Passdoodles; a Lightweight Authentication Method

Christopher Varenhorst

under the direction of
Max Van Kleek and Larry Rudolph
Massachusetts Institute of Technology

Research Science Institute
July 27, 2004

Abstract

This paper investigates the use of unique finger traces, or doodles, as a means of authentication in a pervasive environment. Velocity here is investigated as means to uniquely identify a doodle. A blurred distribution grid created from combined training samples and the variance across this grid is also used for recognition. These three systems used together have produced accurate results for a population of ten users. The research presented here may have applications to hand writing and drawing recognition as well.

1 Lightweight Authentication Mechanisms

New demands of authentication today are simplicity and effortlessness. Biometric technologies offer a partial solution but are be too robust for the relatively small issues such as personalization. Privacy concerns and trust also inhibit public acceptance due to the inextricable ties of biometric imprinting. The remainder of this paper discusses the design and implementation of a lightweight "passdoodle" system where a unique finger trace or doodle is used to quickly identify users in an integrated intelligent (or pervasive) computing environment. [1]

1.1 Prior Research

One of the building blocks for the proposed system was a user study conducted by Joseph Goldberg, Jennifer Hagman and Vibha Sazawal that was presented at Computer Human Interaction Conference(CHI). [1] The study found that the visual elements of written passdoodles and passwords were recalled equally well after 3 months. The paper was solely a user study where passdoodles were written on paper. Its only purpose was to examine the feasibility of a passdoodle system. [2] Numerous fields have investigated handwriting and symbol recognition but no one has implemented a passdoodle authentication system.

1.2 The Passdoodle System

The proposed passdoodle system would operate as follows. An initial doodle training period would teach the system the unique shape and movement of the user's passdoodle, in order to distinguish from other users. After this training period, the user authenticates himself to the system by tracing his doodle on a touch screen or similar technology. The emphasis here is

[1] The term passdoodle in is first found in [1]

[2] The study allowed the participants to create a passdoodle with different colors, it was found that people were unable to remember the colors of their doodle as well as they could remember the general shape of it.

Figure 1: An Example of a Passdoodle

not for authentication to personal workstations but to the technology spreading throughout our lives.

The issue of recognition prevents widespread use of the passdoodle. The length and identifiable features of the doodle set the limits of the system. Only a finite amount of computer differentiable doodles can be made. The doodle here is used as the sole means of identification. To maintain security the system cannot simply authenticate a user as the user whose recorded doodle is most similar, a minimum threshold of likeliness and similarity must be set. This prevents the use of blatant guessing to authenticate as a random user.

However speed and accuracy remain top priorities for the system. A complicated recognition design requiring a hundred training samples and a minute of computation to authenticate negates the purpose of the original pervasive design. The proposed system uses a combination of doodle velocity and distribution mapping to recognize and authenticate a doodle.

2 Methods

The doodle recognition system must allow for natural differences in the user's doodle, but still maintain enough accuracy to distinguish between different users. However, one of the difficulties that arise is that the passdoodle system identifies and confirms the identity of the user solely on the basis of that user's unique passdoodle. The passdoodle is both your user name and password.

This is made feasible by the fact that there are far more possible passdoodles than passwords: while there are only $2.08 \cdot 10^{11}$ 8 letter passwords, there are 10^{400} different 100-point doodles in a 100 x 100 grid. This does not even take into account other unique aspects of the doodle such as velocity. Of course, this is the absolute description of a doodle that cannot be replicated easily by a human. The large space of such doodles allows the recognition system to remain viable. Ingenuity of the system and the limits of human acuity ultimately determine the possible number of passdoodles.

Various features of a doodle were investigated for their usefulness in identification. Ideal features would possess a small variance within the training samples of a single user and high variance within the set of users. We investigated several methods of identification, and eventually chose three different recognition methods, distribution grid, instantaneous speed, and point variance across the distribution grid. These three features are then used together to determine the authenticity of a doodle. Any two of the three must show a high degree of similarity to confirm the identity of the doodle.

2.1 Basis of a doodle

A *doodle* is more rigorously defined as an ordered set of points, each equipped with an additional timestamp that records the time of creation in miliseconds from the first point. To create the illusion of a path an algorithm draws connecting values between points in a grid. It seems more likely that a doodle would follow the same path as a previous doodle, rather then have the exact sample points. Due to processing constraints the time interval between sample points dynamically change with current conditions.

