Universität der Bundeswehr München
Institut für
Softwaretechnologie

der Bundeswehr
Universität München

Using hash visualization for real-time user-governed password validation

Julian Fietkau, Mandy Balthasar

Workshop Usable Security and Privacy
Mensch und Computer 2019
September 8, 2019

Agenda

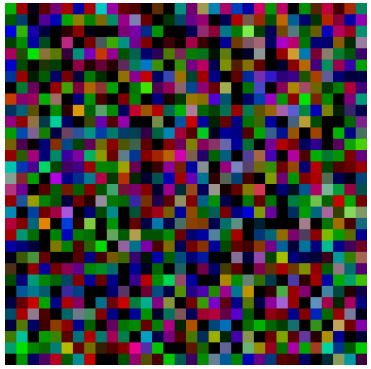
1. **Introduction**
2. Related work
3. MosaicVisualHash
4. Design recommendations

Core concept

- What is hash visualization?

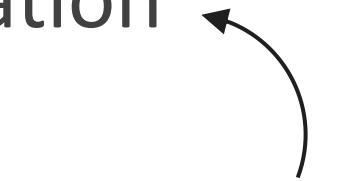
„My data of arbitrary length…“

1c8bfe8f801d79745c4631d09fff36c8



Usage scenarios

- Automatic online pseudonymization
- Human-appropriate checksum validation
- User-governed password validation



Goals for this presentation

- Quality criteria
- Presenting our algorithm
- Design recommendations

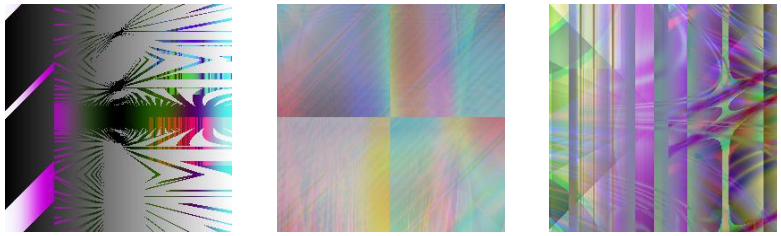
Agenda

1. Introduction
2. **Related work**
3. MosaicVisualHash
4. Design recommendations

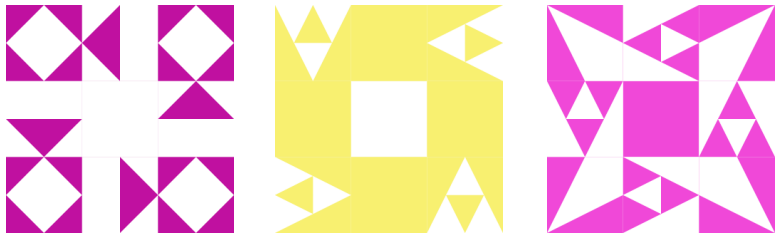
Covering the basics

- Perrig & Song (1999)
  - Concept and definition for “hash visualization”
  - Usage scenarios
    - PKI signature validation
    - User authentication
  - Quality criteria
    - Perceptive collision resistance
    - Regularity
    - Minimum complexity

Examples for visualizations



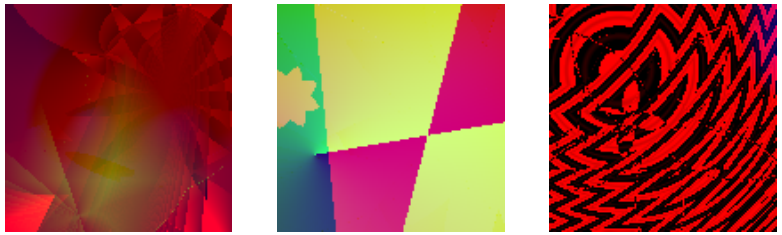
Random Art (Bauer, 1998)



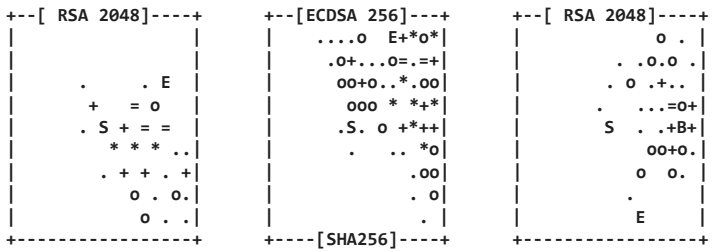
Identicon (Park, 2007)

vizHash (Sauvage, 2011)

RoboHash (Davis, 2011)

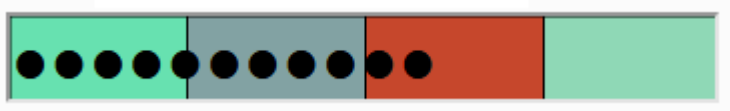


Vash (Cole, 2011)



