The strength, or rather weakness, of partial encryption is derived from the process of separating the content into perceptually significant and insignificant regions. A fundamental requirement to be met by any partial encryption scheme is that the encrypted parts must be independent of the unencrypted parts. If this does not hold, the encrypted pixels could be guessed based on their correlations with the unencrypted pixels.

As multimedia encryption systems have to deal with

Received 18 November 2011, online published 23 January 2012

voluminous data, it is preferred to have encryption techniques that are light-weight. In the original connotation of the term, light-weight means using software to perform encryption operations rather than using dedicated hardware. The rationale being–software implementations are easily upgradable and cheaper than hardware based systems. In the context of multimedia encryption, light-weight stands for encryption with lesser overheads and hence lesser effort. Thus light-weight encryption is an objective which is achieved through efficient and low cost software implementations and using techniques like partial encryption. We now give a brief overview of some multimedia encryption approaches in the literature.

Multimedia encryption techniques are many in number; an exhaustive list of these techniques is presented in a recent survey by Shiguo Lian[4]. One of the first multimedia encryption techniques is based on space-filling curves[5]. This forms the basis of one of the fundamental ideas behind image encryption –scramble or permute the pixels of the image in such a way that it becomes unintelligible for human consumption in the scrambled form (which is reversible). A related approach[6] adopted by European TV networks is to permute pixels in each line in the TV field.

By permuting a Huffman tree as in relabelling the edges of the tree, one gets another Huffman tree. Such a permutation could be achieved based on a key. The permutation could be static or dynamic. In the former, one of the possible permutations of the tree is used. In the latter, to encode each symbol one uses a random Huffman tree. Details of such variations are given[7,8]. This type of multimedia content encryption is also called as simultaneous encryption and compression: Huffman coding compresses while randomizing the tree helps in encryption. In another variation to Huffman code encryption, encryption of the perceptually significant parts based on the length of the Huffman code is suggested[9]. The assumption here is that longer codes correspond to edges and hence selectively encrypting the DCT blocks containing code longer than a specified threshold value would result in reducing the encryption load.

Yekkala & Madhavan[10] shows that encrypting just two significant bit-planes is sufficient for image security. As per the authors, the intact information in the remaining bit planes does not contribute to any significant perceptual quality. The authors also observe that encryption does not induce additional noise in least significant bit planes–the LSB plane is noisy as it is.

In the context of jpeg compression, instead of the conventional zig-zag scan, DCT coefficients in each 8 x 8 block was permuted[11,12] to achieve images that are imperceptible.

An image encryption and compression approach that uses fractal objects known as space-filling curves is presented.

3. HILBERT SPACE-FILLING CURVES

The Hilbert curve, H_{2^n}, for $n \geq 1$, is a fractal structure that is generated by the following recursive production rule:

H_{2^n}: $\rightarrow$ *rightRot*($H_{2^{n-1}}$) $\rightarrow U \rightarrow H_{2^{n-1}} \rightarrow R \rightarrow$
$H_{2^{n-1}} \rightarrow D \rightarrow$ *leftRot*($H_{2^{n-1}}$) $\rightarrow$
H_2: $\rightarrow U \rightarrow R \rightarrow D \rightarrow$
rightRot(H_{2^n}) : $\rightarrow R \rightarrow U \rightarrow L \rightarrow$
leftRot(H_2)) : $\rightarrow L \rightarrow D \rightarrow R \rightarrow$

where D, U, L and R indicate the directions taken by the curve –down, up, left and right.

Generation of Hilbert space-filling curves based on the above rule could be described as follows. To generate H_{2^n},

Copy $H_{2^{n-1}}$ to the top two quadrants
Left rotate $H_{2^{n-1}}$ and place it in the lower left quadrant
Right rotate $H_{2^{n-1}}$ and place it in the lower right quadrant
Connect the top two quadrants with an R
Connect the bottom and top left quadrants with a U
Connect the top and bottom right quadrants with a D
H_{2^n} has $2^n \times 2^n$ points and is referred to as the nth order Hilbert curve or $H(n)$

An image could be sequenced as a linear array of pixels using Hilbert curves by re-ordering its pixels chronologically as the curve visits them. In our applications, the Hilbert scan enters an image from the top row first pixel and exits it through top row last pixel. The pixels visited are listed in the chronological order and called as space-filling curve reordering of the image. Figure 1 illustrates the curve construction for different orders. The first row of the image is in the bottom in our representation.

