Space Filling Curves in Steganalysis pp. 28–37 in Edward J. Delp III, Ping Wah Wong (Eds.): Security, Steganography, and Watermarking of Multimedia Contents VII, January 17–20, 2005, Proceedings of SPIE, San José, CA, 200

Space Filling Curves in Steganalysis

Andreas Westfeld

Technische Universität Dresden, 01062 Dresden, Germany

ABSTRACT

We introduce a new method to increase the reliability of current steganalytic techniques by optimising the sample order. Space filling curves (e. g., Hilbert curve) take advantage of the correlation of adjacent pixels and thus make the detection of steganographic messages with low change densities more reliable. The findings are applicable, but not limited to LSB steganalysis.

An experimental comparison of five different sampling paths reveals that recursive principles achieve by far the best performance. All measures, such as mean distance, median autocorrelation, and the ability to detect even tiny modifications show substantial improvements compared to conventional methods. We elaborate the relationship between those parameters and quantify the effectiveness with a large test database of small images, which are usually hard to detect.

Apart from quantitative advances, visualisation of steganalytic measures can also gain from the application of reverse space filling curves.

Keywords: Steganalysis, space filling curve, Hilbert curve

1. INTRODUCTION

Steganography is the art and science of invisible communication. Its aim is the transmission of information embedded invisibly into carrier data. The goal of steganalysis is to discover steganographic alterations to carrier data.

The carrier data can be, for example, image or audio files. These files share a common property that adjacent samples differ less than more distant ones. Early steganalytic methods solely regarded histograms and ignored those local correlations entirely (e. g., Chi-square attack[1]). More recent methods, such as Pairs Analysis,[2] RS,[3] and Sample Pairs,[4] consider the neighbourhood of samples. However, the correlations are not reflected in an optimal way, because the samples are evaluated row by row. This paper elaborates that recursive space filling curves can profit from two-dimensional correlations best and thus increase the performance of well-known steganalytic techniques to its maximum. Other researchers already experimented with the way groups of pixels are assembled. Fridrich suggested to use 2×2 squares of pixels instead of 4×1 slices in the RS attack.[3] Ker continued and came up with new proposals to exclude non-continuous pixels from Pairs Analysis, and to enlarge the sampling area for RS.[5] However, we consider that employing a space filling curve ultimately solves the sampling order problem.

LSB steganography is the most researched and well known steganographic method. Because of this, attacks on this method are especially useful for demonstration of the success of space filling curves. Their usefulness is, however, not limited to the detection of LSB steganography.

The following section gives an overview, which transformations are possible with space filling curves. Section 3 compares the conventional scan path (row by row) with four different optimisations. We will see that recursive scan paths perform best. To set an example, Section 4 describes the application of space filling curves for Pairs Analysis. The last section summarises and gives an outlook.

2. APPLICATION OF SPACE FILLING CURVES

A space filling curve is a continuous map of a one-dimensional interval into a two-dimensional area (plane-filling) or a three-dimensional volume. David Hilbert, a German mathematician, invented a simple space-filling curve known as the Hilbert curve, which fills a square. The Hilbert curve can be simply encoded with the initial string L and the following string rewriting rules[6]

$$\begin{aligned} L &\longrightarrow +RF - LFL - FR+ \\ R &\longrightarrow -LF + RFR + FL- \\ F &\longrightarrow \text{go one pixel forward} \\ + &\longrightarrow \text{turn right} \\ - &\longrightarrow \text{turn left} \end{aligned}$$

These rules terminate after a specific recursion depth.

2.1. Turn an image into a sequence

Figure 1 shows the well-known Hilbert curve for the recursion depths 1, 2, and 3. The bold enumeration follows

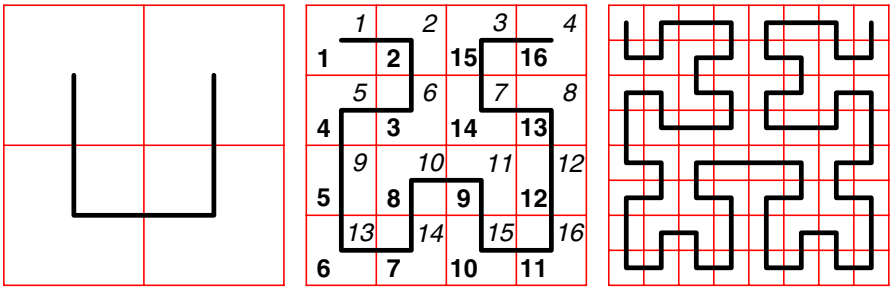

Figure 1. Hilbert curves for the recursion depths 1, 2, and 3

the curve and the italic follows the rows. We will use both to explain permutations later. Using the first curve, we can scan 2×2, with the second 4×4, and with the third 8×8 pixels. For larger images we need to increase the recursion depth according to the size.

