5Z-5

ネットワーク上でデータと所有者を直接的に紐付けできるステガノグラフィを用いたデータ共有

福本 真輝† 宮嵜 仁志† 奥村 香保里†
福田 洋治‡ 廣友 雅徳†† 毛利 公美‡‡ 白石 善明†††
†名古屋工業大学 ‡愛知教育大学 ††佐賀大学 ‡‡岐阜大学 †††神戸大学

1. はじめに

一般にネットワークを介したデータ共有では相手の顔が見えないため，なりすましや改ざんなど不正な行為が行われる可能性がある．それらの被害を防ぐには，共有するデータとその所有者を紐付けしなければならない．

紐付けとは，あるデータに別の情報を関連付けることである．ネットワークを介してデータを共有する場面でデータとその所有者を紐づけるとは，データとデータの所有者を関連付けることを指す．このとき誤った人物を共有するデータと紐付けしないためには，本人確認を行わなければならない．

対面の取引では相手が顔見知りならば直接顔を見ることで本人確認できるが，非対面の取引では第三者が発行した本人確認のための証明書が必要である．ネットワーク上での従来のデータ共有は非対面の取引にあたる．ネットワーク上の本人確認のための認証は公開鍵暗号方式による信頼基盤の上で行われてきた．認証は電子署名によって行われるが，署名の作成者が署名鍵の所有者であるか確認できない．そこで証明書によって署名の作成者の認証が行われ，公開鍵の配布元が保証される．

公開鍵暗号方式による信頼基盤は Public Key Infrastructure(PKI) [1]と Pretty Good Privacy(PGP) [2]がよく知られている．PKI と PGP，いずれの信頼モデルにおいても本人確認はネットワーク上ではなく，第三者がオフラインで公開鍵配布元の本人確認をする．そして第三者の保証を公開鍵が正当である根拠としている．本人確認をネットワーク上でできれば，第三者を介さずに所有者の本人確認ができ，データと所有者を紐付けすることができる．

本稿では，顔見知りの二者間なら第三者を介することなくデータと所有者を直接的に紐付けできるデータ共有システムを提案する．ステガノグラフィを使用して相手が特定できる連続静止画に共有データを埋め込むことで，データと所有者が紐付けられるデータ共有を実現する．本人確認が正しく行われているか確認するために評価用システムを実装し，システムの基本性能の計測とユーザ実験を行った．

2. 電子署名と公開鍵による信頼基盤

2.1. 電子署名

公開鍵暗号方式を使用してデータを共有するとき，公開鍵が確かに相手のものであるか確認するには，電子署名による認証と公開鍵配布元を保証する証明書が必要である．署名の作成者の認証が不十分である場合，なりすまし，メッセージの偽造，改ざんにより電子署名は機能を果たさなくなる．

2.2. 認証パスの構築

従来は公開鍵による信頼基盤の上で，認証局(CA)と呼ばれる第三者がオフラインで鍵の所有者の本人確認を行い，CA の署名が入った証明書を発行することで認証が行われてきた．証明書は公開鍵と所有者を保証する．証明書の有効性検証は以下の手順で行われる．

1) 認証パスの構築
検証する証明書を発行した CA から出発して CA の信用関係を順にたどり，自分が信用しているトラストアンカー[1]まで結ぶ認証チェーンを認証パスと呼ぶ[1].

2) 認証パスの検証
認証パスのトラストアンカーから対象となる証明書までの全ての証明書に対して，証明書の署名，有効期限，失効の有無，証明書ポリシーの一致と制約条件を満たすかを検証する．すべての検証が成功したときに対象となる証明書が信頼できることがわかる．

2.3. PKI と PGP

公開鍵による信頼基盤は，PKI と PGP がよく知られている．PKI は，CA と呼ばれる第三者機関が利用者に公開鍵証明書を発行する．PGP は，公開鍵の保証を信頼できる第三者がすることにより個人レベルで信頼関係を構築する．いずれの方式もネットワーク上で本人確認ができないので，第三者をトラストアンカーにし，認証を行っている．

3. 第三者を介さないデータと所有者の紐付け

対面の取引では，顔を直接見ることができるため，顔見知りであれば本人確認できるが，非対面であるネットワーク上では本人確認ができない．もし本人確認をネットワーク上でできれば，第三者を介することなくデータと所有者を紐付けできる．

ネットワーク上で本人確認するには，顔が確認できる画像データと共に共有データを送る方法が考えられる．しかし，画像データと共有データは容易に分離できるため，データの変更や複製が可能である．本人確認をネットワーク上で安全に行うには画像データと共有データを紐付ける必要がある．