OpenSSH Drunken Bishop
(Loss, Limmer & von Gernler, 2009)

Field-bound visualizations



Sawaya visualization (Sawaya, 2011)

HashMask (Dary, 2009)

Chroma-Hash (Thompson, 2011)

Non-hash-based approaches

HalfMask (Dary, 2009)

Passquerade (Khamis et al., 2019)

TransparentMask (Gruschka & Lo Iacono, 2010)

Agenda

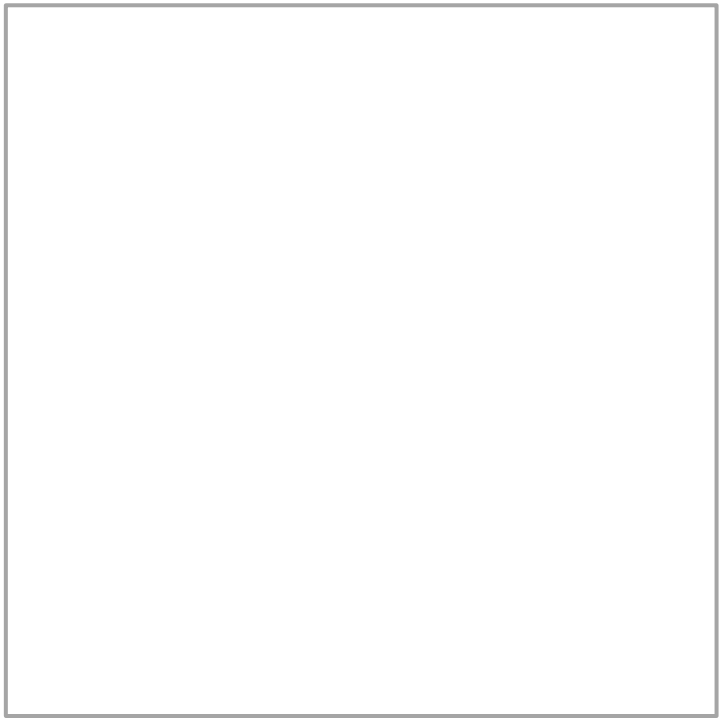
1. Introduction
2. Related work
3. **MosaicVisualHash**
4. Design recommendations

Quality criteria

- Perceptive collision resistance
- Regularity & minimum complexity
- Additionally: aesthetic impression

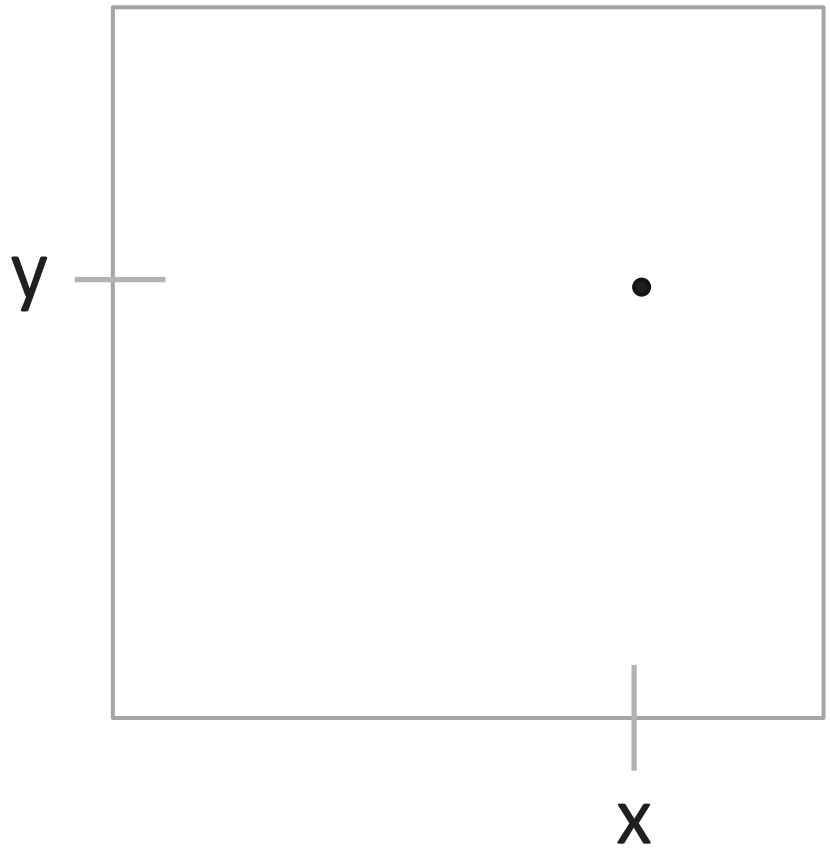
Algorithm (0/10)

