

## ハイブリッド画像を用いた PIN 認証の視認性とユーザビリティに関する研究

田中 雄也<sup>†</sup> 菊池彩子<sup>‡</sup> 長谷川まどか<sup>‡</sup>宇都宮大学大学院 地域創生科学研究科<sup>†</sup> 宇都宮大学大学院工学研究科<sup>‡</sup>

## 1. はじめに

ハイブリッド画像とは、2枚の異なる画像の一方をハイパスフィルタ、もう一方をローパスフィルタで処理し、両出力を合成することで得られる画像である[1]。ハイブリッド画像は、視認できる画像が視距離によって異なり、近距離では高周波画像、遠距離では低周波画像を視認しやすい。

Papadopoulos らは、このハイブリッド画像をスマートフォン端末の PIN 認証に応用し、覗き見攻撃に耐性のある「ハイブリッドキーパッド」を使用した“IllusionPIN (IPIN)”を提案している[2]。IPIN では、数字の配置が異なる 2枚のキーパッド画像から成るハイブリッドキーパッドを PIN 入力に用いる。

Papadopoulos らは、アタッカー視点での視認性の数学的モデルの構築と、評価実験を行い、所定の視距離以上であれば、アタッカーがユーザの PIN を認識できないと結論づけている。しかし、ユーザの立場におけるハイブリッドキーパッドの使いやすさについては十分な検討が行われていない。

そこで本研究では、ユーザの立場におけるハイブリッドキーパッドの視認性とユーザビリティに関する評価実験を進めている。また、ハイブリッドキーパッドの視認性の改善の検討も行っている。本稿では、まず、ハイブリッドキーパッドの生成法と視認性評価実験について述べる。次に、PIN 認証アプリケーションを実装し、各キーパッドのユーザビリティ評価を行い、その有効性と問題点について考察する。

## 2. ハイブリッドキーパッド

ハイブリッドキーパッドは、2枚のキーパッド画像から作成される。アタッカー用キーパッド $I_s$ は通常の PIN 認証で用いられるものと同一の数字配置であり、これにローパスフィルタ $G_l$ (Gaussian フィルタ、標準偏差 $\sigma_l=35$ (cycle/image))を施し、低周波画像 $I_s^l$ を得る。一方、ユーザ用キーパッド $I_u$ は、数字の配置が通常と異なり、これにフィルタ $G_h^l$ (Gaussian フィルタ、標準偏差 $\sigma_h^l=440$ (cycle/image))を反転したハイパスフィルタをかけ、高周波画像 $I_u^h$ を得る。ハイパスフィルタ $G_h$ は式(1)で与えられる。ハイブリッドキーパッド $I$ は式(2)により作成される。

$$G_h = 1 - G_h^l \quad (1)$$

$$I = I_s^l + I_u^h \quad (2)$$

文献[2]では、同じ位置で数字を重ねているが、視認性に難がある。そこで、新たに、高周波画像(ユーザ用数字)を低周波画像(アタッカー用数字)の中心位置から左へ 0.5 文字(30pixel)ずらした場合についても検討を行う。前者を Hybrid1、後者を Hybrid2 と呼ぶ。図 1 に各ハイブリッドキーパッド上の数字の一例を示す。

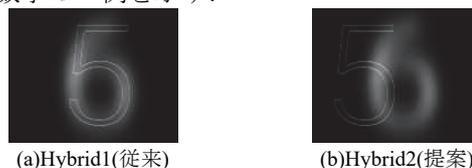


図 1 各ハイブリッドキーパッドの一例

## 3. 視認性の評価実験

## 3.1. 実験概要

上述のハイブリッドキーパッドについて、ユーザ用数字の視認性の比較実験を行った。実験では、ユーザ用数字の配置が異なるキーパッド画像を複数用意し、端末上に順次提示して、実験参加者に読み取った数字を回答させた。参加者が端末を見る位置は、アタッカー視点(視距離 63.5cm, 角度 30 度)とユーザ視点(視距離 25cm, 35cm, 角度 0 度)を用意した。

使用端末は Nexus6(5.96inch, 2,560×1,440 画素)であり、スクリーンの輝度は最大に設定した。実験参加者は、事前に同意を得た、視力が正常な 20~25 歳の学生 27 名である(矯正視力を含む)。

## 3.2. 実験手順

各参加者は、まず、アタッカー視点での読み取り実験を行った。Hybrid1 を 9 種、Hybrid2 を 9 種の計 18 種について、キーパッド上の 10 個のユーザ用数字を回答させた。

続いて、ユーザ視点で実験を行った。まず視距離 25cm で上述の 18 種についてユーザ用数字を読み取り、10 分間の休憩後、視距離 35cm でも同様の実験を行った。実験参加者 1 人あたり全試行の終了まで 1 時間程度を要した。なお、各参加者を 3 人 1 組の 9 グループに分け、18 種のキーパッドの提示順序をグループごとに変化させることで順序効果の除去を行った。

## 3.3. 実験結果

数字の正答率の平均値、最高値、最低値について、ユーザ視点での結果を表 1、アタッカー視点での結果を表 2 に示す。表 1 より、ユーザ視点では、従来の Hybrid1 に比べ、Hybrid2 の平均正答率が視距離 25cm では 1.5%、35 cm では 3.4%、高いことが分かる。最高値は、いずれのキーパッドでも 100%であ

