Parameter Dependency and Sufficient Iterations for Limit Figures in Authentication Algorithm

Takeshi Yoshikawa, Tsutomu Da-te and Hidetoshi Nonaka
Division of Systems and Information Engineering, Hokkaido University
Kita 13, Nishi 8, Kita-ku, Sapporo, 060-8628, Japan.
E-mail: yosikawa@main.eng.hokudai.ac.jp

Abstract
In this paper, we deal with the parameter dependency for the limit figures and the sufficient number of iterations in drawing the limit figures of quadratic transformations. The structure of the limit figures depends on the coefficients of the transformation, and has turned out to be complicated. Using the property that the limit figures are one-way functions, Da-te (2001) proposed an authentication algorithm. For the purpose of verification of the securities in the authentication algorithm, we show the experimental results for some properties of the limit figures.
Keywords: quadratic transformation, limit figure, authentication, parameter dependency, sufficient iterations

1 Introduction

Behavior of iteration process of a quadratic transformation depends both on the initial position and on the coefficients of the transformation, and it is complicated in contrast with the case of a linear transformation. It has been investigated in detail (Da-te (1978)), especially in the two-dimensional homogeneous case, their limit figures have exhaustively been cleared and the structure of boundaries of the convergence region has turned out to be complicated. We also showed intuitively simple properties of limit figures in the two-dimensional inhomogeneous case (Yoshikawa (2002)).

Da-te (2001) proposed an authentication algorithm using the limit figures as one-way functions. This algorithm can detect the legitimate right holder among the persons claiming to be the copyright holder of a digital content. It is achieved by a successive refinement procedure, that is, the specification of regions in the limit figures by the authority and the response with the limit figure by the claimers.

In this paper, we examine experimentally the parameter dependency for the limit figures and the sufficient number of iterations in drawing the limit figures by this algorithm. By the parameter dependency, only one who knows the right parameters of the transformation can draw the right limit figure. The sufficient number of iterations will be determined by the trade-off between the time of an authentication process and the time for

a brute force attack. The results of this work are effective to a quantitative verification of securities in the authentication algorithm.

2 Quadratic Transformation and its DCB

In this section, we introduce a quadratic transformation, its divergence-convergence boundary (DCB), and an algorithm to illustrate DCB.

2.1 Divergence-Convergence Boundary of Homogeneous Case

An n-dimensional homogeneous quadratic transformation is written in the form:

$$x'^k = f^k(\boldsymbol{x}) = P^k{}_{rs}\, x^r\, x^s$$
$$(k = 1, 2, \ldots, n;\ r, s, = 1, 2, \ldots, n;\ \boldsymbol{x} \in \boldsymbol{R}^n;\ P^k{}_{rs} \in \boldsymbol{R}), \qquad (1)$$

where $\boldsymbol{f}$ can be considered a mapping from $\boldsymbol{R}^n$ into itself.

Many properties and canonical forms of homogeneous quadratic transformations were investigated in Date and Iri (1976).

A divergence-convergence boundary (DCB) is defined in Date (1978), and the shapes of DCBs in two dimensions are investigated and classified in detail.

For a homogeneous quadratic transformation, we introduce a convergence region C as

$$C = \{\boldsymbol{x}^{(0)} \mid \lim \| \boldsymbol{f}^m(\boldsymbol{x}^{(0)}) \| = 0 \text{ for } m \to \infty\}, \qquad (2)$$

where $\boldsymbol{x}^{(0)}$ is the coordinates of initial point. Then, we can define a divergence-convergence boundary B as

$$B = \{r(\Theta)\, \Theta \mid r(\Theta) < \infty\}, \qquad (3)$$

where $r(\Theta) = \sup\{\alpha \mid \alpha\Theta \in C\}$ for $\Theta \in S$ is a mapping from the unit sphere $S = \{\boldsymbol{x} \mid \|\boldsymbol{x}\| = 1\}$ into $\boldsymbol{R} \cup \{\infty\}$. A divergence region D is defined as $D = \boldsymbol{R}^n - B - C$.

The DCB is a limit figure, which is obtained by infinite number of iterations of a transformation.

There are many algorithms to illustrate images of DCBs, and an algorithm that gives the images more quickly by using the properties of the DCB in a homogenous case was introduced in Da-te (1978). The algorithm used in this paper is shown in the next section.