Correlation preserving properties of Hilbert curve are well known in the context of 2-D compression. Lempel and Ziv[13] showed that Hilbert space-filling curves provide the best possible correlation preserving sequencing of 2-D objects. Matias and Shamir[5] proposed an image obfuscation scheme based on traversals on images based on space-filling curves.

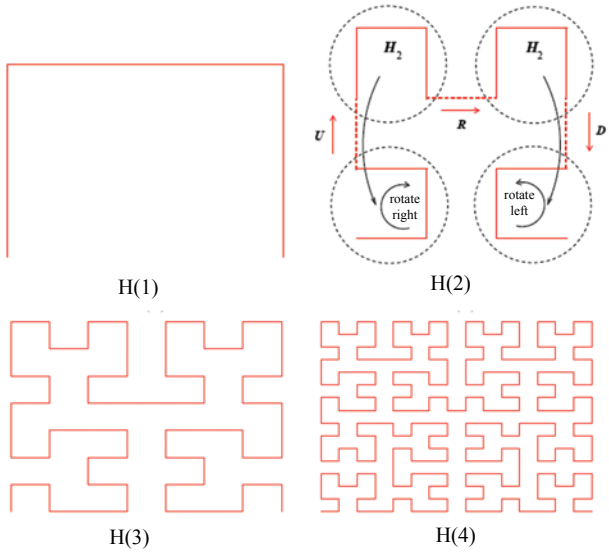

Figure 1. Hilbert curves for different orders with the construction of Hilbert curve of 2nd order based on the production rule illustrated.

Gross[14], *et al.* extended this scheme to design image space-filling curves that are specific to individual images to achieve better compression.

Owing to their correlation enhancing properties, space-filling curves have been studied in the context of image compression–especially[15,16], are in the context of a critical application like medical image compression. However, in the context of encryption– outside the above mentioned approaches,

namely[5,14]–space-filling curves have not seen an effective utilisation, especially in the context of partial encryption. Also, their potential to effect a high quality lossy compression has not been studied so far.

We first illustrate the correlation preserving property of Hilbert curves by using them to achieve linear approximations of images that have low errors. Following this, we present our partial encryption scheme that use space-filling curves. We also show that the approach also gives scope to effect high quality lossy compression of the image. In our discussions, we call the pixel sequence generated by reordering the image pixels with the appropriate Hilbert space-filling curve as the Hilbert Image.

4. LINEAR APPROXIMATION AND HILBERT CURVES

Images can be represented as linear pixel sequences by reordering the pixels as per the order in which the Hilbert curve visits them. This is far superior to writing them as sequences in the conventional row or column-major order or raster format in terms of preserving pixel-correlations in the resulting sequence. This is due to the fact each pixel's eight adjacent pixels in a 3×3 neighbourhood appear far apart in the raster sequence thereby resulting in a loss of correlation. On the other hand, Hilbert curve, upon visiting a pixel dwells in and around a pixel's neighbourhood for longer durations which results in correlation preservation to a greater degree in the linear sequence. This translates to having smoother pixel variations in the sequence generated by the Hilbert curve as against the natural ordering of pixels in the row-major order. As mentioned earlier, we refer to images generated by traversing them with the Hilbert curve as 'Hilbert images', also conventional images will be referred to as 'normal images' when used in conjunction with the term Hilbert images. Suppose an image is divided into equal sized blocks of n pixels each. Each of the blocks could be represented by a straight line using the standard least squares approximation. Thus for each block, we would get two parameters–slope and the intercept. The error values are the difference between the actual values and the values predicted by the straight line. The entire image could then be represented as a sequence of error values and the straight line parameters for each block. We note that the straight line parameters, slope and intercept, are represented in the byte range.

We illustrate the distribution of the error values and slopes for Hilbert and normal images for the red plane of standard lena image in Figs 2 and 3, respectively. Each block contains 32 pixels – a value which we use throughout. The error values are much sharper for Hilbert image than for the normal image, implying that the former is better suited for linear prediction and hence compression. This is also justified by the sharper peak for the slope distribution at zero degree for the Hilbert image when compared to a normal image. We quantify these statements in the Table 1 that compares the mean and standard deviations of Hilbert and normal images. Though the facts are presented for the standard lena image, it is representative of the general trend observed for many natural images in our experiments.