Start with a square canvas



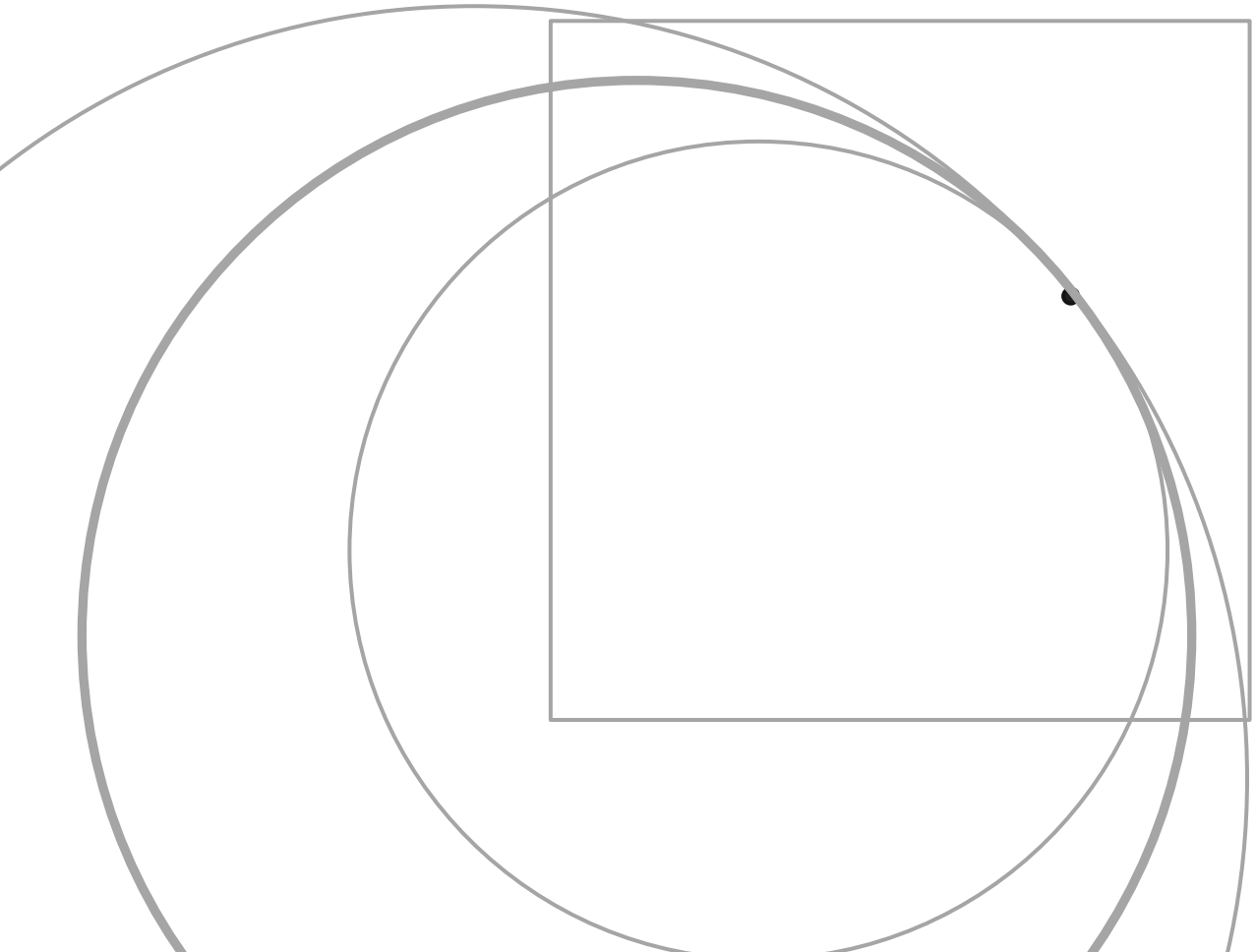
Algorithm (1/10)