We show two examples of the approximate image of convergence regions in homogeneous quadratic transformations in Fig. 1. In these figures, the black region represents a convergence region and the white region does a divergence region. The boundary of these two regions corresponds to a DCB. In Fig. 1(a), the upper and the lower curves of the DCB are smooth. On the other hand, the left and the right curves are complicated and considered to have a self-similar structure. In Fig. 1(b), the convergence region has many spikes, and they are considered to extend to infinity.

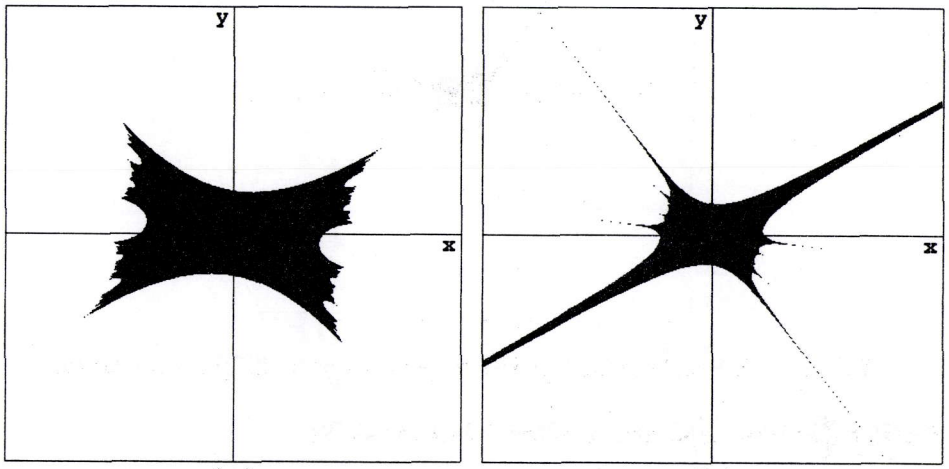
2.2 Divergence-Convergence Boundary of Inhomogeneous Case

An n-dimensional quadratic transformation is written in the form:

$$x'^k = f^k(\boldsymbol{x}) = P^k{}_{rs}\, x^r\, x^s + P^k{}_t\, x^t$$
$$(k = 1, 2, \ldots, n;\ r, s, t = 1, 2, \ldots, n;\ \boldsymbol{x} \in \boldsymbol{R}^n;\ P^k{}_{rs},\ P^k{}_t \in \boldsymbol{R}), \qquad (4)$$

where f can be considered a mapping from R^n into itself.

In an inhomogeneous case, we modify the definition of a DCB of homogenous quadratic transformations. The DCB is, intuitively, a set of initial points that neither converge to the origin nor diverge to infinity in transformation process.



(a) (b)

Fig. 1: Examples of DCB in homogeneous quadratic transformations

In this paper, we illustrate the images of DCBs by the following process.

1. choose a pixel for initial point $x^{(0)}$
2. for $m = 1, 2, \ldots, M$,
   if $|f^m(x^{(0)})| >$ INF, then $x^{(0)} \in D$,
   if $|f^m(x^{(0)})| <$ EPS, then $x^{(0)} \in C$,
   where INF ($\in R$) is a sufficiently large fixed number, EPS ($\in R$) is a sufficiently small fixed number, and M ($\in N$) is fixed.

We apply the same procedure for all pixels.

The values of INF, EPS, M are given in consideration of the programming language system or the coefficients of transformation, etc.

Fig. 2 is an example of the images of DCBs in inhomogeneous quadratic transformations. As shown this figure, in inhomogeneous cases, there exists, generally, many points of DCB on a certain straight line through the origin. The convergence region in Fig. 2 has a self-similar structure, i.e. the shape of its portion at the end of each branch is similar to the whole.

For certain inhomogeneous quadratic transformations, a set of initial points converging to a fixed point other than the origin forms a region. We call the set a boundary region in this paper. When there is a boundary region, there is a region that is neither a convergence region nor a divergence region as a limit figure.