For an image with the dimensions x and y (in pixels), a recursion depth of $\lceil \log_2 \max(x, y) \rceil$ is adequate. For example, an 800×600 image requires a Hilbert curve with a depth of 10, which is sufficient for up to 1024×1024 pixels. Positions of the Hilbert curve outside the image are ignored and do not contribute to the resulting sequence of pixel values.

Figure 2 shows a second version of the Hilbert curve. With these three curves for the recursion depth 1, 2, and 3, we can scan images with up to 3×3, 9×9, and 27×27. As before, we have to increase the recursion depth for larger images. For an image with the dimensions x and y (in pixels), a recursion depth of $\lceil \log_3 \max(x, y) \rceil$ is sufficient. An 800×600 image requires a Hilbert 2 curve with a depth of 7, which is enough for up to $2\,187 \times 2\,187$ pixels.

The 6×4 images in Figure 3 show how we can adapt the first version of the Hilbert curve with depth 3 or the second version with depth 2 to the image format by skipping the curve's positions outside the rectangle.

In the following example, we bring the pixels of a 4×4 image into a Hilbert 1 sequence. After scanning the pixels row by row into a sequence, we apply the following permutation*. The upper row denotes the old positions of the elements, the lower their new positions:

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 1 & 2 & 15 & 16 & 4 & 3 & 14 & 13 & 5 & 8 & 9 & 12 & 6 & 7 & 10 & 11 \end{bmatrix}.$$

*bold enumeration in Figure 1 read row by row

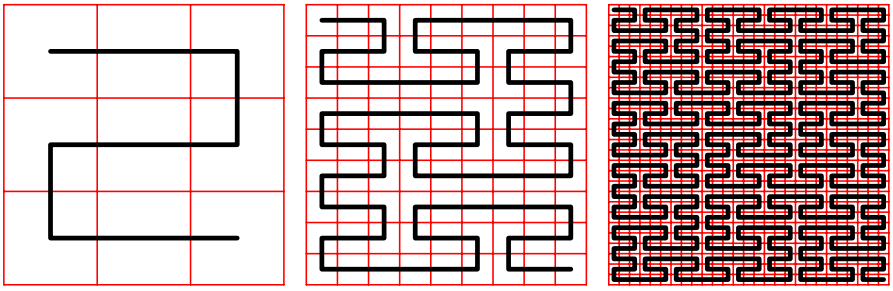

Figure 2. Version 2 of the Hilbert curve for the recursion depth 1, 2, and 3

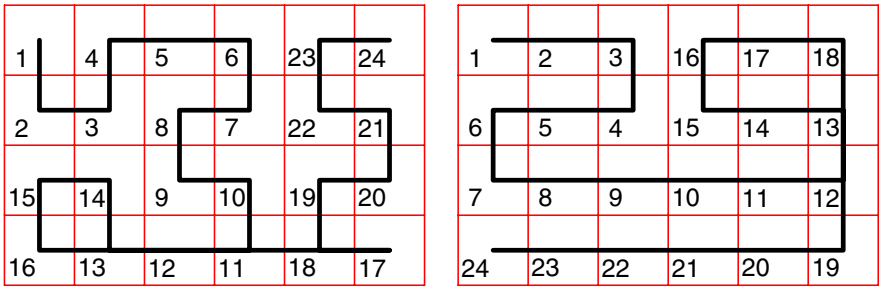

Figure 3. Cropping for format adaptation of version 1 and 2 of the Hilbert curve

The advantage is that the image is probed "nest by nest," i. e., in small, tightly coupled groups of pixels now. Consecutive elements in the sequence show a stronger correlation after the permutation. We will look at the correlation in Section 3 more thoroughly.

2.2. Turn a sequence into an image

The opposite case visualises a sequence as a plane, so that we can judge the image by appearances even if the relation to original pixels cannot be recovered or such a relation never existed (as in audio files, for example).

In the next example, we will take a sequence of the length 16 and represent it visually with a Hilbert 1 sequence. First we apply the following inverse permutation[†]:

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 1 & 2 & 6 & 5 & 9 & 13 & 14 & 10 & 11 & 15 & 16 & 12 & 8 & 7 & 3 & 4 \end{bmatrix}.$$

The resulting sequence is shown row by row as a squared 4×4 image. When visualising a sequence we will notice that in most cases the Hilbert curve is not completely used. For a sequence of the length n we use $\lceil \log_2 \sqrt{n} \rceil$ for the recursion depth (resp. $\lceil \log_3 \sqrt{n} \rceil$ for the second version of the curve).