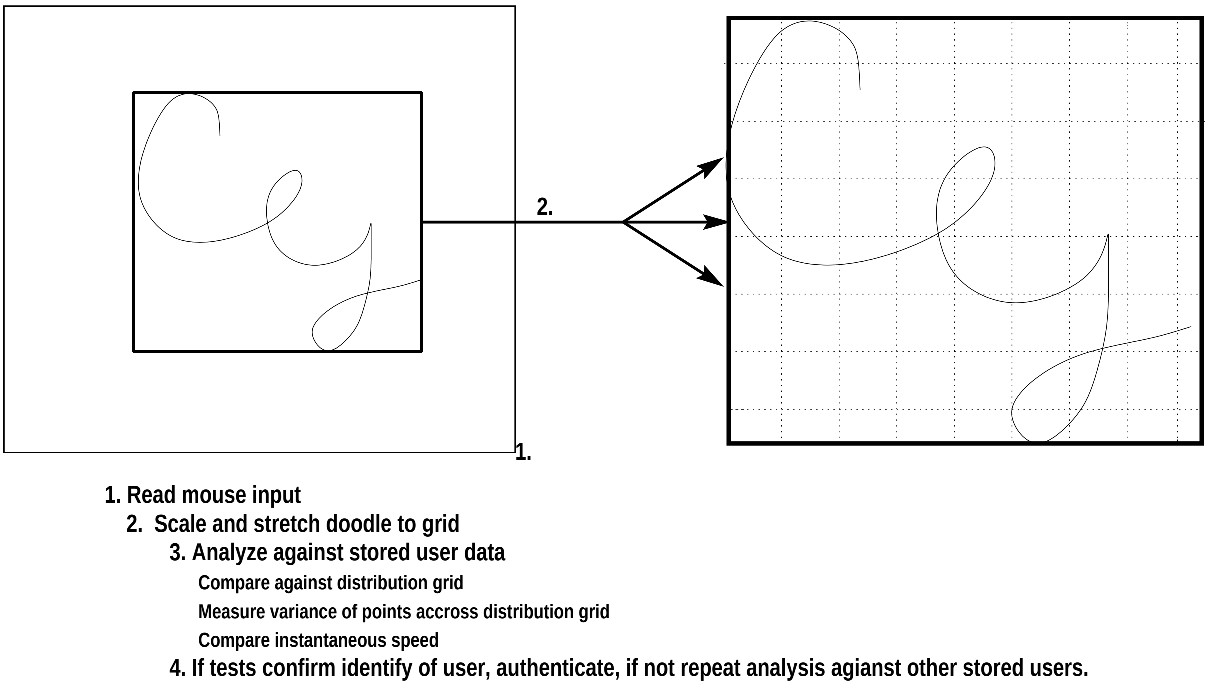

Figure 2: Overview of the authentication process

2.2 Doodle distribution grid

In the pervasive environment, a simple and direct computation method is key. The recognition system begins by boxing the doodle based on its high and low points, stretching it to a grid (this is know as canonicalization) and combining the doodles of various training samples to arrive at something similar to the image in Figure 3. Each doodle possesses the same weight when added to the training grid and no point on the grid can be greater than 1.

The system then takes the combined training doodles and performs a Gaussian convolution on the image. This convolution creates a blurring effect with a controllable variance that is used to distribute grid values around the training doodles. [3]

A doodle to be authenticated is then processed with the distribution map. Every point

[3] the Guassian formula used is $\sigma\sqrt{2\pi}e^{(x^2+y^2)/2\sigma}$ where σ is the variance of the normal. The variance used is 1.6.