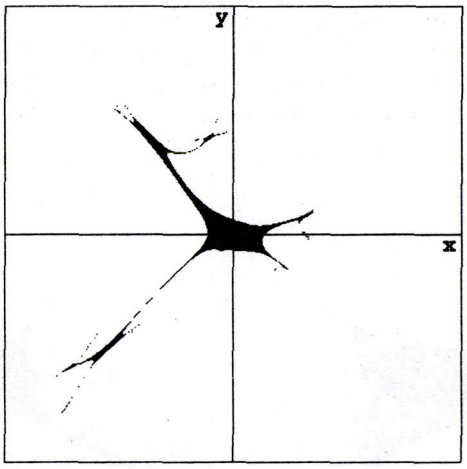


Fig. 2: An Example of DCB in inhomogeneous quadratic transformations

3 Authentication Algorithm using Limit Figures

Da-te (2001) proposed an authentication algorithm using the limit figures. This algorithm uses the property that only one who knows the right parameters of the transformation can draw the right limit figures. And it can detect the right holder among the persons claiming to be the copyright holder of a digital content.

We can assume the limit figures as the one-way functions. If we know the parameters of the transformation, we can draw the limit figures. But even if we see the limit figure, we can not obtain the parameters. For example, we can not obtain the parameters of each transformation exactly from the figures in Fig. 1 or Fig. 2.

I roughly show the authentication process in following.

The authority detects the legitimate right holder. Assume the only two know the parameters of the transformation. Only two are the authority and the right holder. The other claimers of the copyright don't know the parameters. Therefore, these parameters are the private keys.

Firstly, the authority requests certain part of the limit figure to the authors. Each author, both the legitimate right holder and the other claimers, draws the requested figure and sends it to the authority.

The authority also draws the limit figure and compares between own image and the received image from each author. If an author sends the exactly same image as the authority's, the author is the right holder. If the authority can not detect the right holder, for example, more than one authors send the right image, it requests the other part of the limit figure again.

This successive process asymptotically refines the legitimate right holder from the others.

4 Experimental Results

4.1 Parameter Dependency for Limit Figures

We perform an experiment for the verification of the security for an estimation of the transformation parameters.

We examine the difference between the limit figures of the transformation

$x' = 0.3\,x^2 - xy$,

$y' = -x^2 + 0.3xy + 2y^2$

and the limit figures of the transformation with slightly different coefficients of x^2 or xy of x':

$x' = (0.3 + \varepsilon)\,x^2 - xy$,

or

$x' = 0.3\,x^2 + (-1 + \varepsilon)xy$,

We show the results in Table 1 for each coefficient or each enlarged image.

Table 1: The number of different pixels in limit figures with different coefficients of x^2 (left) or xy (right) of x'

deviance of x^2 (ε)	the number of pixels (in 400 x 400 pixels)		
	x1 image	x2 image	x4 image
$+10^{-3}$	38	67	230
$+10^{-4}$	4	5	27
$+10^{-5}$	0	1	1
$+10^{-6}$	0	0	1
$+10^{-7}$	0	0	0

deviance of xy (ε)	the number of pixels (in 400 x 400 pixels)		
	x1 image	x2 image	x4 image
$+10^{-3}$	30	45	166
$+10^{-4}$	0	3	20
$+10^{-5}$	0	1	3
$+10^{-6}$	0	0	1
$+10^{-7}$	0	0	0

When the number of pixels is not zero, two limit figures are different each other. Then, the authority can detect the right holder.

If the value of ε is smaller values, the authority can not detect. But, by the requests of the enlarged figure, it can.

By these results, the authentication algorithm always can detect the right holder, conceptually.

4.2 Sufficient Iterations in Drawing Limit Figures

We perform an experiment for the verification of the security for a brute force attack.

We examine the number of iterations in drawing the limit figures of the following homogeneous quadratic transformation,

$x' = xy$,

$y' = x^2 + y^2$

and 9 inhomogeneous ones with different parameters P^k_t,

$x' = xy + P^1_1 x + P^1_2 y$,

$y' = x^2 + y^2 + P^2_1 x + P^2_2 y$.

These 10 transformations have the same quadratic terms.

We show the distribution of the number of iterations for each pixel in the convergence region and in the divergence region, respectively in Table 2 and Table 3.