3. COMPARISON OF DIFFERENT SCAN SEQUENCES

In this section, we will examine different scan sequences for steganalysis and their ability to keep the present correlation. In this process we will answer some questions: Why does steganalysis profit from high correlation? Are recursive scan principles superior to others? Which version of the Hilbert curve yields better results?

It is easy to answer the first question: The inherent structure of images causes a correlation of adjacent pixels. Steganography, especially the replacement of least significant bits by independent message bits, destroys certain

[†]italic enumeration in Figure 1 read along the curve

structures in the image. Steganalysis with higher order statistics utilises the correlation of adjacent pixels to prove the loss of structure and detects steganography by this means.

The stronger the present correlation before embedding, the clearer we will recognise particularities of steganograms. The correlation depends on the scanning sequence, particularly on the spatial (Euclidean) distance of the pixels. However, the conventional row by row sequence is not optimal in terms of distance.

The common scan order is row by row. To scan pixels row by row, we just read them one after another from the image file, possibly after a decompression step. The downside is that the scan path jumps after each row to the beginning of the next row (cf. Figure 4). The correlation between the pixels before and after a return is

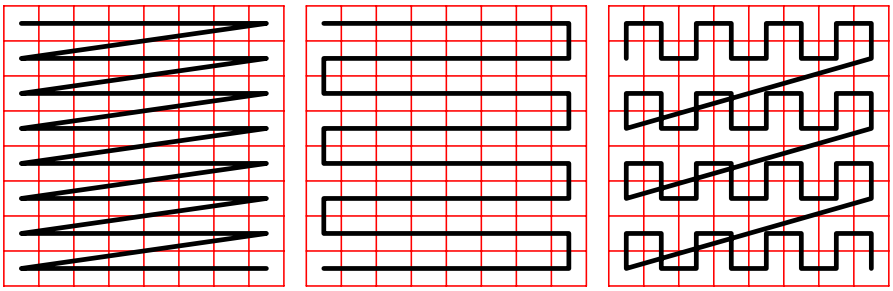

Figure 4. Row by row, slalom, and meander scan

small.

The second variation in Figure 4 turns around after each row and changes the scan direction, continuing a slalom course to the end of the image. The distance between consecutive elements in the sequence is always one pixel.

However, the slalom course has a drawback, too, which it shares with the row by row scan order: if we collect the pixels in a row we go away from previous samples on the shortest path. The earlier and faster the distance grows, the more rapidly the correlation decreases. For a more slowly growing distance it is more convenient to follow a meander path.

Pairs Analysis[2] scans an image multiple times and collects values dependent on pixels into a vector. In Sect. 4 we will go more into the details of Pairs Analysis. Figure 5 shows histograms of the Euclidean distances of pixels that are consecutively evaluated by Pairs Analysis. However, only the top of the bars is marked by a dot. Otherwise the about 32,000 bars in each histogram would draw a black area and larger bars covered completely the smaller ones. 536 greyscale images with the size 341×454 contributed to each histogram. The maximum distance of two pixels is $\sqrt{341^2 + 454^2} = 567.8$. Scanning in either Hilbert sequence shifts the mass of the frequencies to shorter distances. The density curve is more suitable for comparison. We estimate the density using a triangular window and a width of 20. Table 1 lists the number of short distances and the mean distance for the different scan orders. The column "≤ 3," e. g., comprises the distances 1, $\sqrt{2}$, 2, $\sqrt{5}$, $\sqrt{8}$, and 3 from the histograms in Figure 5.

Table 1. Number of small distances and mean distance for different scan orders

	$= 1$	≤ 3	≤ 6	≤ 10	Mean distance
Row by row	24,406,584	36,031,059	43,343,341	48,659,685	35.01
Slalom	25,758,228	38,960,877	47,007,036	52,768,368	24.60
Meander	28,842,260	45,392,457	52,791,135	57,743,123	24.76
Hilbert 1	29,384,613	52,513,152	66,189,063	73,689,384	5.19
Hilbert 2	29,612,378	51,551,806	65,517,080	72,905,013	5.66

