October 2003

Performance Measurement of Watermark Embedding Patterns

R. Scealy
University of Wollongong

R. Safavi-Naini
University of Wollongong, rei@uow.edu.au

N. P. Sheppard
University of Wollongong, nps@uow.edu.au

Performance Measurement of Watermark Embedding Patterns

Abstract

Segmented watermarking is an approach to multiple watermarking that can be used to acknowledge the contribution of multiple authors or to embed a fingerprint code-word, but is susceptible to cropping attacks that discard portions of the watermarked media. Careful selection of the watermark embedding pattern can increase the resilence of a segmented watermark in the presence of cropping attacks. In this paper, we consider performance measures for embedding patterns and compare the performance of several proposed embedding patterns using these measures.

Keywords

digital watermarking, fingerprinting

Disciplines

Physical Sciences and Mathematics

Publication Details

This paper was originally published as: Scealy, R, Safavi-Naini, R & Sheppard, NP, Performance Measurement of Watermark Embedding Patterns, Second International Workshop on Digital Watermarking 2003 (IWDW 2003), Seoul, Korea, October 20-22 2003, 77-85.

Performance Measurement of Watermark Embedding Patterns

Robert Scealy, Reihaneh Safavi-Naini, and Nicholas Paul Sheppard

School of Information Technology and Computer Science
The University of Wollongong NSW 2522
Australia
{rcs07,rei,nps}@uow.edu.au

Abstract. Segmented watermarking is an approach to multiple watermarking that can be used to acknowledge the contribution of multiple authors or to embed a fingerprint code word, but is susceptible to cropping attacks that discard portions of the watermarked media. Careful selection of the watermark embedding pattern can increase the resilience of a segmented watermark in the presence of cropping attacks. In this paper, we consider performance measures for embedding patterns and compare the performance of several proposed embedding patterns using these measures.

1 Introduction

In a segmented watermarking scheme [6], the object to be watermarked is divided into a series of segments, and each segment is watermarked independently. In this way, the ownership of multiple owners can be represented by embedding each of the owners' watermarks into a different segment, or a fingerprint code word can be encoded by embedding one code letter into each segment.

This method is obviously subject to a cropping attack, in which an attacker may discard some of the segments of no interest to him or her, possibly eliminating one or more watermarks or code letters from the object. Since, in general, there may be more segments than watermarks or code letters, and each watermark or code letter may be embedded multiple times, we can expect the segmented watermark to have at least some resilience against this kind of attack.

The *embedding pattern* chosen for mapping watermarks or letters to segments will affect the resilience of the overall watermark to these kinds of attacks. A good embedding pattern should allocate watermarks and letters to segments in such a way as to minimise the possibility of a watermark being eliminated or a code word being lost.

In applications where each segment represents a fingerprint code letter, we consider the case where the mark in each segment encodes both the letter itself and its position in the code word, that is, it encodes (i, c_i) for position i and letter c_i. In another approach, the letter's position in the code word might be implied only by the location of the segment in the original object. However, this

location information is likely to be lost in any significant cropping attack. The measure of resilience of the former kind of encoding is the same as in the case where each segment represents an owner: after a cropping attack, we would like to have at least one segment corresponding to each $i \in \{1, \ldots, m\}$ for a set of m owners or code words of length m.

In this paper, we consider segmented watermarking of still images by dividing them into rectangular blocks, and an attacker who selects a rectangular sub-image from the original image. We propose average-case metrics for measuring the resilience of embedding patterns in the presence of cropping attacks based on the idea of a *minimal cropping region*, and give the values of these metrics for various embedding patterns.

2 Related Work

Our problem is similar to the problem of multi-dimensional data de-clustering, used in databases to reduce latency when retrieving data from multiple disks using parallel I/O. In this problem, the time required to process a query is proportional to the greatest amount of data retrieved from a single disk.

A *range query* is a query formed by taking all of the data points that lie between a given maximum and minimum value in each dimension, i.e. a kind of "cropping" of the data set. To minimise the time required to satisfy such a query, we want the segments of data in the range query to be distributed as homogeneously as possible over all disks. If we think of the disks as watermarks, the similarity between this problem and ours becomes apparent.