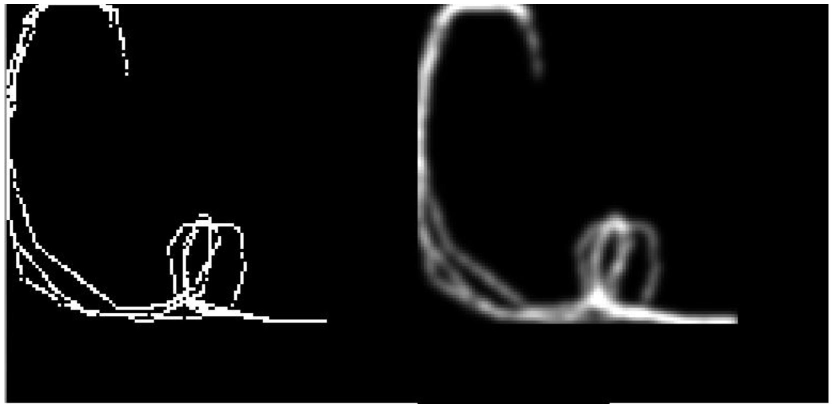

Figure 3: Example of a merged and Gaussian blurred map.

on the doodle is used to find the corresponding point on the distribution grid. The negative log of the value of this grid at each point on the doodle is then summed, and taken over the total number of points on the doodle. Because the range of the distribution grid is 0 to 1, the negative log is used to invert the data, so that the values of each test point increase with the distance from the peak of the distribution. This is then done with every stored training sample and if the sum in one case creates a low enough value, the identity of the user is confirmed.

2.3 Speed

The instantaneous speed of a doodle is also useful for recognition. The speed with which one traces a doodle can be as unique as the doodle itself. One person may consistently speed up when coming to a high point in a loop where another may slow down. (Figure 4) Recognition research has not extensively examined the order and speed of doodles. However, if the speed of a user's doodle is found to be consistent using it may help determine the identify of a user.

Speed comparison operates as follows. The points of a stroke are examined two at a time sequentially. The distance between the two strokes is found and taken over the difference of

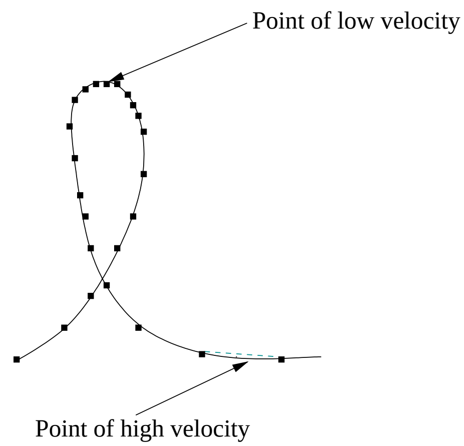

Figure 4: Example of speed change throughout the tracing of a doodle

the timestamps between the points. This number is then stored in a vector whose index is the scaled time from the initial point. During the training process a vector that contains the average speed at each index is created for each user. To compare, at each index the absolute value of the differnce between this vector and vector of the doodle being tested is summed. This will return a number indicating the relative similarity of the stroke to that user. An exact copy would return 0.

2.4 Doodle Variance

Another aspect used in doodle recognition is the variance between the points of a specific doodle over its values on the blurred distribution map. This feature is virtually independent of the value returned from the blurred distribution map comparison. To help visualize this, if we consider the blurred distribution map to be a mountain range with height corresponding to values, a doodle that followed this mountain range at the same height continuously would have a low variance. A doodle that criss-crosses this range would have a high variance. Ideally we can distinguish between two different doodles that appear similar in the blurred distribution grid but possess very different contours.

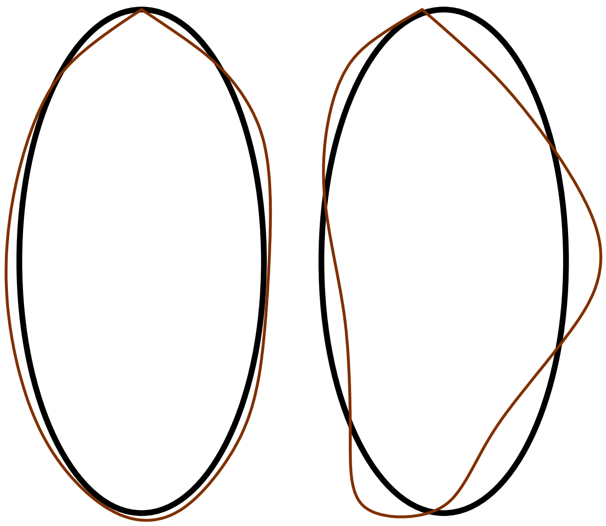

Figure 5: Illustration of variance of points across distribution grid

3 User Study

After the initial design, we conducted an informal user study of 10 people to examine the doodles people create, and to gather data to test the performance of the system. These ten users proved sufficient to test the feasibility of the system. The size of the grid used to store the doodles was 100 by 100.