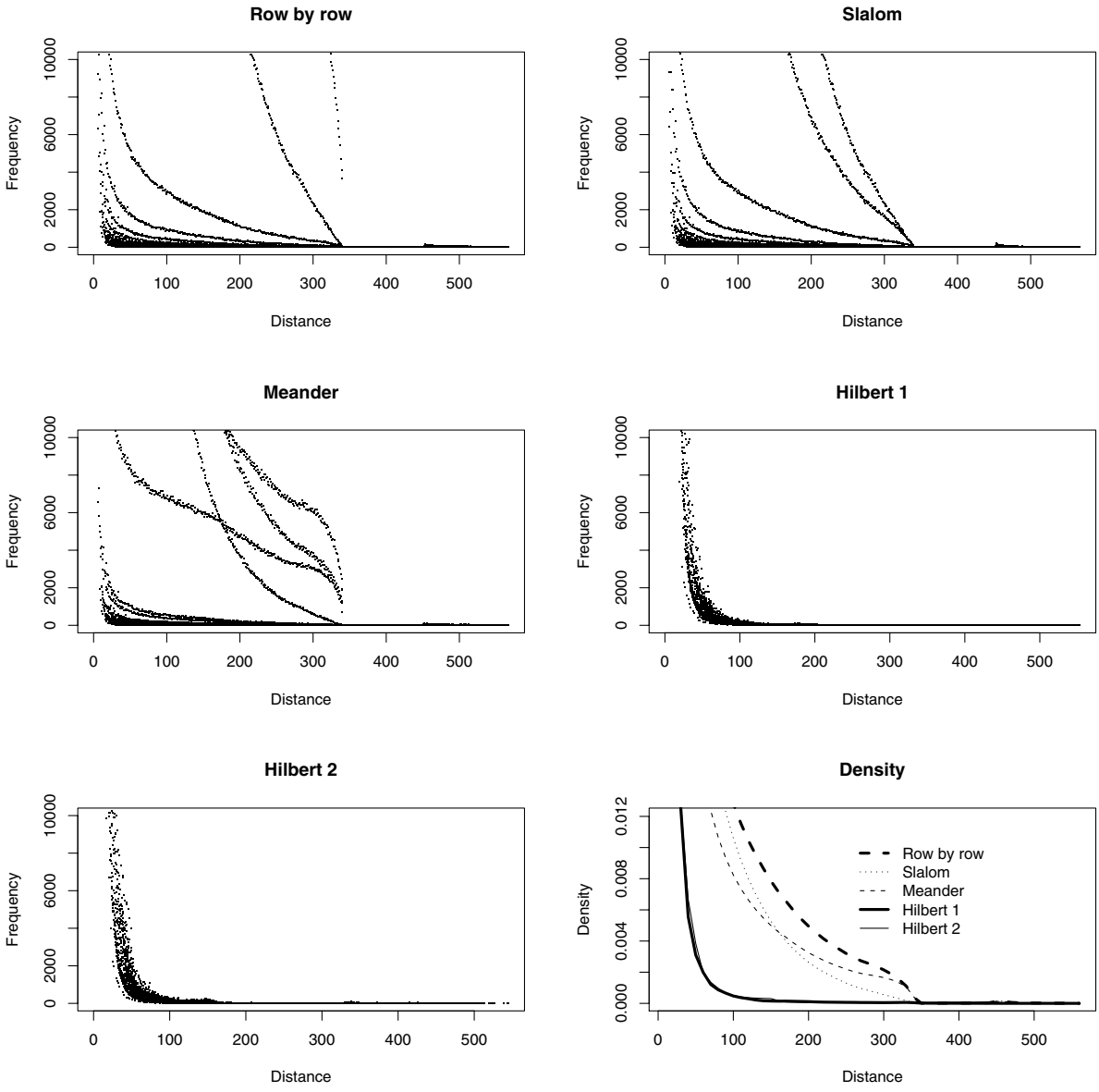

Figure 5. Pairs Analysis: Histogram of the Euclidean distances

In a second experiment we consider 536 smaller greyscale images with 213×284 pixels. We measure the autocorrelation in the sequence of scanned values $a_1, \ldots, a_n$. For the lag $l = 1, \ldots, 300$, we determine the correlation between the sequences $a_1, \ldots, a_{n-l}$ and $a_{1+l}, \ldots, a_n$. Figure 6 depicts the median of the 536 curves for each of the five different scan sequences. The winner is the Hilbert 1 curve in the first version closely followed