The two problems are not quite identical, however. In the de-clustering problem, we wish to minimise the number of segments in any region that lie on a single disk. In our waterkmarking problem, we wish to maximise the number of different watermarks in any region. Nonetheless, an allocation that is good for one seems likely to be a good choice for the other one.

Prabhakar, et al. [5] give a survey of de-clustering methods and propose a general paradigm (the *cyclic* paradigm) for de-clustering that generalises many previously-existing schemes. They compare them by computing the average cost of a query over all possible range queries. Obviously this approach becomes impractical for large data sets, and they later resort to using a randomly-chosen subset of all possible queries. In this paper, we propose a deterministic method of choosing the subset of cropping regions to be tested such that the set chosen gives a good representation of the performance of the embedding pattern against an arbitrary attack.

Atallah and Frikken [2] define an area as *complete* if it contains at least one copy of all watermarks (equivalently, uses all disks), and *full* if it does not contain any duplicate watermarks (or disks). They then define two metrics called the *maximum non-complete area* (MNCA) and *minimum non-full area* (MNFA). They show that the optimal values for the MNCA and MNFA can be achieved only for a number of watermarks $m = 1, 2, 3$ or 5, in the sense that an "optimal" pattern is one in which any rectangle of area at least m contains all watermarks.

They furthermore show how to construct embedding patterns that have a non-optimal MNCA of $O(m)$ and a non-optimal MNFA of $\Omega(m)$. They also give an experimental evaluation of both metrics for a number of different embedding patterns taken from work in database de-clustering.

The notion of a complete area seems more applicable to the watermarking problem than the notion of a full one, since in this case we are only interested in whether or not watermarks are present and not so much in whether or not they are duplicated (the latter is more of an issue in the data de-clusterig problem). The MNCA is a measure of the worst-case performance of an embedding pattern in the presence of cropping attacks. In this paper, we will introduce metrics that measure the average-case performance of embedding patterns in terms of the completeness of cropped regions.

3 Embedding Patterns

For the purposes of this study, an embedding pattern is a map $\phi : \mathcal{N} \times \mathcal{N} \to \mathcal{A}$ from a two-dimensional space to an m-element data set $\mathcal{A} = \{0, \ldots, m-1\}$, where m is the number of watermarks to be embedded. The segment at position (x, y) in the segmentation grid will receive watermark $\phi(x, y)$.

3.1 Cyclic Methods

Many of the methods currently used for data de-clustering can be categorised as *cyclic* methods [5]. In these methods, we set

$$\phi(x, y) = (xH + yJ) \bmod m \tag{1}$$

for some integers H and J. For example, the "disk modulo" method [3] is a cyclic method with $H = J = 1$ and the "optimal" method [1] is a cyclic method with $H = \lfloor \frac{m}{2} \rfloor$ and $J = 1$. The latter method is optimal for a few special values of m in the sense that no range query of size T requires more than $\lceil \frac{T}{m} \rceil$ disks.

If we choose H and J to be relatively prime to m, we will guarantee that every element of $\mathcal{A}$ will appear in the pattern (assuming that the range of x and y is large enough). In this paper, we will always choose $J = 1$ but allow H to vary, as in [5].

3.2 Fieldwise Exclusive Method

The *fieldwise exclusive* (FX) method [4] was introduced for the case when m is a power of two, however, its definition is also valid for arbitrary m. In this method, we set

$$\phi(x, y) = x \oplus y \bmod m`, \tag{2}$$

where '$\oplus$' denotes the bit-wise exclusive-OR function.

3.3 Tile Rotation Method

It is possible for an embedding pattern to have an unbounded MNCA if it contains incomplete rows or columns, that is, an $a \in \mathcal{A}$ such that $\phi(x, y) \neq a$ for any x with fixed y, or any y with fixed x. To avoid this, we would like to ensure that every row and column of the pattern contains every watermark. We can achieve this by forming a large pattern from rotations of a basic complete pattern, which we will call the *tile rotation* method.