Pick a random point



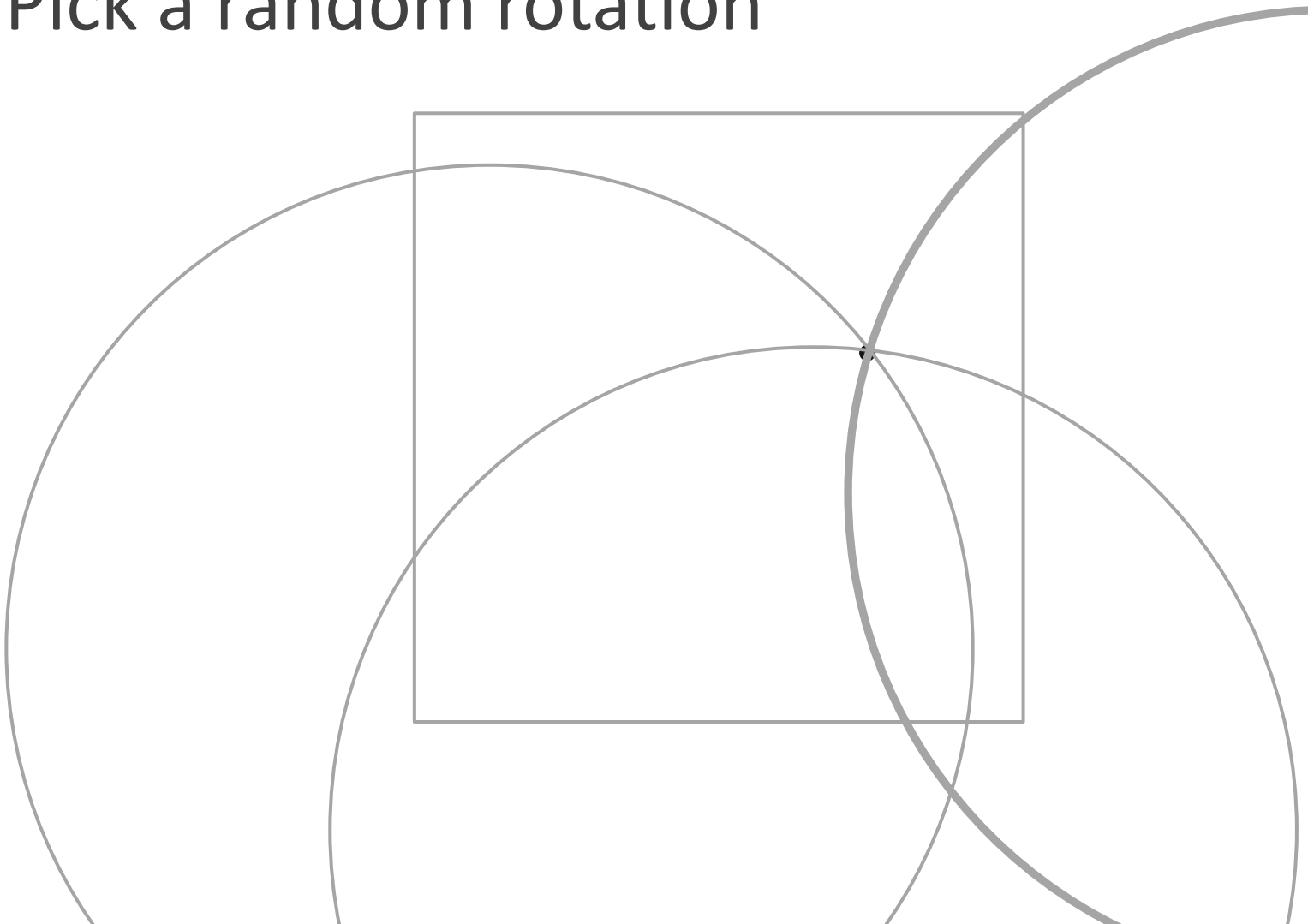
Algorithm (2/10)