画像データと共有データを紐付けるための方法としてステガノグラフィの利用が考えられる．ステガノグラフィでは，隠したいデータ‘埋め込みデータ’を隠すメディア‘カバーデータ’に埋め込み，‘ステゴデータ’を作成する．ステゴデータから埋め込みデータを復元する作業を‘抽出’，埋め込みや抽出で使う鍵を‘ステゴ鍵’と呼ぶ．ステガノグラフィは情報が伝送されていること自体を隠すことを主目的にした情報ハイディング技術である[3]が，2 つのデータを結びつける目的で応用する．カバーデータを受信者が送信者を確認できるデータとし，埋め込みデータを送りたいデータとすることで，第三者を介することなくデータと所有者を紐付けることができる．

4. データと所有者を直接的に紐付けできるデータ共有システム

本章では，顔見知りの二者間のデータ共有において，対面でやり取りするのと同様に，直接的にデータと所有者を紐付けできる，画像に対するステガノグラフィを用いたデータ共有システムを提案する．そして，想定される提案システムへの攻撃とその対策について述べる．

4.1. 提案システムの構成

提案する認証付きデータ共有のモデルを図 1 に示す．送信者と受信者がそれぞれ操作するデバイスには，小型カメラと通信インタフェースが搭載されているものとする．提案システムは，

Authenticated Data Sharing Using Steganography
† Masaki FUKUMOTO, Hitoshi MIYAZAKI and Kaori OKUMURA・Nagoya Institute of Technology
‡ Youji FUKUTA・Aichi University of Education
†† Masanori HIROTOMO ・Saga University
‡‡ Masami MOHRI・Gifu University
††† Yoshiaki SHIRAISHI・Kobe University

Copyright ©2014 Information Processing Society of Japan.
All Rights Reserved.

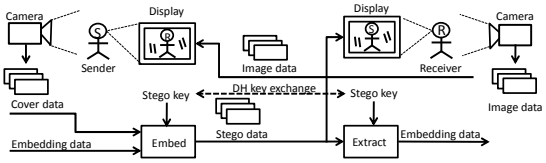

図 1　提案する認証付きデータ共有のモデル

以下の 4 つのフェーズから成り，これらを順に実現することにより認証付きデータ共有を実現する．

(1) ステゴ鍵共有フェーズ

DH 鍵共有法[4]に従い，ステゴ鍵を共有する．

(2) 本人確認フェーズ

共有したステゴ鍵のダイジェストから動作指示を生成する．受信者と送信者は互いにその指示に応じたアクションをカメラ前で行い，カメラから撮影した連続静止画をやり取りする．受信した連続静止画から相手が確かに意図した通信相手であるか，相手のアクションと動作指示が一致するかを確認する．

(3) セッション鍵共有フェーズ

送信者はセッション鍵を生成し，カメラから撮影した連続静止画の画像 1 枚 1 枚にステゴ鍵を使ってセッション鍵を埋め込み，受信者へ送信する．受信者はステゴ鍵を使って連続静止画からセッション鍵を抽出する．

(4) データ共有フェーズ

(3)と同様に，送信者はセッション鍵で暗号化した共有データを連続静止画に埋め込み，受信者へ送信する．受信者は，連続静止画から抽出したデータをセッション鍵で復号する．

データ伝送の観点では，通信経路上のノイズや第三者の偽造，改ざんによるステゴデータの変化を検出することが求められる．これについては埋め込みデータに共有データのダイジェスト，フラグメント情報を含めることで検出する．

送信者を写した連続静止画と共有データを結び付けるという観点では，連続静止画とステゴ鍵の関連付けが重要である．これについてはステゴ鍵のダイジェストから指示を生成し，カメラ前でそれに応じたアクションをとることとしている．

4.2. 提案システムへの攻撃についての考察

DH 鍵共有法に対しては，攻撃者が二者間に介在して両者になりすます中間者攻撃が可能である．ランダムに変化するステゴ鍵に合った送信者のアクションの映像を作り出すことが困難であることを前提として，提案システムでは動作指示により攻撃を検出することができる．

また，攻撃者が多数蓄積した送信者のアクションの映像を使って，なりすまし行為の検出をすり抜ける行為が懸念される．この対策として，ステゴ鍵と同様に共通鍵を共有し，ステゴデータを AES などの共通鍵暗号を用いて暗号化する方法が挙げられる．

5. 提案システムの評価

提案システムにおいて，連続静止画の表示品質が悪いと通信相手が本人であるか識別できなくなるため，安定して受信側で表示を続けなければならない．本章では評価用システムを実装して基本性能を測定し，それを用いてユーザ実験を行う．