Let $m' = a \times b$ be the smallest composite number at least as large as m. Consider an $a \times b$ tile L consisting of all the elements of $\mathcal{A}$ in an arbitrary arrangement (note there will be empty positions if $m' > m$). Let $\mathrm{rotr}(L, i)$ denote and i-column rotation of the rows of L, and $\mathrm{rotc}(L, i)$ denote rotation of the columns similarly. Then we can define an embedding pattern by dividing the segmentation grid into $a \times b$ blocks and assigning $\mathrm{rotr}(\mathrm{rotc}(L, j), i)$ to the block at (i, j). That is, set

$$\begin{aligned}\phi(x, y) &= \mathrm{rotr}(\mathrm{rotc}(L, \lfloor \frac{y}{b} \rfloor), \lfloor \frac{x}{a} \rfloor)(x \bmod a, y \bmod b) \\ &= \mathrm{rotc}(L, \lfloor \frac{y}{b} \rfloor)(x + \lfloor \frac{x}{a} \rfloor \bmod a, y \bmod b) \\ &= L(x + \lfloor \frac{x}{a} \rfloor \bmod a, y + \lfloor \frac{y}{b} \rfloor \bmod b) \qquad (3)\end{aligned}$$

4 Measurement Methods

For the purposes of watermark detection, a segment can be considered to have been completely eliminated if there is an insufficient part of it remaining to reliably detect the watermark after cropping, and to be wholly intact otherwise. Hence we can consider all cropping to take place along the segment boundaries.

In principle, an attacker may crop an image to some arbitrary rectilinear polygon. However, non-rectangular images are of limited value and, furthermore, could not reasonably be accepted as a proof of ownership since they have obviously been tampered with. Our metrics will consider only rectangular regions to be interesting.

In general, no rectangle of the original image is any more valuable to the attacker than any other. We therefore model a cropping attack as the random selection of a rectangular area of the segmentation grid.

4.1 Minimal Cropping Regions

Ideally, we would like every area of size m or greater to contain the complete set of watermarks. However, Atallah and Frikken have shown that this is possible only for a very limited choice of m. One method of measuring the performance of an embedding pattern, then, might be to test all regions of size m, and count the number of attacks that would succeed, that is, count the number of points at which the embedding pattern fails to be optimal.

However, this can give misleading results if m has few factors since there will not be many rectangles with area exactly m and this selection of rectangles may not be very representative of the collection of possible cropping attacks. In particular, if m is prime, only $1 \times m$ and $m \times 1$ rectangles will be tested, completely ignoring attacks that take square or near-square regions.

On the other hand, an obvious way of measuring the performance of an embedding pattern would be to test all possible cropped regions, and count the number of attacks that succeed, similar to the experiments performed in [5]. However, this leads to testing many very large areas that will never fail under any reasonable embedding pattern, and very small areas that cannot possibly contain all watermarks.

We define a *minimal cropping region* for area T to be an $a \times b$ sub-image C of B such that

- if $a \leq b$ and $a \leq \sqrt{T}$, then $b = \lceil \frac{T}{a} \rceil$; and
- if $a > b$ and $b \leq \sqrt{T}$, then $a = \lceil \frac{T}{b} \rceil$.

Intuitively, the set of all minimal cropping regions for an area T is the set of all rectangles with area at least T and minimal in each dimension. For example, the minimal cropping regions for $T = 5$ are of size 5×1, 3×2, 2×3 and 1×5.

An embedding pattern ϕ is *periodic* if $\phi(x + \delta x, y + \delta y) = \phi(x, y)$ for some periods δx and δy; all of the patterns considered in this paper are periodic. Our measurements consist of placing every possible minimal cropping region at every possible position over one period of the pattern, and counting the number of incomplete regions found. This reduces the number of tests required by a linear factor compared to testing all regions, since the number of minimal cropping regions is $O(m)$ but the number of all possible regions is $O(\delta x \delta y)$ and all of the embedding patterns used in this study have $\delta x, \delta y \geq m$.

4.2 Proposed Metrics

We propose two new average-case metrics based on the concept of a minimal cropping region, and two variations of Atallah and Frikken's worst-case metrics.

The All-Exclusion (AE) Metric. We define the *all-exclusion metric* as the number of complete minimal cropping regions, divided by the the total number of minimal cropping regions. This metric gives an indication of the general robustness of the embedding pattern.