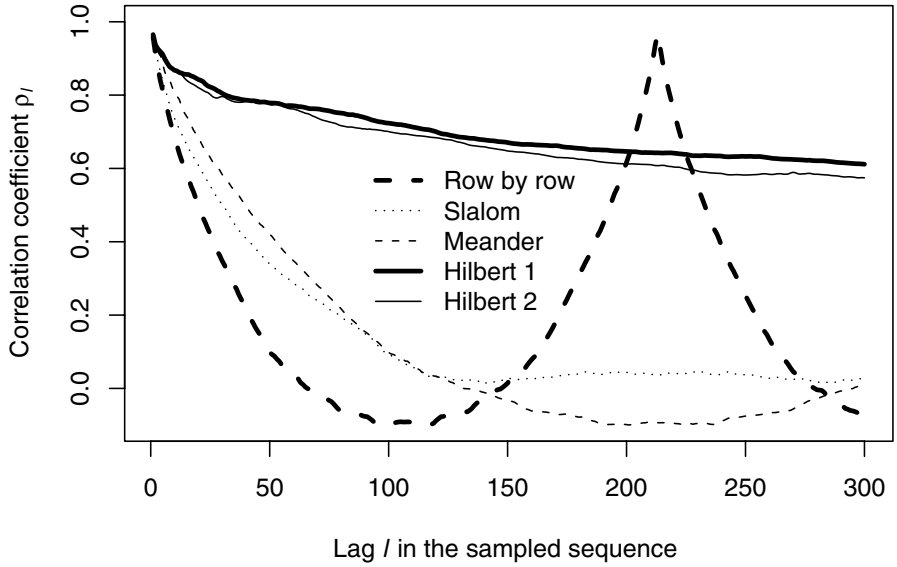

Figure 6. Median of the autocorrelation coefficients for 536 test images (213×284 pixels) for five scan sequences

by its second one. Probably the lower area increase per recursion layer is an advantage, at least for the images used here. As expected, the row by row scan has the largest decrease of correlation. This curve has a clearly visible periodicity. After a distance of one row ($l = 213$), the curve has a local maximum in the correlation. It has a distance of one pixel along the side of two consecutive rows then. The correlation of slalom drops faster than the meander at the beginning, but later exceeds it—apparently because of the row skip in the meander. Slalom and meander have a period of two row lengths, since after $l = 426$ pixels the left border of the image is reached again.

4. EXAMPLE: PAIRS ANALYSIS

Pairs Analysis is a frequently used detection method for steganography. It is characterised by its ability to detect steganography with diluted changes, uniformly straddled over the whole carrier medium. In addition, it can estimate the length of the embedded message.[2] We apply this method to images with a greyscale palette here. Every pixel represents one of 256 different levels of brightness and is encoded in one byte.

Pairs Analysis creates binary vectors z_n, $(n = 0, 1, \ldots, 127)$ for pairs of grey values $(2n, 2n+1)$, which differ only in the least significant bit, i. e. $\{(0,1), (2,3), \ldots, (254, 255)\}$. To gather all these grey values, the image is scanned 128 times. Likewise another 128 vectors z'_n are created for $(2n+1, 2n+2)$, the dual pairs of grey values $\{(1,2), (3,4), \ldots, (255, 0)\}$. The pixels are scanned in the order they occur in the image file, i. e. row by row:

- if the value $2n$ occurs, z_n is appended by 0,
- if the value $2n+1$ occurs, z_n is appended by 1,
- if the value $2n+1$ occurs, z'_n is appended by 0, and
- if the value $2n+2$ occurs, z'_n is appended by 1.

These 2×128 vectors are concatenated to two vectors:

$$\begin{aligned} z &= z_0 z_1 z_2 z_3 \dots z_{127} \text{ and} \\ z' &= z'_0 z'_1 z'_2 z'_3 \dots z'_{127} \end{aligned}$$

(z'_{127} refers to the values 255 and 0).

If we look at these vectors it turns out that the two vectors scanned from an image without embedded message both mainly contain homogeneous pairs (00 and 11). When scanned from an image with steganographic payload, the proportion of inhomogeneous pairs (01 and 10) increases in z while most pairs in z' are still homogeneous.

536 greyscale images from a digital camera were investigated. We reduced their size by the ratio of 5:1 (341×454) and 8:1 (213×284) to ensure that possible compression artefacts of the initial JPEG encoding are effectively removed.[7]

The diagram in Figure 7 shows the receiver operating characteristic (ROC), which opposes the probability of