It is clear from Table 1 that for prediction errors, Hilbert images have means that are at least three times closer to zero than the normal images. Also the sharp peaks are captured by standard deviation values for Hilbert images that are typically 40 per cent lesser than the corresponding normal images'. For slopes, the mean values for Hilbert images, for all practical

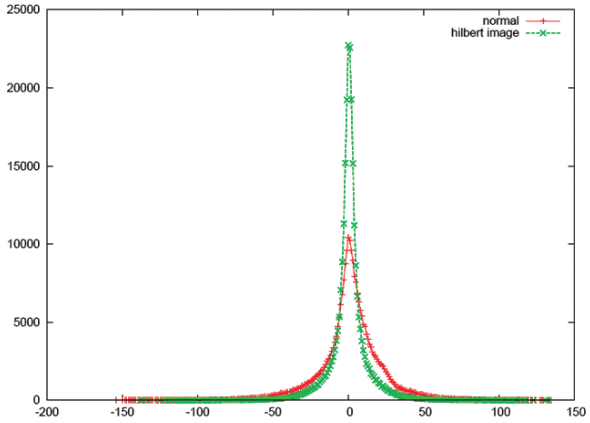

Figure 2. Distribution of errors for normal image *vs* Hilbert image. X-axis represents the error values and Y-axis represents the frequency of the error values. Note that the Hilbert distributions have sharper peaks.

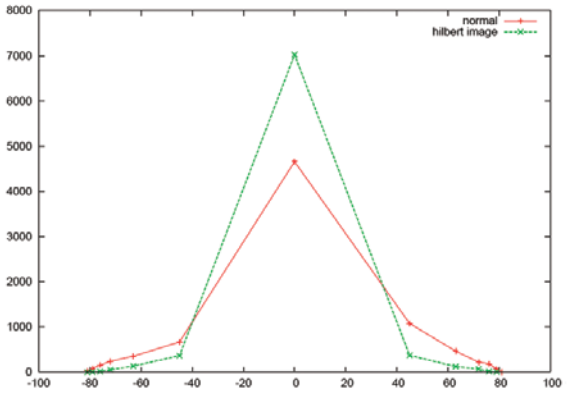

Figure 3. Distribution of slopes for normal image *vs* Hilbert image. X-axis represents the slope values and Y-axis represents the frequency of the slope values. Note that the Hilbert distributions have sharper peaks.

Table 1. Mean and standard deviation: Normal *vs* Hilbert images

Colour	Errors				Slopes			
	Mean		SD		Mean		SD	
	normal	hilbert	normal	hilbert	normal	hilbert	normal	hilbert
Red	0.47	1.58	12.40	20.81	0.07	2.87	20.59	38.55
Green	0.46	1.94	15.19	24.51	-0.02	3.78	22.78	42.46
Blue	0.50	1.73	12.73	18.79	-0.02	2.52	17.32	33.62

purposes, are zero when compared to those for normal images. The standard deviations for the Hilbert image are typically half of that of that of normal images. These provide ample evidence to the fact that Hilbert images are better suited for prediction with linear curve fitting models. In fact the error values of the Hilbert images could be discarded and yet fairly accurate reconstructions of the image could be obtained. This is illustrated in Fig 4.

Figure 4. Image generated by dropping the errors and just using the straight line parameters. Hilbert image (b) retains better clarity when compared to the normal image (a). The corresponding errors when viewed as images. The errors of the normal image (c) reveals more about the image than its Hilbert counterpart (d).

If the block sizes are increased, the quality of the approximation drops and as a result the information content of the error values increase. Lesser sized blocks would lead to lower errors. However, the quality of approximation for Hilbert images is better when compared to normal images irrespective of the block size. Figure 5 shows images generated with a block size of 64 – each block has 64 pixels as against Fig 2 which is shown for block size of 32. It is clear that the quality of the approximation deteriorates much faster for normal image than for Hilbert image. The choice of 32 as block size was arrived at by experimenting with different block sizes. The quality of images resulting from block size of 32 provides a reasonable trade-off between high quality approximation and the encryption load for images.

