Symbol-Based Visual Cryptographic Authentication Mechanisms: Attacks and New Constructions
Huangyi Ge, Tianhao Wang, Omar Chowdhury, Hemanta Maji, Ninghui Li

I. Visual Cryptography

- Divide each pixel into 4 sub-pixels, overlap two shares, distinguish by gray level:
  - □ + □ = □ 0
  - □ + □ = □ 1

II. PassWindow: Symbol-Based Authentication

- Use Digits as symbols to authenticate
  - customer holds the secret i.e., transparent credit card challenge sent by server
  - server knows the secret user authenticate with response 7

III. Attacks

- Take a whole column (7 edges) into consideration. Model the problem theoretically.
  - $X_{p,k}$, where $p$ ranges over all positions on a frame, and $k$ ranges over $P_K$, the set of all patterns that can be used on the key. $X_{p,k} = 1$ if and only if the key has pattern $k$ at position $p$.
- Then use general SMT solvers to get result, but it is slow.
- Use optimizer or multiplicative update to accelerate, but it is only an approximate.
- Extendable to other designs.

IV. New Constructions

- SCol: split columns.
- NoNF: remove noisy frames.
- OSD: be careful when picking challenges.
- RDD: show two digits, and let user input either digits.
- HDD: show two digits, and let user compute a simple hash (addition modulo 10).
- TDD: show even three digits.
- User study\(^2\) indicates they are user friendly.

V. Evaluation & Future Direction

- Results show the effectiveness of our improvements
- Effectiveness of our new schemes
- Security of varying length

Future Direction:

- Find efficient and accurate guessing algorithms.
- Come up with new schemes that withstand attacks.
- Take advantage of other human solvable problems (Captcha).
- Use it to build primitives for Physical Cryptography.

\(^1\) passwindow.com
\(^2\) dunes.cs.purdue.edu/wang2842/pass_window_survey/index.php