Pick a random circle radius



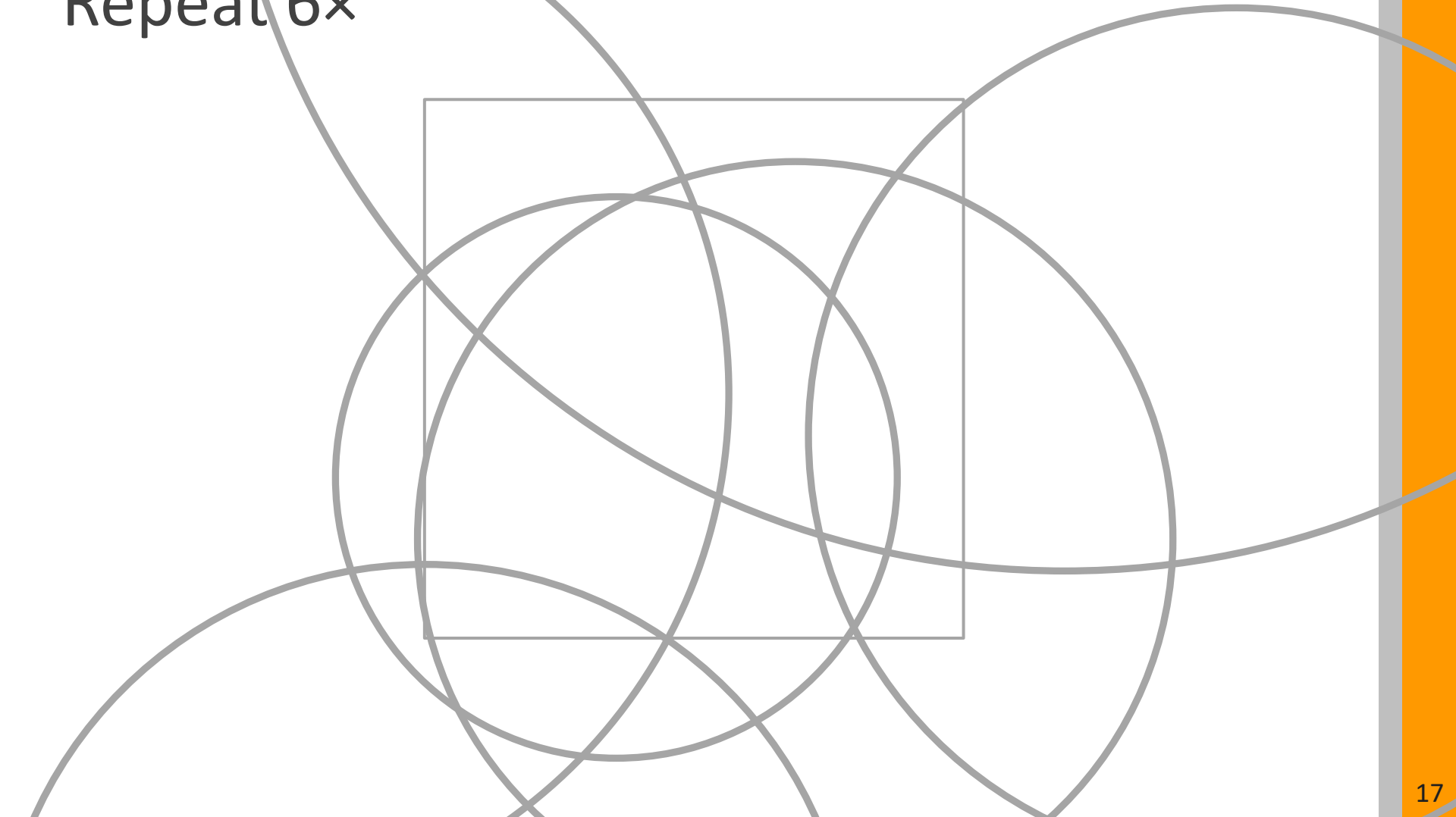
Algorithm (3/10)

