

携帯電話によるユーザ認証のための二次元コード解析について

石田 雄一[†] 山元 規靖[‡]
福岡工業大学 情報工学部情報通信工学科

1. まえがき

現在、ユーザ認証はパスワードによるものが主流であるが、パスワードの盗難や、ユーザによる管理の煩雑さに問題がある。バイオメトリクス等の認証方法では、ハードウェアの増設や手続きの煩雑化、利用者の心理的抵抗などの問題⁽¹⁾があり、ユビキタスなネットワーク利用には向かない。そこで我々は、急速に普及している携帯電話を用いたユーザ認証を提案している。この手法では、携帯電話で二次元コードを撮影することにより認証を行うが、携帯電話ではメモリや処理能力に大きな制限がある。本稿では、この制限下でも十分なセキュリティと速度を有するソフトウェアによる手法を提案する。また、提案した手法の検証を行い、実用的な手法であることを示す。

2. 提案するユーザ認証システム

現在の携帯電話は、標準で http/https アクセスがサポートされ、携帯電話上で動作するアプリケーションからも利用が可能⁽²⁾である。そこで、以下のような流れで個人の認証を行う。

- ① ユーザは、クライアント PC から https で Web サーバにアクセスをする。
- ② Web サーバ側で生成したワンタイムパスワードとアクセスしてきたクライアント PC の識別コードをデータベースへ登録をする。
- ③ 生成されたワンタイムパスワードを二次元コードに変換し、ログイン画面に表示する。
- ④ 表示された二次元コードを、あらかじめ携帯電話にダウンロードしておいたアプリケーションを用いて撮影を行う。
- ⑤ 撮影した二次元コードを解析し、ワンタイムパスワードを取り出す。
- ⑥ アプリケーションから https を使って Web サーバに二次元コードから解析したワンタイムパスワードと携帯電話固有 ID を通知。
- ⑦ Web サーバは、ワンタイムパスワードからアクセスしているクライアント PC、携帯電話

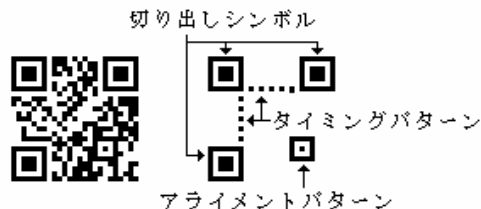


図1 QRコード例

固有 ID からユーザを特定する（携帯電話固有 ID とは携帯電話に一意に決まっているハードウェアアドレスの事であり携帯電話を識別するのに利用する）。

- ⑧ 認証の結果を携帯電話に通知し、ログイン可能状態になった事をユーザに知らせる。
- ⑨ クライアント PC からログインボタンを押し、Web サーバが認証済みであるかをデータベースに問い合わせ、認証済みであれば認証制限のかかったサイトへアクセスできる。

3. 二次元コード認識アルゴリズム

提案した認証システムでは、携帯電話で二次元コードを認識する必要がある。今回用いる二次元コードは、現在携帯電話でも普及しつつある QR コードを改良したコード用いる。QR コードとは、1994 年株式会社デンソーによって開発され、高速読取を重視したマトリクス型二次元コード⁽³⁾である（図1）。

一部の携帯電話では読み込んだ QR コードをアプリケーションに渡すことが可能であるが、大半の携帯電話ではまだ QR コードを読み込めない。従って、携帯電話上で QR コードを読み込むアプリケーションを作成する必要がある。しかしディスプレイに二次元コードを表示する本研究では、QR コードは汎用的過ぎて処理に時間がかかってしまう。そこで、QR コードの機能を縮小した二次元コードを用いる。QR コードから踏襲するのは、切り出しシンボルやタイミングパターンと言った、データ位置を取得するための情報である。

この二次元コードの切り出しシンボルをすばやく正確に見つける事により、データを高速かつ確実に読み込める。一般に画像処理で形の決まった図形を探すアルゴリズムにはパターンマッチングを用いる。しかし、処理能力の非力な携帯電話では、回転・伸縮する画像を探すのに

The Processing of Two Dimensional Symbol for User Verification by the Mobile Phones

