

1 写真入りクレジットカードのセキュリティ向上方法

会津大学

コンピュータ理工学部 コンピュータ・サイエンス部門

教授 趙 強 福

■新技術の概要

本技術は、疑似写真生成方法、写真復元方法、復元鍵情報の分散管理方法などから構成される。クレジットカードの持ち主の写真を変形してからカードに記載することによって、第三者によるカードの不正使用を抑制することが本技術の狙いである。

■従来技術・競合技術との比較

写真入りカードは偽造、類似人物による不正使用は避けられない。写真を暗号化してカードに記載することもできるが、攻撃技術の進歩が懸念される。暗号化されていること自体が分からない本技術はより安全性の高いカードを提供できる。

■新技術の特徴

- ・写真ではなく、それが再生できる疑似写真をカードに記載する。
- ・写真を復元するための鍵を、サーバ、端末、カードに分散的に管理し、元の写真が固く守られる。
- ・写真を復元するための鍵は、端末依存であり、これは不正使用の特定と回避に有効である。

■想定される用途

- ・クレジットカードホルダの認証
- ・電子マネー、お財布ケータイなどのユーザ認証
- ・運転免許、住居カードなど各種身分証明カードのホルダ認証

写真入りクレジットカードのセキュリティ向上方法

会津大学
コンピュータ理工学部
コンピュータサイエンス部門
教授 趙 強福

問題: クレジットカードの偽造と不正使用



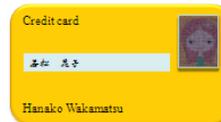
研究背景

- クレジットカードの偽造と不正使用は大きな社会問題となっている。
- ICカードの普及により被害は著しく減っているが、リスクは依然として存在する。
- 主なリスクは、偽造や改竄よりも、「ナリスマン」である。
 - カードとパスワードを同時に盗まれる場合 → 店での買い物
 - カード情報が盗まれた場合 → ネットショッピング

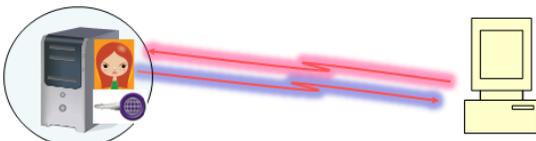


従来技術とその問題点

- 従来方法1:
 - 写真を印刷し、カードが使用されるときに確認する。
- 問題点:
 - 写真の張り替えは可能。
 - 写真が小さいので、ほとんどの場合に使用されてしまい。
 - ホログラムを使うことも可能だが、写真がより不鮮明になる。

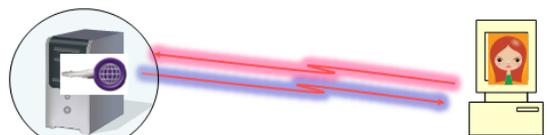


従来技術とその問題点



- 従来方法2:
- サーバから写真を送ってもらう。
- 問題点:
- 通信負担が重い。
 - 大量な個人情報流出しやすい。

従来技術とその問題点



- 従来方法3:
- 暗号化された写真をカードに入れ、サーバから鍵だけもらい、写真を復号化して表示する。
- 問題点:
- カードが攻撃され、情報が読み取られるリスクがある。
 - 攻撃技術の向上で、近い将来、安全でなくなる可能性がある。

新しい提案→データをより安全なものにする

- 写真を変形してからカードに記載する。
- カードを使用する際に、元の写真を復元する。
- 復元に使用される「復元鍵」は、サーバ、端末、カードに分散され、全部揃わないと復元不可能である。



提案システムの基本コンセプト



新技術の基となる技術その1: 画像変形と復元



- 原画像を目標画像へモーフィングしていく。
- 中間画像は擬似的画像である→変形画像。
- 「鍵」さえあれば、変形画像から原画像が復元できる。

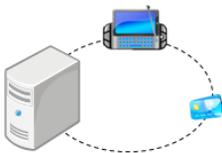
新技術の基となる技術その2: 写真復元鍵の分散化

鍵の種類	保存場所
目標画像	
変形画像	
使用される目標画像のID	
特徴量	or
変形率	

すべての鍵を揃えなければ、原画像は復元できない

本技術の使用例

- サーバ側
 - ③カードと端末認証する。
 - ④カード固有の写真復元鍵の一部を端末の公開鍵で暗号化し、端末に送る。
- 端末側
 - 1)カードと端末が相互認証を行う。
 - 2)会員情報を読み取り、サーバに送る。
 - 5)復元鍵を復号化して取り出し、端末のメモリから復元鍵の一部(目標画像)を獲得する。
 - 6)カードから写真復元鍵の一部(変形画像)を読み取り、もとの写真を復元する。
 - 7)写真を表示し、オペレータがユーザの認証を行う。

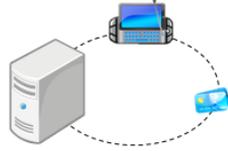


新技術の特徴・従来技術との比較

- 従来技術の問題点であった、セキュリティリスクを抑えることができる。
- セキュリティの向上だけではなく、変形画像を「芸術的に」することより、さまざまな顧客のニーズに答えられる。
- 例えば、自分の写真をより若く、より綺麗に変形できれば、好きなスター、好きなキャラに変形することもできる。
- 本技術の適用により、個人情報である写真が固く守られているため、次世代のクレジットカードとして期待される。

想定される用途

- 本技術は人の目でユーザの確認を可能にする技術である。
- もっとも有効と思われる応用としては、クレジットカードである。
- その他として、電子マネー、お財布携帯、免許書、住基カードなどへも応用できる。



13

想定される業界

- **利用者・対象**
 - 各種カードの製造会社、発行会社、商社など
- **市場規模**
 - 年間数千万枚と想定すれば、市場規模は数百億になると思われる。

14

実用化に向けた課題

- 現在、本技術に関連するアルゴリズム、プログラムなどはすべて開発済み、理論的には問題がない。
- 実装に当たっては、
 - カード側: 必要とされるメモリの削減
 - 端末側: 再現プログラムの高速化
 - サーバ側: より繊細な変形画像をより速く生成する手法などについて考察する必要がある。
- メモリの削減と画像の高速再現について、新しい方法を提案している(出願済み、出願中)。

15

企業への期待

- 端末について、基本的に本技術のソフトを組み込めば、既存の端末を多少更新すれば使用できる。
- このような端末を、カードの読み書きと写真の表示などの技術を持つ企業(例えば、デジカメ、携帯電話、ICカードリーダなどのメーカー)と共同開発したい。
- 十年経っても安心して使えるクレジットカード、身分証明カードなどを顧客に提供したいカード会社、政府機関などには、本技術の導入が有効と思われる。

16

本技術に関する知的財産権

発明の名称	認証カード、カード認証端末、カード認証サーバ及びカード認証システム
出願番号	特願2009-144420(平成21年6月17日出願)
出願人	公立大学法人会津大学
発明者	趙 強福

17

本技術に関する知的財産権

発明の名称	認証カード、カード認証端末、カード認証サーバ及びカード認証システム
出願番号	特願2010-144368(平成22年6月25日出願)
出願人	公立大学法人会津大学
発明者	趙 強福

18