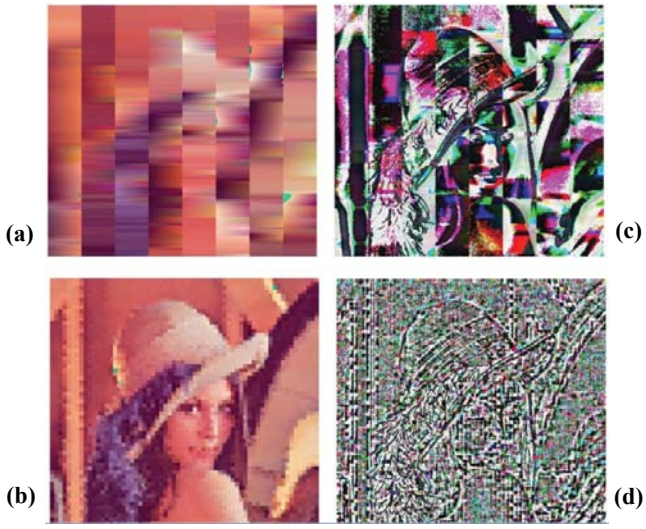

Figure 5. Same as Fig 4 but with block size of 64. Though a sharp drop in quality is perceptible, Hilbert image, (b) has a better perceptibility than normal image (a). The drop in quality results in significant errors; (c) & (d) shows that this is higher for the normal image compared to the Hilbert image.

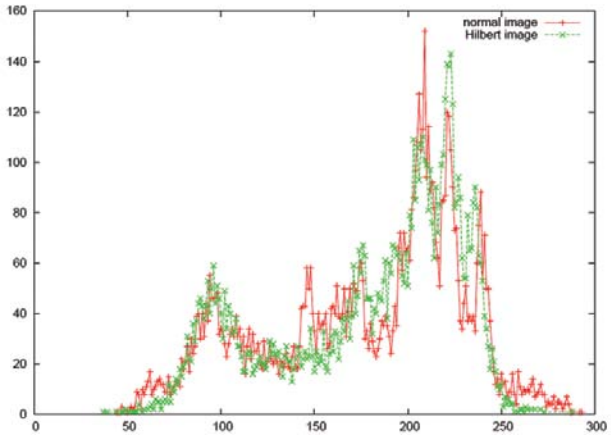

Figure 6. Distribution of intercepts for normal image *vs* Hilbert image. X-axis shows the intercept values and Y-axis represents the frequency of the intercept values. Unlike the error and slope distributions, the intercept distribution for the Hilbert and the normal image are similar. This shows that the intercepts, rather than the slopes or error values, carry useful information about the image.

5. ENCRYPTION AND LOSSY COMPRESSION

As a lossy compression scheme, one could compress only the straight line parameters and discard the errors. From the point of view of multimedia encryption, one needs to encrypt only the intercepts to achieve incomprehensibility. This is evident from the intercept distribution shown in Figure 6 for Hilbert and normal images. Unlike those observed for slopes and errors, these distributions are non-trivial and cannot be approximated easily. On the other hand observe that for slopes one could make a reasonable first cut approximation–all slopes are zero degree. Thus intercepts carry more meaningful information about the image when compared to the slopes; hence intercepts rather than the slopes have to be encrypted. Note that this amounts to performing a partial and light-weight encryption of the image.

Authors' approach presents the twin possibility of performing both encryption and compression on the image. By encrypting only the intercepts, one effects a partial encryption. By discarding the error values one achieves a lossy compression. The nature of the information loss is determined by the block size. Larger the block, lower is the quality of the compressed image. With smaller sized blocks, loss is lesser but the number

of intercepts to be compressed increases. Thus a trade-off is required as mentioned earlier. In the present experiment with block size 32, one gets two parameters in the byte range for each block. This amounts to a lossy compression of 1/16. Further, as all the slopes are very close to zero, the slope can be encoded efficiently to take advantage of this. Thus, the net compression is determined by the compressibility of the intercept values. In practice, depending on the nature of the image, the net compression could be much smaller than the base estimate of 1/16.

Approximations that use higher-order polynomials too yield similar results for Hilbert images. However, unlike the straight line parameters, they require more than the byte range for their representation and the errors too tend to increase beyond the byte range. Hence in practice, representation of blocks as linear approximations using straight line parameters turns out to be adequate.

The algorithm used for encrypting the intercepts could be a conventional algorithm like DES or AES. Our approaches effectiveness is not affected by the choice of the encryption algorithm as the main objective in partial encryption is in segregating the image into a relatively smaller part that contains data corresponding to the perceptual quality of the image while the insignificant part could be left alone. In the present case, the unencrypted part would correspond to the lower right image in Fig 2.