Pick a random rotation



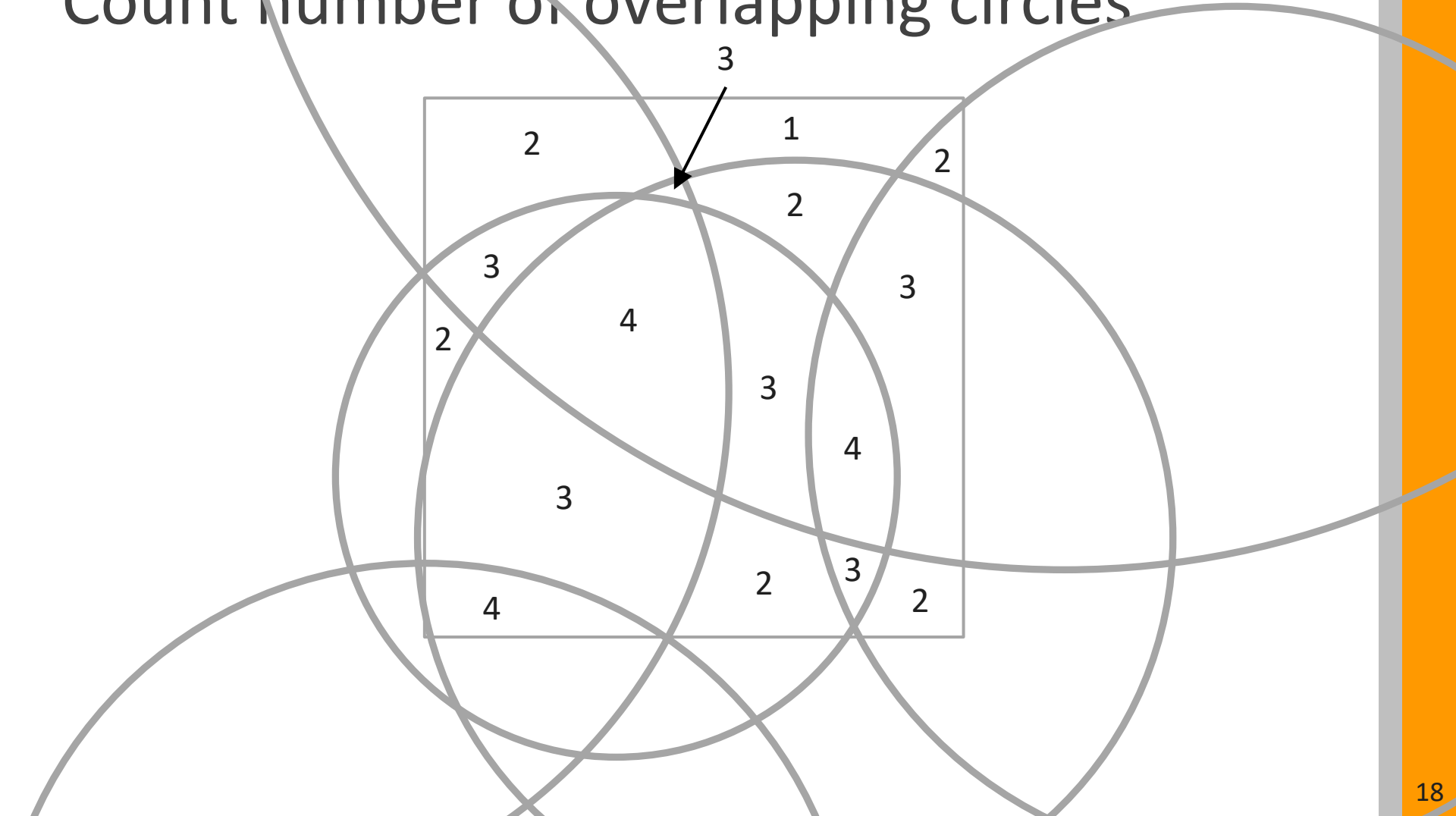
Algorithm (4/10)

Repeat 6×



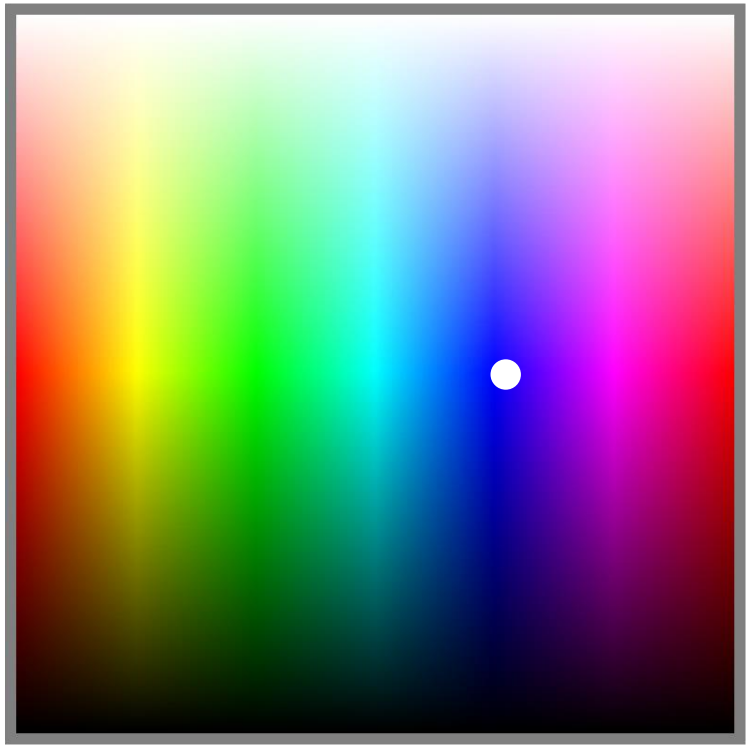
Algorithm (5/10)