Users were asked to formulate and then replicate a unique finger trace on a touch screen device. They could see the trace as it was made and look at the it once it was complete. The screen was cleared once another sample began. No specific directions were given other than to repeat as nearly as possible the same doodle.

The system was trained on all but one of a user's doodles (sample numbers range from 7-28), the untested doodle is then tested against the trained system. A random incorrect doodle from each other user is also selected and tested against the trained system. This is then repeated on 7 doodles from every user with a different doodle excluded and then compared every time. This method is used due to the relatively limited amount of data.

4 Results and Analysis

Method	# Incorrect	Percent Correct
Distribution grid	2	97.1
Speed comparison	30	57.1
Variance in grid	3	95.7
All methods used in tandem	1	98.5

The analysis shows that the combined use of all three features of the system yields extremely accurate results. As seen above, among the 70 comparisons only 1 sufficiently lacked the values to confirm authentication. Individually the distribution map comparison was incorrect only twice and the distribution map comparison variance three times.

The high failure rate of the speed comparision can be partly attributed to canonicalization. Specifically there are the speed changes involved in drawing a large doodle versus the same doodle scaled down.

We analyzed the time it took different users to draw their doodles and found that, while some users had a very low variance in the time it took to trace doodles, others did not. Users whose how had a low variance were more likely to receive a match on the speed comparision. If users had been instructed to replicate their speed during the training, the system may have been more accurate. (See appendix for complete results)

The other two features of the system demonstrated more consistency. However, some concern arises as to whether the distribution grid comparison, and the variance between point values across the distribution map are completely independent. If they are not the use of both is pointless. In the data collected only twice did one find a match while the other did not. This cannot be easily explained, other than by the nature of the doodle, however mathematically the two are independent.

5 Conclusion and areas of future work

This work has shown the feasibility of a lightweight doodle based authentication system. The recognition technology outlined here could possibly be applied to new fields such as hand writing and drawing recognition. If further study continues, one of the first things that should be seen is the effect on the system with a much greater number of users. Also, investigation into a better speed recognition system, along with other methods, could extend its accuracy even more.

6 Acknowledgments

I would like to thank my mentor Larry Rudolph and Max van Kleek for giving me terrific support and guidance throughout my stay here at MIT. I would like to thank Dawn Petersen, Jenny Sendova, James Skelly, Dan Haspel, and Kartik for being wonderful aids throughout the writing process. I would like to thank Anatoly Preygel, and all the other RSI TAs, and of course the nobodies. Finally I wish to thank CEE and RSI for granting me this wonderful opportunity to expand myself in new ways both intellectually, and socially.

References

[1] Joseph Goldberg, Jennifer Hagman, Vibha Sazawal.: Doodling Our Way to Better Authentication. *Computer Human Interaction Conference*. April 2002.

[2] Rubine, Dean.: Specifying Gestures by Example. *Computer Graphics Volume 25*. (July 1991).

[3] Van Kleek, Max, Christopher Varenhorst, and Larry Rudolph. *Lightweight authentication for enabling personalization on public displays*. Submission pending, MIT Student Oxygen Workshop, Cambridge, MA, 2004.

A Analysis of Samples Doodles

User	Mean time	Variance
User 1	1432	201.41
User 2	1928	1046.57
User 3	1567	144.54
User 4	573	462.34
User 5	1335	240.41
User 6	2473	192.98
User 7	528	100.29
User 8	1209	470.47
User 9	522	487.27
User 10	1191	95.56

B Touch Screen Input Difficulties

Lack of precision when doodling on the touch screen during the user study distorted much of the input. The movement of a finger across the screen results in a very narrowly and sharply oscillating line. This seems to be happening at the hardware level, a possible correction for this would be to run the doodle through an algorithm that can smooth out and remove this noise. However the oscillation's effect on the overall performance seems quite minimal, scaling down to a grid of 100 by 100 removes most of the noise.