5.1. 評価用システム

連続静止画による本人確認が正しく行われるかを評価するための評価用システムを実装する．実装した評価用システムのステゴ画像 R 成分の平均 PSNR(dB)，ステゴ画像の受信速度，データの受信速度を計測する．さらに，本人確認が正しく行われているかをユーザ実験により評価する．

評価用システムは，Java 言語，JDK7.0，Java Media Framework2.1.1e，TCP ソケット通信により実装している．使用した PC は，Windows7 Pro 64bit，メモリ 8GB，Intel Core i5-3210M 2.50GHz，Realtek PCIe GBE Family Controller である．動作指示は，ステゴ鍵のダイジェストから上下左右の指示を生成し，それに応じて体の一部を動かしてもらう，という方法を想定して実装した．ステガノグラフィは MBNS 法[5]を用いて，カラー静止画の R 成分(256 階調)のピクセル値にデータを埋め込んでいる．

表 1　基本性能の測定結果

画像サイズ	ステゴ画像の平均 PSNR (dB)	ステゴ画像の受信速度 (枚/sec)	データの受信速度(byte/sec)
128x128	39.2	22.0	22010
256x256	40.1	10.3	10310

5.2. 評価用システムの基本性能

カバーデータに対するステゴデータの品質劣化の割合は，PSNR=10 log10(256-1)2/MSE, MSE=1/(h・w)Σi Σj (P(i, j) - P'(i, j))2(縦 h ピクセル，横 w ピクセルの 256 階調グレイスケール画像の場合）により評価する．PSNR が大きいほどノイズが少なく，36dB 以上のとき人間にはステゴデータであることを知覚されないと言われている[6]．N=500 枚の ppm 形式カラー静止画へ長さ L=500,000 バイトの伝送データ m を分割して，埋め込み強度 1/Δ=2.0 で埋め込み，あて先へ TCP 送信する．100Base-TX の有線 LAN インタフェースによりハブ 1 台を介して対向接続し，画像 1 枚に対する埋め込みデータサイズを 1024byte(|i|=4byte, |N|=4byte, |m(i)|=1000byte, |dm(i)|=16byte)と設定し，画像サイズは 128x128 と 256x256 の 2 通りを計測した．計測結果は表 1 に示す．平均 PSNR は人間が知覚できないレベルである 36dB 以上となった．またステゴ画像の受信速度は毎秒 10 枚程度であり，送信者の本人確認に使用できるものと考える．このとき，毎秒 10Kbyte のデータ伝送ができることが確認できた．

5.3. ユーザ実験

ユーザ実験では，評価用システムを用いて 21 歳～26 歳の 12 人を対象にし，本人確認の際に録画によるなりすましであるか，本物であるかを判断してもらうかたちで 1 人ずつ実験を行った．その結果，被験者全員が録画と本物を見分け，本人確認できた．

6. おわりに

本稿では，顔見知りの二者間なら，第三者を介することなく，ステガノグラフィを用いたデータと所有者を直接的に紐付できるデータ共有システムを提案した．データ共有にはステガノグラフィ技術を用い，カバーデータを通信相手が確認できるデータとし，埋め込みデータを送りたいデータとすることで，データと所有者を紐付けている．

本人確認が正しく行われるか確認するために，評価用システムを実装して基本性能を測定し，それを用いてユーザ実験を行った．実験の結果，被験者全員が録画と本物の映像を正しく見分け，本人確認できた．実際の利用する場面に即した WAN や無線通信などの環境下においても評価をし，安定した動作をするように改良することを今後の課題とする．

参考文献

[1] IPA：情報セキュリティ分析ラボラトリー準備室，PKI 関連技術情報，<http://www.ipa.go.jp/security/pki/pki.html>，(参照 2014-01-08).

[2] Atkins, D., Stallings, W. and Zimmermann, P.: PGP Message Exchange Formats, IETF RFC 1991(1996).

[3] 松本勉：インフォメーションハイディングの概要，情報処理学会誌，Vol.44，No.3，pp.227-235 (2003).

[4] Diffie, W. and Hellman, M.: New Directions in Cryptography, IEEE Trans. Information Theory, Vol.22, No.6, pp.644-654 (1976).

[5] Zhang, X. and Wang, S.: Steganography Using Multiple-Base Notational System and Human Vision Sensitivity, IEEE Signal Processing Letters, Vol.12, No.1, pp.67-70 (2005).

[6] Wu, N.I. and Hwang, M.S.: Data Hiding: Current Status and Key Issues, International Journal of Network Security, Vol.4, No.1, pp.1-9 (2007).

Copyright ©2014 Information Processing Society of Japan.
All Rights Reserved.