6. CONCLUSION

Authors have applied Hilbert's space filling curves to sequence images and studied the correlation preserving properties of the resulting pixel sequences. They showed that Hilbert images are ideal for linear piece-wise linear representations of images. They showed that the parameters of the linear-approximation could be used to realise an effective partial image encryption as well as a quality preserving lossy compression.

REFERENCES

1. Peano, G. Sur une courbe, qui remplit toute une aire plane. *Mathematische Annalen*, 1890, **36**, 157-60.(in German)
2. Hilbert, D. Uber die stetige Abbildung einer Linie auf ein Flachenstuck. *Mathematische Annalen*, 1891, **38**, 459-60. (in German)
3. Peitgen, Heinz-Otto; Jurgens, Hartmut & Saupe, Dietmar. Chaos and fractals: New frontiers of science. Springer-Verlag, New York, 1992.
4. Lian, Shiguo. Multimedia content encryption, techniques and application. CRC Press, 2009.
5. Yossi, Matias & Adi, Shamir. A video scrambling technique based on space filling curves. *In* Proceedings of the Theory and Applications of Cryptographic Techniques on Advances in Cryptology, CRYPTO 87. Springer-Verlag, 1988, pp. 398-417.
6. European committee for electrotechnical standardization (CENELEC). Access Control System for the MAC/Packet Family: EUROCRYPT. European Standard EN 50094. Brussels: CENELEC. 1992.
7. Wu, C. & Kuo, C.-C.J. Efficient multimedia encryption via entropy codec design. *In* International Symposium on Electronic Imaging (SPIE), San Jose, CA, USA, 2001, **4314**, pp. 128-138.
8. Wu, C. & Kuo, C.-C.J. Fast encryption methods for audiovisual data confidentiality. SPIE Photonics East - Symposium on Voice, Video and Data Communications, Boston, MA, USA, 2000, **4209,** pp. 284-295.
9. Yekkala, Anil Kr.; Udupa, Narendranath; Bussa, Nagaraju & Veni Madhavan, C.E. Lightweight encryption for images. International Conference on Consumer Electronics (ICCE), 2007, Las Vegas, USA, pp. 1-2.
10. Yekkala, Anil & Veni Madhavan, C.E. Bit plane encoding and encryption. PReMI 2007, LNCS **4815**, 2007, pp. 103-10.
11. Tang, L. Methods for encrypting and decrypting MPEG video data efficiently. *In* the 4th ACM International Multimedia Conference, Boston, MA, USA, 1996, pp. 219-30.
12. Tosun, A.S. & Feng, W.-C. Efficient multi-layer coding and encryption of MPEG video streams. *In* the IEEE International Conference on Multimedia and Expo, New York, NY, USA, 2000, **1**, pp.119-122.
13. Lempel, Abraham & Ziv, Jacob. Compression of two-dimensional data. *IEEE Trans. Infor.Theory*, 1986, **32**(1), 2-8.
14. Gross, M.; Hopgood, F.R.A.; Dafner, Revital; Cohen-or, Daniel & Matias, Yossi. Context-based space filling curves. *Eurographics*, 2000, **19**(3), 209-18.
15. Liang, J.; Chen, C.; Huang, C. & Liu, L. Lossless compression of medical images using Hilbert space-filling curves. *Comput. Med. Imaging Graphics*, 2008, **32**(3), 174-82.
16. Maniccam, S. S. & Bourbakis, N.G. Lossless image compression and encryption using SCAN. *Pattern Recognition*, 2001, **34**(6), 1229-245.

Contributors

Dr V. Suresh obtained his PhD and MS from Indian Institute of Science (IISc), Bengaluru. Currently working as a Research Associate in the Department of Computer Science and Automation, IISc, Bengaluru. His interests include: Data mining and cognitive science.

Prof C.E. Veni Madhavan obtained his BE and ME from Madras and Pilani respectively and PhD from IISc, Bengaluru. He is a Professor in the Department of Computer Science and Automation, IISc, Bengaluru. He has published over 70 papers, delivered over 100 invited talks, guided 14 PhD, 10 MS, and 80 ME theses. His interests include: Algorithms, cryptography, and cognitive science.