The Single-Exclusion (SE) Metric. We define the *single-exclusion* metric as the probability that a minimal cropping region will contain any given watermark. Let c_n be the proportion of minimal cropping regions that exclude n watermarks. Then we can compute the SE metric as

$$\mathrm{SE} = 1 - \sum_{n=1}^{m} \frac{c_n n}{m}. \tag{4}$$

This metric favours cropping regions that are closer to being complete (i.e. do not exclude many watermarks) and gives an indication of how evenly distributed the watermarks are.

The (modified) Maximum Non-Complete Area (MaxNCA). For ease of computation, we modify Attallah and Frikken's notion of the maximum non-complete area to incorporate minimal cropping regions. Our modified maximum non-complete area is the maximum integer N such that there exists an incomplete minimal cropping region of size N. This metric gives an indication of the largest cropping attack that might succeed. As noted in Section 3.3, this value is unbounded if the pattern contains incomplete rows or columns (which would extend indefinitely through all periods of the pattern). In our tests, our program aborted with an error if it found an incomplete minimal cropping region of some large size chosen to control the programme's running time.

The Minimum Complete Area (MinCA). Similarly, we define the *minimum complete area* as the minimum integer N such that there exists a complete minimal cropping region of size N. This metric gives an indication of the smallest cropping attack that might fail.

5 Results

We computed the values of all of the metrics described in Section 4.2 for $2 \leq m \leq 10$ for each of the embedding patterns described in Section 3.

For the cyclic method, we performed two series of tests with different step sizes H. The first has $H = 1$, i.e. it is the "disk modulo" method.

Since the pattern for $H = m - a$ is symmetric to the pattern for $H = a$, we do not need to consider H's greater than half m. If H is not relatively prime to m, the pattern will not include all watermarks. Therefore we chose the second H to be the greatest number that is relatively prime to m but not greater than half m; this is equivalent to the "relatively prime HalfM" method of Prabakhar, et al. We conjectured that this would be the best choice for H since it maximises the difference between two adjacent rows, therefore minimising the number of repetitions within a rectangle covering two or more rows. Indeed, Prabakhar et al. show results indicating that this method is superior to all of the previously-existing methods for database de-clustering.

Figures 2 and 3 show our all-exclusion and single-exclusion metrics, respectively.

Figures 4 and 5 show the maximum non-complete area and minimum complete area, respectively. Note that the FX method with $m = 6$, 7, 9 and 10 has an unbounded MaxNCA.

6 Discussion

As we might have expected from the observations made in Section 2, our results are broadly similar to those obtained by Prabhakar, et al. for data de-clustering.