Count number of overlapping circles



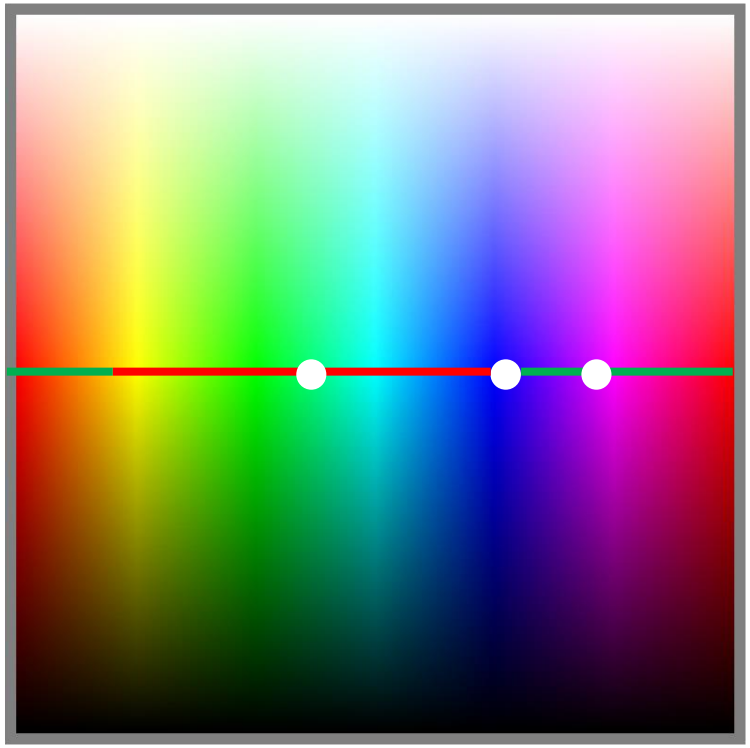
Algorithm (6/10)

Pick first hue at random



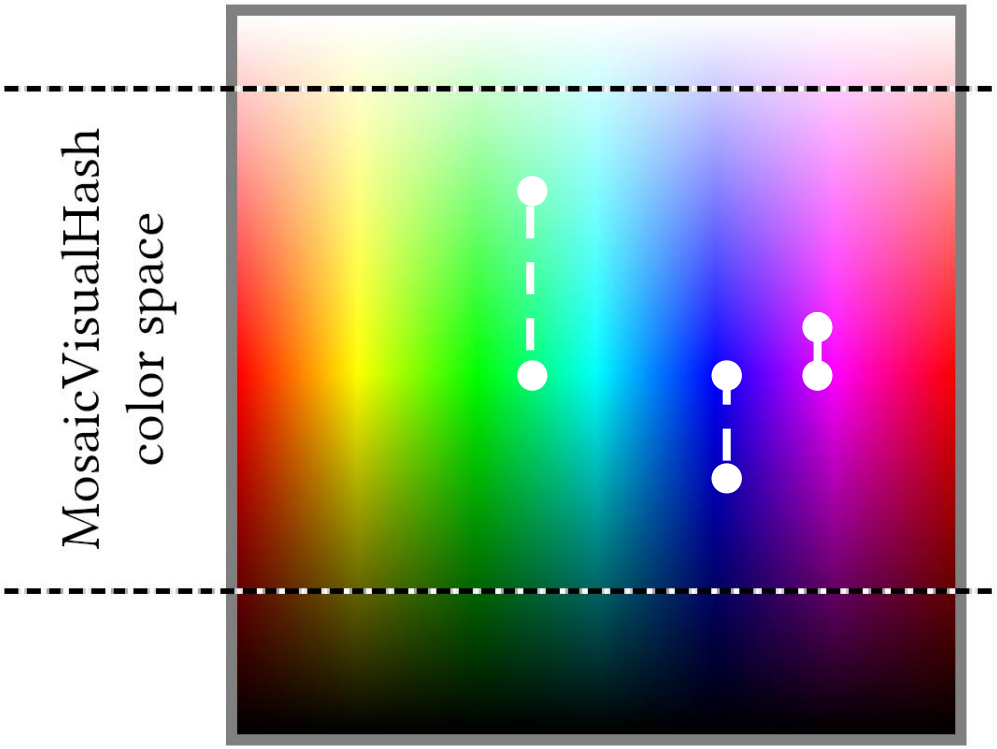
Algorithm (7/10)

Pick 2nd and 3rd hue at random distances



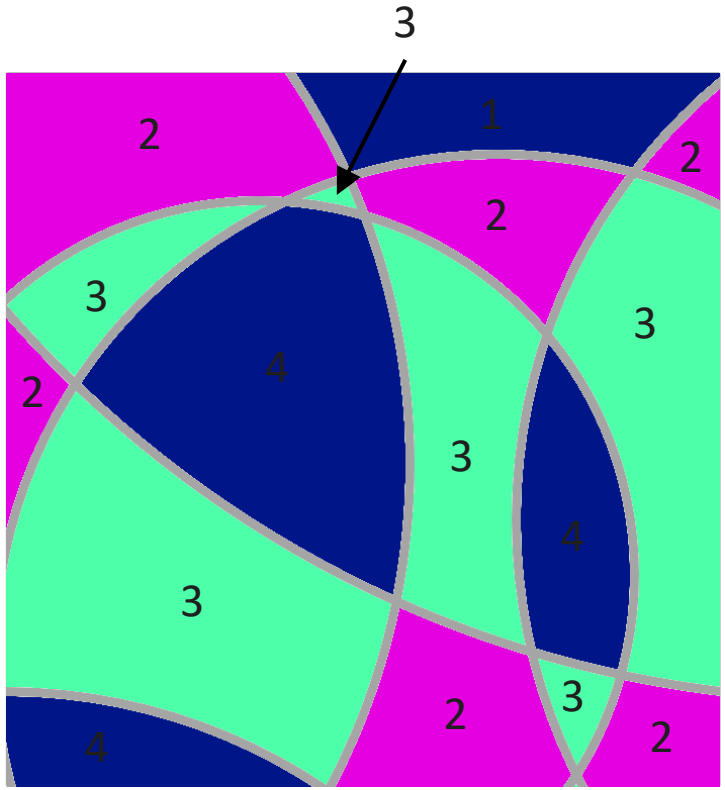
Algorithm (8/10)