[†] Yuichi Ishida

[‡] Noriyasu Yamamoto

Information and Communication Engineering, Fukuoka institute of technology

大変時間がかかる。そこで本研究では、特徴点から幾何学的に図形を特定するアルゴリズムを提案する。検出の具体的な流れは、以下のような手順である。

- ① 撮影データにエッジ検出⁽⁴⁾⁽⁵⁾を施し、検出されたエッジから連続する無駄な点を削除して特徴点を取り出す。
- ② 取り出した特徴点から考えられる2点の組み合わせの距離を調べ、一定の距離以下の組み合わせを削除する。
- ③ 残った組み合わせの2点間の直線上にどの程度の割合で黒色が出現するか調べ、一定の割合以下の組み合わせを削除する。
- ④ 残った座標から左上・右上・左下・右上の4座標を抽出し、「4辺の長さが等しい」「向かい合う辺は平行である」「交わる辺は直交である」の3条件に一致するかを計算により求め、4座標が正方形であるかを求める。

4. 実験結果

このアルゴリズムとパターンマッチングを用いた実機によるシンボルのみの読取速度を表1と表2に示す。テストに用いた切り出しシンボルはすべて同じ画像を用いた。サイズの違い回転は、カメラと画面の距離を調節・カメラ自体を回転させた。表の時間は5回撮影を行い、その平均時間を載せている。実験に使用した携帯電話はNTT docomoのP505iであり、505iシリーズの中で数値演算速度は6機種中3番目に速い⁽⁶⁾。従って他の機種を用いても、同程度の速度が期待できる。

さて実験結果からわかることは、パターンマッチングではサイズ・回転角度が変化しても比較的速度に違いがなく、提案方式では回転角度が大きくなればなるほど、速度が低下する点である。これは、考えうるパターンを全て調べて、その適合率から図形を判断するパターンマッチングではサイズ・回転角度にあまり依存しない。一方、提案方式は特徴点から切り出しシンボルを計算により求める。そのため回転角度が大きくなるほど特徴点の数が増え、その結果、計算量が増大し認識に時間がかかっていると考えられる。

今回の二次元コードはディスプレイに理想的な状態で表示されるため、ユーザが意図的にカメラを回転しない限りこのアルゴリズムは実用的である。

シンボルのサイズ	提案方式	パターンマッチング
50 x 50 (±3)	2031	20225
60 x 60 (±3)	2348	24523
70 x 70 (±3)	2693	28478

表1：シンボルのサイズによる違い（角度±2°）

シンボルの角度	提案方式	パターンマッチング
0° (±2°)	2038	20225
10° (±2°)	6573	25273
20° (±2°)	13937	27672

表2：角度による違い（サイズ50 x 50 (±2)）

時間単位：ミリ秒

5. むすび

ユビキタス時代に必要なユーザ認証課題を指摘すると同時に、一解決方法を提案した。他の解決方法⁽⁷⁾⁽⁸⁾もあるが、本研究では使い慣れた技術を用いる事により運用によるセキュリティ低下・新規システム開発によるセキュリティホール誘発を抑制することが出来る。本研究で示した簡潔な解決方法はセキュリティ上の観点からでも有用である。

また、本研究で提案した切り出しシンボルの認識では、従来の手法に比べ高速に認識できた。この手法を応用する事により、コード全体の読取速度向上につながると考えられる。

今後は、現試作プログラムの回転角度制限をなくし、データのデコード時間短縮のため独自のエンコードをQRコードと同形式のデコードを搭載して互換性を持たせると言ったことを検討していきたい。

参 考 文 献

- 1) 日経 NETWORK 2003年12月号、日経 BP 社
- 2) <http://www.nttdocomo.co.jp/>
- 3) <http://www.qrcode.com/>
- 4) 田村 秀行：コンピュータ画像処理、オーム社
- 5) 谷口 慶治：画像処理工学、共立出版
- 6) <http://www.itmedia.co.jp/>
- 7) 小越 康宏、日名田 明、広瀬 貞樹、木村 晴彦：打鍵間時間を基にした認証システムのリズム打鍵による改善、情報処理学会論文誌、Vol.44, No.2
- 8) 白井 治彦、西野 順二、小高 知宏、小倉 久和：対話的計算機環境におけるコマンド入力連鎖を用いた認証手法の提案、電子情報通信学会論文誌、Vol.J82-A, No10