ISS-P-99

Android端末に向けた新たな認証システム

酒井　芳章†　　崎山　一男††
† 電気通信大学 情報理工学部　　†† 電気通信大学 大学院情報理工学研究科

1.　はじめに

カメラ付き携帯電話の普及に伴い，QRコードを利用する機会が増えている．QRコードは，表示媒体上のコードをリーダーで読むことにより，情報の取得ができ，物の識別だけでなく入場チケットとしても使われている．しかしQRコードはコピーが容易なため，不正利用が懸念される．本稿では，Android端末間において，AESを用いたチャレンジ・レスポンス認証を基盤とし，カメラと時間変化する画像を用いることで，リアルタイムでの画像コピーが困難となる認証を提案する．

2.　提案する認証システム

2.1.　概要

Android端末2台を用い，それぞれをVerifier，Proverとする．128bitの共通鍵をVerifier，Proverのアプリに内蔵する．Verifier，Prover共にインカメラで互いの画面を撮れるように向い合せで設置する．

チャレンジの送信は，QR コードにて行う．また，レスポンスは，AES暗号化の平文と暗号文の中間に位置する5ラウンド目の値を用い，値をRGB値の輝度値に読み替えた画像の表示にて送信を行う．

RGBの3色の画像を比較したところ，G値が認証に適していたため，画像の輝度値にはG値を用いる．

2.2.　認証処理手順

認証の流れを図1と以下に示す．

① VerifierがQRコードをチャレンジとして表示し，Proverがカメラを用いて受信
② Proverは共通鍵を使ってチャレンジをAESで暗号化
③ Proverは5ラウンド目をG値として1byteずつレスポンスとして表示し，Verifierがカメラを用いて受信
④ Verifierはレスポンスと5ラウンド目の相関値を計算
⑤ Verifierが閾値と相関値を比較し，認証の可否を表示

3.　認証実験結果

本人認証を100回，他人認証を200回行い相関値を取得し，閾値の設定を行った．

結果を図2に示す．本人拒否率と他人受入率が同じとなる等誤り率は，1%であり，そのときの閾値は0.56となった．また他人受入率が0%のとき，閾値は0.75となった．

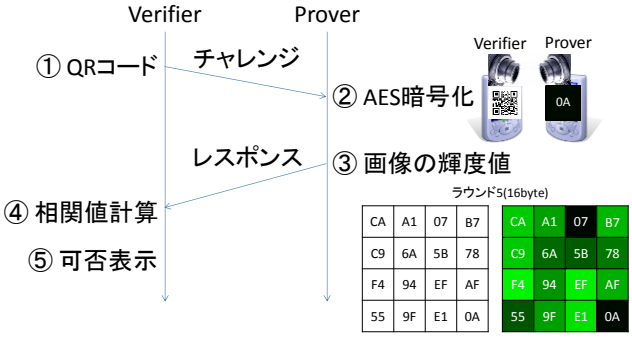

図１．認証システムの流れ

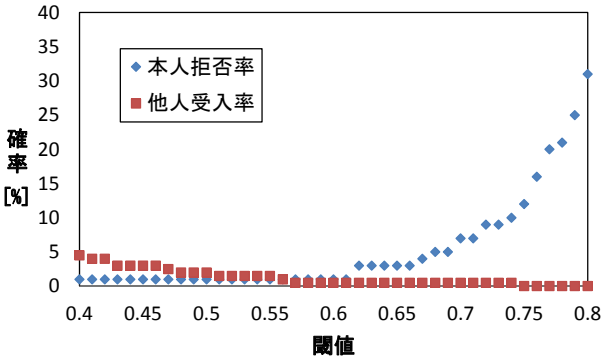

図2．閾値における本人拒否率・他人受入率

以上より，閾値を0.56～0.75に設定することにより，他人受入率が1%以下の認証を行うことができると考えられる．

4.　まとめ

適切な閾値を設定することにより，Android端末間での画像の輝度値を用いた認証を行えることが確認できた．

5.　今後の課題

使用デバイスによる違いやProverの数に応じた適切な閾値の調査，画像のコピー攻撃への耐性の評価が必要になると考えられる．

参考文献

[1]　National Institute of Standards and Technology, “Advanced Encryption Standard (AES),” NIST FIPS PUB 197, (2001)
[2]　瀬戸 洋一 著, “サイバーセキュリティにおける生体認証,” 共立出版株式会社, (2002)
[3]　社団法人日本自動認識システム協会 編, “よくわかるバイオメトリクスの基礎,” オーム社, (2005)