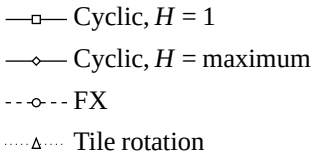

Fig. 1. Graph legend

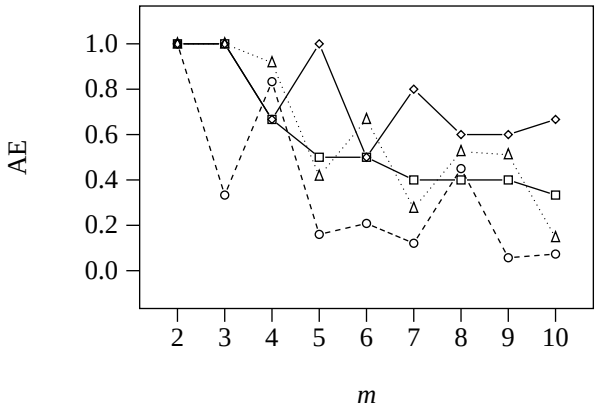

Fig. 2. All-exclusion metric

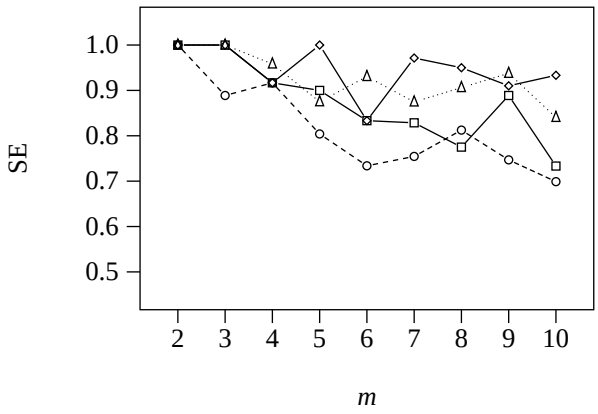

Fig. 3. Single-exclusion metric

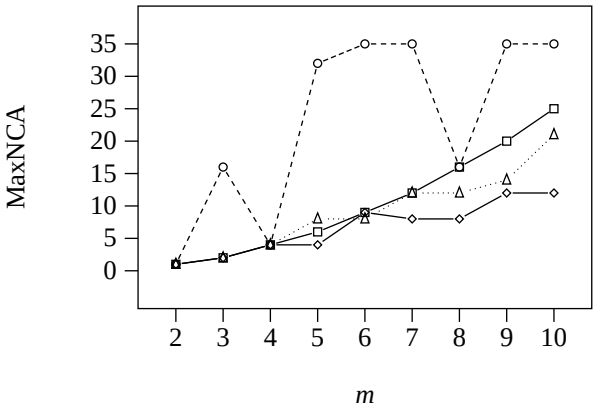

Fig. 4. (Modified) maximum non-complete area

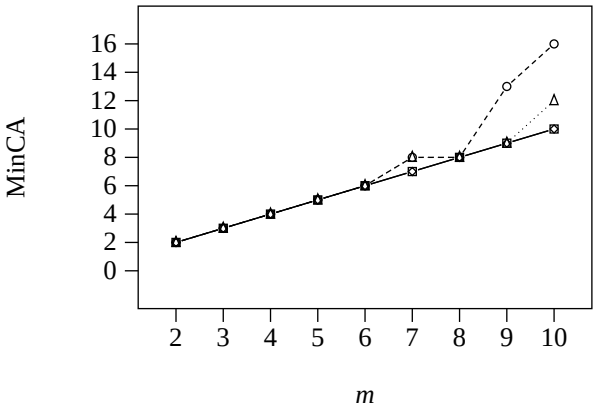

Fig. 5. Minimum complete area

The cyclic method with maximum step generally scores the best results, and always improves on the cyclic method with minimum step. The FX method scores reasonably well when m is a power of 2, but poorly for other values of m.

The new tile rotation method generally scores a little worse than the maximum-step cyclic method, but scores better for $m = 4$ and 6. In these two cases, the highest relatively prime number less than half m is just 1, meaning that the maximum-step method is the same as the minimum-step method.

On the other hand, there are dips in the score for the tile rotation method at $m = 5$ and 7, which are prime numbers. This might be expected since the basic tile from which the pattern is constructed will have an empty position if m is prime (recalling that the tile must have composite area at least as great as m). The presence of empty positions obviously reduces the effectiveness of the pattern.

7 Conclusion

We have introduced two new metrics for measuring the average-case performance of embedding patterns for segmented watermark, based on the notion of a minimal cropping region. Using minimal cropping regions substantially reduces the number of tests required for testing the average-case performance of embedding patterns as compared to the brute force approach.

As in related work, our measurements favour embedding patterns based on the cyclic paradigm, and, in particular, cyclic methods with a large step size.

References

1. K. Abdel-Ghaffar and A. El Abbadi. Optimal allocation of two-dimensional data. In *International Conference on Database Theory*, pages 409–418, Delphi, Greece, 1997.
2. M. Atallah and K. Frikken. Cropping-resilient segmented multiple watermarking. In *Workshop on Algorithms and Discrete Structures*, pages 231–242, 2003.
3. H. C. Du and J. S. Sobolewski. Disk allocation for cartesian product files on multiple-disk systems. *ACM Transactions on Database Systems*, 7:82–101, 1982.
4. M. H. Kim and S. Pramanik. Optimal file distribution for partial match retrieval. In *ACM International Conference on Management of Data*, pages 173–182, Chicago, USA, 1988.
5. S. Prabhakar, K. Abdel-Ghaffar, D. Agrawal, and A. El Abbadi. Efficient retrieval of multi-dimensional datasets through parallel I/O. In *ACM Symposium on Parallel Algorithms and Architectures*, pages 78–87, 1998.
6. N. P. Sheppard, R. Safavi-Naini, and P. Ogunbona. On multiple watermarking. In *Workshop on Security and Multimedia at ACM Multimedia*, pages 3–6, Ottawa, Canada, 2001.