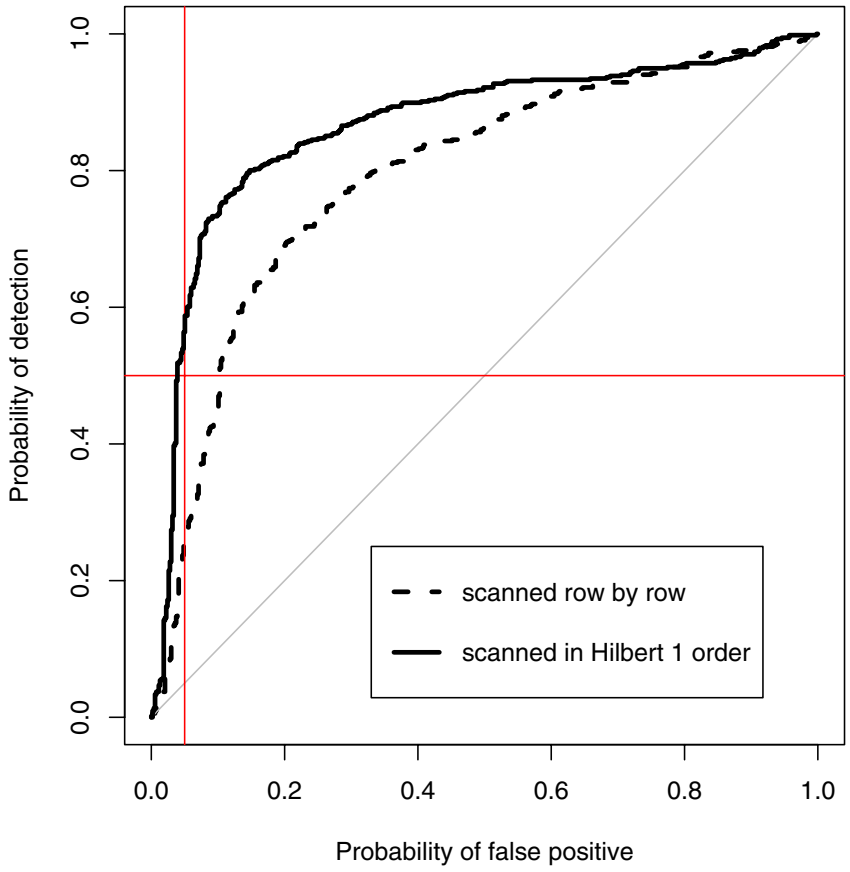

Figure 7. ROC curve (Receiver Operating Characteristic) for 2×536 test images (213×284 pixels)

false positives α to the probability of detection $1 - \beta$. The dashed curve represents the result of Pairs Analysis for images with 5 % of the capacity used and scanned row by row. The solid curve is for the same images scanned with the Hilbert 1 sequence. We can measure the quality of the steganalytic method in two ways:

1. The area bounded by the ROC curve and the diagonal should be as large as possible. The reliability ρ (doubled area) is 0.58 for the dashed curve and 0.73 for the solid curve.

2. The probability of false positives α should be at most 5 % for a detection rate of 50 %.[5] For the dashed curve it is 10.3 %, while with the proposed scanning sequence the false positives are reduced to 3.9 % (solid curve). Table 2 summarises further results.

Table 2. Increased reliability by scanning along a Hilbert 1 curve

Capacity (%)	341×454 pixels				213×284 pixels			
	ρ		$\alpha(\beta = 0.5)$		ρ		$\alpha(\beta = 0.5)$	
	in rows	SFC	in rows	SFC	in rows	SFC	in rows	SFC
1	0.2124	0.2626	0.3321	0.2761	0.1456	0.1989	0.3750	0.3284
2	0.4059	0.4774	0.1922	0.1437	0.2727	0.3794	0.2854	0.1996
3	0.5537	0.6383	0.1157	0.0690	0.3873	0.5292	0.2146	0.1157
4	0.6681	0.7481	0.0728	0.0410	0.4934	0.6463	0.1474	0.0616
5	0.7572	0.8188	0.0485	0.0280	0.5842	0.7308	0.1026	0.0392
10	0.9407	0.9680	0.0093	0	0.8479	0.9155	0.0317	0.0112
15	0.9871	0.9920	0	0	0.9356	0.9785	0.0112	0.0019
20	0.9966	0.9973	0	0	0.9631	0.9903	0.0075	0.0019
50	1	1	0	0	0.9936	0.9960	0.0019	0.0019

$\alpha(\beta = 0,5)$: Probability of false positives α at 50 % detection rate $1 - \beta$
ρ: Reliability (doubled area bordered by the ROC curve and diagonal)
in rows: scanning *row by row*
SFC: scanning along a *space filling curve* (Hilbert 1 curve)

5. VISUALISATION

There is a simple visual attack[1] that inspects the steganographic values optically. This attack works only if there are saturated areas or smooth gradients in the image. Newer mathematical attacks achieve highly precise results. However, they are not as illustrative as the visual attack. In this section we will see that mathematical attacks can be supported visually, e. g. for didactic purposes.

As described in Section 2.2, we can visualise the vectors z and z' extracted by Pairs Analysis. We will visualise them in the following example for an embedding rate (capacity usage) of 0 %, 50% and 100% (see Figure 8).

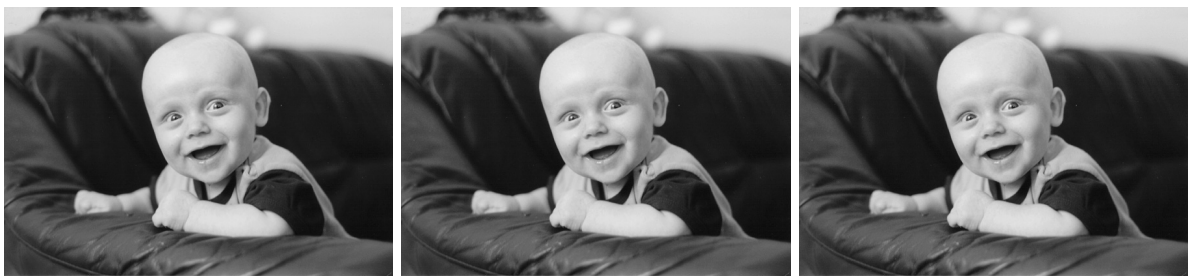

Figure 8. Image without message, with 50 %, and 100 % capacity used

The old visual attack does not help to distinguish between carrier medium and the two steganograms, since there is no saturated area and too much randomness in the gradients of this example image (see Figure 9).