Pick 3 random lightnesses (within range)



Algorithm (9/10)

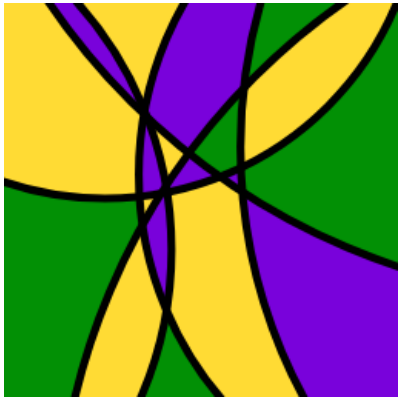
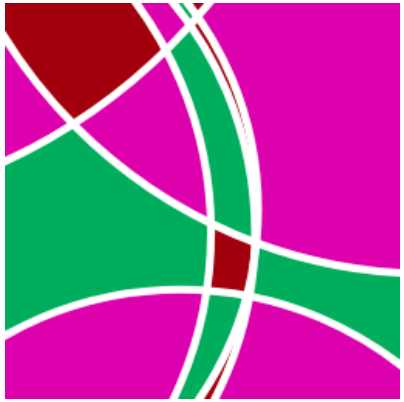
Color each segment according to palette

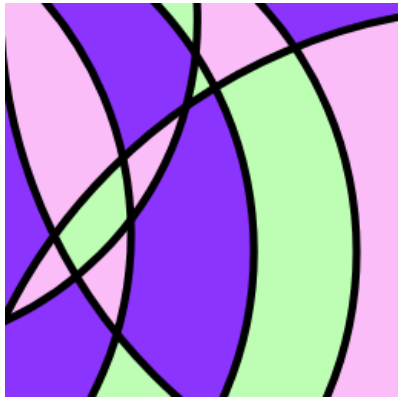


Algorithm (10/10)

Color the contours black or white

More examples

https://fietkau.software/mosaic_visual_hash

Evaluation

- Perceptive collision resistance
  - Difficult to judge without empirical testing
- Regularity & minimum complexity
  - Clearly recognizable structure, visually memorable
- Additionally: aesthetic impression
  - Subjective judgment: attempt succeeded

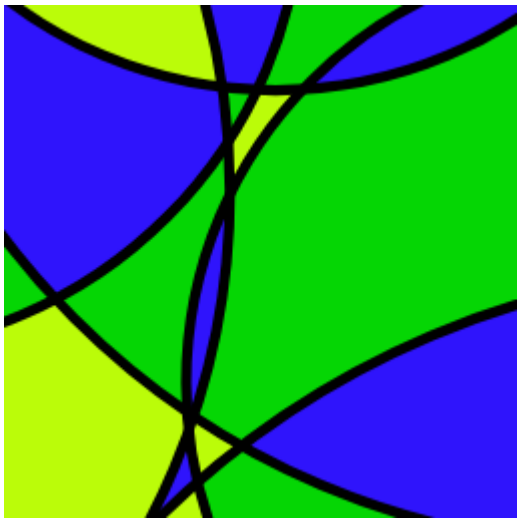
Agenda

1. Introduction
2. Related work
3. MosaicVisualHash
4. **Design recommendations**

Design recommendations

Using hash visualization for user-governed password validation:

- Live visualization as you type
- Visualization delay
- Minimum password length
- Jitter



Thank you for your attention!

Questions

Julian Fietkau, Mandy Balthasar
Professur Mensch-Computer-Interaktion
Institut für Softwaretechnologie
Universität der Bundeswehr München
Werner-Heisenberg-Weg 39

Tel.: +49 (0)89 6004-2613
Fax: +49 (0)89 6004-4447
julian.fietkau@unibw.de
mandy.balthasar@unibw.de
https://www.unibw.de/inf2/mci