Table 2: The distribution of the number of iterations in the convergence region

iteration	homo-	inhomogeneous								
	geneous	1	2	3	4	5	6	7	8	9
<5	104	0	0	0	0	0	0	0	0	0
<10	1524	1860	1220	1099	1001	770	625	0	0	0
<15	156	695	1622	1330	890	521	401	0	0	0
<20	0	11	56	233	115	27	30	728	0	0
<50	0	0	1	22	2	1	2	961	0	0
<100	0	0	0	0	0	0	0	0	0	418
<200	0	0	0	0	0	0	0	0	0	210
<300	0	0	0	0	0	0	0	0	0	0
<400	0	0	0	0	0	0	0	0	0	0
<500	0	0	0	0	0	0	0	0	3	0
<600	0	0	0	0	0	0	0	0	12	0
<700	0	0	0	0	0	0	0	0	218	0
<800	0	0	0	0	0	0	0	0	412	0

Table 3: The distribution of the number of iterations in the divergence region

iteration	homo-	inhomogeneous								
	geneous	1	2	3	4	5	6	7	8	9
<5	8952	9728	9963	10027	10076	10305	10578	9068	11971	11409
<10	29108	27574	27022	26901	26974	27832	28075	29006	26880	27463
<15	156	128	113	363	903	526	285	230	361	384
<20	0	4	3	22	34	18	4	4	91	77
<50	0	0	0	3	5	0	0	3	52	38
<100	0	0	0	0	0	0	0	0	0	1
<200	0	0	0	0	0	0	0	0	0	0

In the convergence region (Table 2), it is cleared that for the inhomogeneous cases, the number of iterations is increased in general.

In the inhomogeneous cases, in fact, the transformations from No.1 to No.6 have the similar linear terms. Therefore, these distributions are also similar to each other. The

other distributions are totally different. In other words, the distribution in the convergence region depends on the linear terms. It is because that in the neighborhood of the origin, the linear terms are dominant in the transformation process.

In the divergence region (Table 3), all transformation has the similar distribution. It is because that the quadratic terms are dominant far from the origin.

These results are effective to choice of the transformation requested by the authority in the authentication process.

5 Conclusion

In this paper, we cleared experimentally some properties of the limit figures in the authentication algorithm. By the parameter dependency, it is cleared that the algorithm always detects the legitimate right holder from the others. And we cleared the difference of the number of iterations between in the convergence region and in the divergence region. These results are effective to a quantitative verification of securities in the authentication algorithm.

In the authentication process, it is necessary to clear that what values of the parameters are suitable, or where part of the limit figure should the authority requests, and how do we obtain these values automatically. And we have not yet sufficiently investigated the properties of the limit figures for other type of transformations, for example, more general quadratic transformations or higher order transformations.

References

[1] Date T. (1978) Properties of Divergence-Convergence Boundaries of Quadratic Transformations, in Japanese, *IPSJ Magazine* **19, 6,** pp.507-513.

[2] Date T. (1979) Classification and analysis of two-dimensional real homogeneous quadratic differential equation systems, *J. Differential Equations* **32**, pp.311-334.

[3] Date T. and Iri M. (1976) Canonical forms of real homogeneous quadratic transformations, *J. Math. Anal. Appl.* **56**, pp.650-682.

[4] Da-te T., Yoshikawa T., Nonaka H., and Kawaguchi M. F. (1995) On Divergence-Convergence Boundary of Homogeneous Quadratic Transformations in Two Dimensions, *Proc. Third European Congress on Intelligent Techniques and Soft Computing*, pp.141-144.

[5] Da-te T., Yoshikawa T., and Shioya H. (2001) A Treatment of Limit Figures of Quadratic Transformations as One-way Functions in Authentication for Pictures or Documents of Digital Contents, *Frontiers in Artificial Intelligence and Applications*, **71**, pp.62-67.

[6] Mandelbrot B. B.(1982) The Fractal Geometry of Nature. Freeman, San Francisco.

[7] Yoshikawa T. and Da-te T.(2000) On Self-Similarity in Homogeneous Quadratic Transformations, *AIP Conf. Proc.* **517**, pp.574-579.

[8] Yoshikawa T., Da-te T., and Nonaka H. (2002) An Intuitively Simple Property of Limit Figures of Quadratic Transformations, *Int. J. Computing Anticipatory Systems*, **11**, pp.413-420.