Nevertheless, we can see in Figure 10 that both vectors show a similar structure for the carrier medium (top left and bottom left). To avoid the unused remainder (additional positions) of the curve, we display only that part of the Hilbert 1 curve, which we already used for scanning the pixels. We restrict the output according

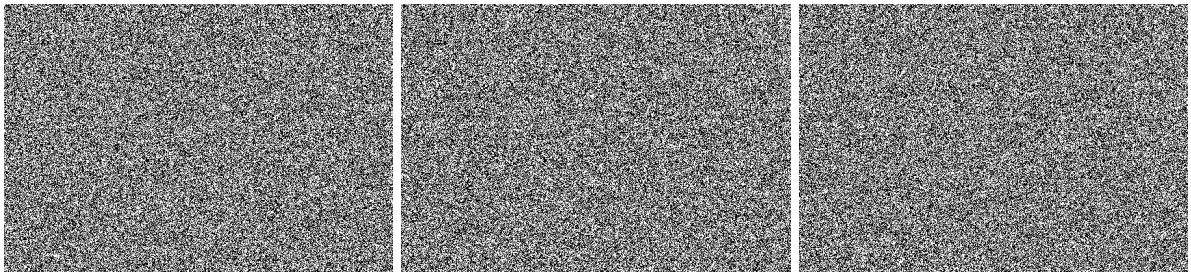

Figure 9. Visual attack[1] for Figure 8 fails

to Figure 3 to the original image format. After embedding a message, the structure in z is tailing off while it increases in z'. The fraction of homogeneous pairs in z' increases from 53.4 % (nothing embedded) to 57.9 % (100 % carrier usage). If we scan the example image in Hilbert 1 order, it increases from 54.8 % to 61.3 %. The fraction of homogeneous pairs is 50.0 % in z after embedding the maximum, independently of the scanning order. However, the difference is clearly more visible between z and z', if the pixels are scanned in Hilbert 1 order.

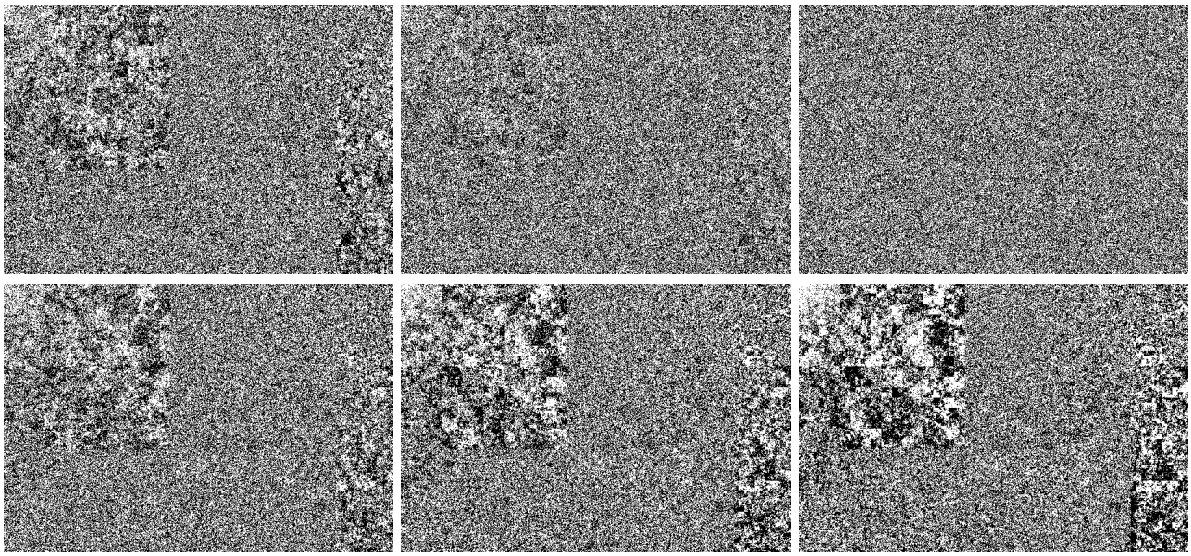

Figure 10. Visualisation of the vectors z (above) and z' (below), which the Pairs Analysis extracts from Figure 8

This method of visualisation is not restricted to the analysis of images. It is also possible to visualise z and z' from, e. g., audio files. Although these are one-dimensional, the resulting vectors can be represented in Hilbert 1 order as a square image. A possible remainder of the curve should be padded with other values that are clearly to distinguish from the elements of the sequence.