り、すべての数字を読み取れた参加者がいたことを意味する。最低値は Hybrid2 の方が上昇している。

一方、表 2 より、アタッカー視点でも Hybrid2 の平均正答率が上昇したことが分かる。最低値は 0% であり、全く読み取れない参加者がいたことを意味するが、最高値はいずれのキーパッドでも 50% 程度あり、半分程度の数字を読み取れた参加者も存在したことになる。文献[2]では、アタッカー視点では PIN を全く読み取れないとしているが、今回の結果は視認性の個人差が大きいことを示唆している。

各キーパッドにおける平均正答率を、ウィルコクソン符号付順位検定を用いて有意水準 5% で検定した。その結果、すべての視点において、Hybrid2 は、Hybrid1 と有意差があることが分かった。よって、数字をずらして重ねることで視認性が向上すると考えられる。ただし、アタッカー視点でも向上しており、注意が必要であることが分かった。

表 1 ユーザ視点の正答率[%] (n=27)

	25cm		35cm	
	Hybrid1	Hybrid2	Hybrid1	Hybrid2
平均	98.1	99.6	95.1	98.5
最高	100.0	100.0	100.0	100.0
最低	84.4	96.7	71.1	87.8

表 2 アタッカー視点の正答率[%] (63.5cm)(n=27)

	Hybrid1	Hybrid2
平均	15.6	27.1
最高	50.0	57.8
最低	0.0	0.0

## 4. ユーザビリティ評価実験

### 4.1. 実験概要

次に、ユーザビリティを比較するため、認証時間と認証成功率の評価を行った。これらの項目は、実験用に構築した PIN 認証アプリケーションを使用して計測した。使用端末と輝度の設定は、3 節の実験と同一である。各参加者は端末を任意の位置で手に持ち、表示される PIN 入力画面に、指定された PIN を入力する。実験参加者は、視力が正常な 20~25 歳の学生 24 人である(矯正視力を含む)。実験には、通常の数字配置のキーパッド(正順)、数字の配置をランダムにしたキーパッド(ランダム)、Hybrid 1、Hybrid 2 の 4 種を使用した。入力用の PIN は、“1234”、“567890”、“2965”、“418073”の 4 種とした。

### 4.2. 実験手順

最初に、実験参加者にアプリケーションの操作方法を説明し、数回の入力練習を行った後に、実験を行った。各参加者は、正順を 1 種、ランダムを 3 種、Hybrid 1 を 3 種、Hybrid 2 を 3 種の順に計 10 種のキーパッドを用いて PIN を入力する。したがって、実験参加者 1 人あたりの総試行回数は(4 種の PIN)×(キーパッド 10 種)=計 40 回となる。また、提示順序に

よる順序効果を取り除くため、参加者を Hybrid 1、2 の順に認証を行うグループ A と、Hybrid2、1 の順に認証を行うグループ B の 2 つに分けた。

### 4.3. 実験結果

表 3 に認証時間、表 4 に認証成功率を示す。

表 3 より、平均認証時間は、Hybrid 2 が Hybrid 1 に比べて 2 秒ほど短いことが分かる。Hybrid 1 と Hybrid 2 の平均認証時間を、ウィルコクソン符号付順位検定を用いて有意水準 5% で検定した結果、有意差があった。よって、Hybrid2 の方が有効であると考えられる。ただし、正順やランダムと比べて 3 倍近い時間を要しており、使いやすさの面で、さらなる改良の余地がある。

一方、表 4 より、認証成功率は、どのキーパッドでもほぼ同じであるが、Hybrid 1、Hybrid 2 ともに、正順やランダムに比べて若干高い傾向にあることが分かる。これは、ハイブリッドキーパッドが覗き見を防ぐために難読化されていることから、実験参加者が慎重に数字を入力したためと考えられる。

表 3 認証時間 [秒](n=24)

	4 桁		6 桁		平均
	1234	2965	567890	418073	
正順	2.69	2.86	3.44	3.46	3.11
ランダム	2.96	3.67	4.33	4.38	3.84
Hybrid 1	8.58	9.38	14.01	13.81	11.45
Hybrid 2	7.43	8.19	10.58	11.57	9.44

表 4 認証成功率[%](n=24)

	4 桁		6 桁		平均
	1234	2965	567890	418073	
正順	95.8	100.0	100.0	95.8	97.9
ランダム	95.8	94.4	100.0	98.6	97.2
Hybrid 1	100.0	100.0	100.0	100.0	100.0
Hybrid 2	100.0	100.0	98.6	100.0	99.7

## 5. おわりに

本研究では、ハイブリッドキーパッドの視認性とユーザビリティに関する評価を行った。視認性、ユーザビリティともに、数字をずらした Hybrid2 が、ずらさない Hybrid1 よりも若干優れることが分かった。しかし、アタッカー視点でも視認性が上がることから、全数字をずらすのではなく、対象を 3 と 8 のような特に視認性の低い組み合わせに限定するなどの検討が必要である。

今後は、今回実装したアプリケーションを使用し、覗き見耐性の評価実験を行う予定である。

### 参考文献

- [1] A. Oliva, A. Torralba, P.G. Schyns, “Hybrid Images,” ACM Trans. on Graphics, Vol.25, No.3, pp.527-532, 2006.
- [2] A. Papadopoulos, T. Nguyen, E. Durmus, N. Memom, “IllusionPIN: Shoulder-Surfing Resistant Authentication Using Hybrid Images,” IEEE Trans. on Information Forensics and Security, Vol.12, No.12, pp.2875-2889, 2017.