6. CONCLUSION

The experiments show that the correlation of adjacent pixels can be better exploited by recursive scanning orders. This reduces the false positives of steganographic attacks to about 1/3 compared with scanning in the order the values occur in the image file. Scanning along a space filling curve increases the reliability of steganalytic tests even for small images with low embedding rates, which are usually hard to detect.

Steganalytic measures can be visualised by reverse space filling curves. Although an earlier visual attack[1] cannot unveil the difference between carrier and steganogram, the proposed visualisation clearly shows the

dissimilar structure between the vectors z and z' created by the Pairs Attack.

Our ongoing work focuses on improving detection of other embedding functions, such as plus/minus one (Hide)[8,9] or additive noise steganography,[10,11] which are still a challenge for steganalysis. Early results are promising.

ACKNOWLEDGMENTS

The work on this paper was supported by the Air Force Office of Scientific Research under the research grant number FA8655-04-1-3036. The U. S. Government is authorised to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation there on. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the Air Force Office of Scientific Research, or the U. S. Government.

The author would like to thank Rainer Böhme for his thoughtful comments.

REFERENCES

1. A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in *Information Hiding. Third International Workshop*, A. Pfitzmann, ed., *LNCS 1768*, pp. 61–76, Springer-Verlag, (Berlin Heidelberg), 2000.
2. J. Fridrich, M. Goljan, and D. Soukal, "Higher-order statistical steganalysis of palette images," in *Proceedings of SPIE, Security and Watermarking of Multimedia Contents V. Volume 5020 of Proc. SPIE.*, E. J. Delp and P. W. Wong, eds., pp. 178–190, 2003.
3. J. Fridrich, M. Goljan, and R. Du, "Reliable detection of LSB steganography in grayscale and color images," in *Proceedings of the ACM Workshop on Multimedia and Security*, pp. 27–30, (Ottawa, Canada), 2001.
4. S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB steganography via sample pair analysis," in *Information Hiding: 5th International Workshop, IH2002 Noordwijkerhout, The Netherlands, October 7–9, 2002, Revised Papers*, F. A. P. Petitcolas, ed., *LNCS 2578*, pp. 355–372, Springer-Verlag, (Berlin Heidelberg), 2003.
5. A. D. Ker, "Improved detection of LSB steganography in grayscale images," in *Information Hiding: 6th International Workshop, IH2004, Toronto, Canada, May 23–25, 2004, Revised Selected Papers*, J. Fridrich, ed., *LNCS 3200*, pp. 97–115, Springer-Verlag, (Berlin Heidelberg), 2004.
6. D. Saupe, "A unified approach to fractal curves and plants," in *The Science of Fractal Images*, H.-O. Peitgen and D. Saupe, eds., pp. 273–286, Springer-Verlag New York, Inc., (New York NY), 1988.
7. J. Fridrich, M. Goljan, and R. Du, "Steganalysis based on JPEG compatibility," in *Proceedings of SPIE, Multimedia Systems and Applications IV, Volume 4518*, A. G. Tescher, B. Vasudev, and J. Bove, V. Michael, eds., pp. 275–280, (Denver, CO), 2001.
8. T. Sharp, "An implementation of key-based digital signal steganography," in *Information Hiding. 4th International Workshop, IHW 2001, Pittsburgh, PA, USA, April 25-27, 2001. Proceedings*, I. S. Moskowitz, ed., *LNCS 2137*, pp. 13–26, Springer-Verlag, (Berlin Heidelberg), 2001.
9. A. Westfeld, "Detecting low embedding rates," in *Information Hiding: 5th International Workshop, IH2002 Noordwijkerhout, The Netherlands, October 7–9, 2002, Revised Papers*, F. A. P. Petitcolas, ed., *LNCS 2578*, pp. 324–339, Springer-Verlag, (Berlin Heidelberg), 2003.
10. J. Fridrich and M. Goljan, "Digital image steganography using stochastic modulation," in *Proceedings of SPIE, Security and Watermarking of Multimedia Contents V. Volume 5020 of Proc. SPIE.*, E. J. Delp and P. W. Wong, eds., pp. 191–202, 2003.
11. J. J. Harmsen and W. A. Pearlman, "Steganalysis of additive noise modelable information hiding," in *Proceedings of SPIE, Security and Watermarking of Multimedia Contents V. Volume 5020 of Proc. SPIE.*, E. J. Delp and P. W. Wong, eds., pp. 131–142, 2003.