4Y-3

Webカメラを用いたステガノグラフィによる送信者確認機能付きデータ秘匿伝送方式

掛布　朋宏†　　毛利　公美‡　　福田　洋治††　　白石　善明†

名古屋工業大学†　　岐阜大学‡　　愛知教育大学††

1. はじめに

ネットワーク通信で離れた相手とデータの送受信を行う場合，悪意のある第三者が送信者になりすますという懸念がある．

なりすましに対抗する手段として，一般的にデジタル署名が用いられる．これは公開鍵基盤を利用し，送信者の公開鍵証明書を信頼できる第三者機関が保証することで実現されるが，事前に送信者が秘密鍵，公開鍵を用意する必要があること，信頼できる第三者機関に公開鍵証明書を発行してもらう必要があること，受信者が送信者の公開鍵証明書を検証する必要があること等，利用に際したコストは大きい．また，秘密鍵が第三者に漏えいしてしまうとなりすましを許し，否認防止ができなくなるため，利用者個人による秘密鍵の管理は厳重になされなければならない．

鍵管理が容易で簡易な認証方式として生体認証がある．これは個人から切り離すことができない身体的特徴あるいは身体的特性を利用することで，第三者によるなりすましを防ぐものであるが，人が人を確認するような認証に用いるのは容易ではない．

そこで，本稿では Web カメラを用い，送信者を写した画像に，ステガノグラフィ技術により共有するデータを秘匿したステゴ画像を作成し，ステゴ画像を連続送信することで，データに対する送信者の関連付けがなされるデータ送受信方式を提案する．この方式は，データ送信と同時に人対人認証を行うという特徴を持つ．受信者が送信者を識別する認証には送信者を写した動画データを用いるため，誤認証の危険性は小さく，また，認証のための鍵の事前準備が必要なく，即時に送信者の検証が可能である．

2. 送信者確認機能付きデータ秘匿伝送方式

提案する方式のモデル図を図 1 に示す．

本方式では，共有したい秘密データを送信者が確認可能なデータに埋め込むことで，データに対する送信者の関連付けを行う．受信者は受信した埋め込みデータから送信者の確認，秘密データの抽出を行いデータを共有する．

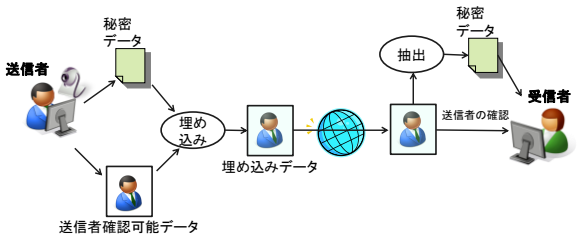


図 1 提案方式のモデル図

ここで，送信者が確認可能なデータとして Web カメラで送信者を写した静止画の連続，つまり動画データを用いる．この動画データは送信者のみが作成可能であり，また，動画データというものは受信者が視覚的に容易に送信者の確認が可能である．送信者の検証は受信者が送信者に簡単な指示を出し，動画の送信者がそのように振る舞うことを確認すればよく，確かに今，動画に映っている送信者がデータを送信しているということを検証できる．

データ埋め込み処理にはステガノグラフィを用いる．ステガノグラフィとはデータハイディング技術の一つであり，データを他のデータに埋め込むことでその存在を他者から隠す技術である．埋め込む先のデータをカバーメディア，カバーメディアにデータを埋め込み，作成したデータをステゴメディアと呼ぶ．特にカバーメディアが画像の時，そのカバーメディアをカバー画像と呼び，作成したステゴメディアをステゴ画像と呼ぶ．また，埋め込み，抽出時に用いる鍵をステゴ鍵と呼ぶ．

3. 確実なデータ伝送

データの伝送はステゴメディアからデータを切り出し，いくつかのパケットに分けて送信を行う．受信者は受け取ったパケットからステゴメディアの再構成，秘密データの抽出を行う．この際パケットロスが発生すると，受信者はステゴメディアの再構成が不可能となり，秘密データの抽出も不可能となる．よって欠落したパケットの再送制御を行うプロトコルが必要であり，パケットロス自体を抑える送信制御も有効であると考えられる．

パケットロスの主な原因として，受信側のビジー状態によるパケットの取りこぼしが考えられる．そこでパケットロスを減らすために送信側で一時的な待機処理による送信制御を行う．送信制御は 1 パケットの送信毎に行われる．

実装したシステムの全体図と動作手順を図 2 に示す．

Data Concealed Transmission Method with Sender Confirmation Function by Using Web Camera and Steganography

† Tomohiro Kakeno and Yoshiaki Shiraishi ・Nagoya Institute of Technology

‡ Masami Mohri ・Gifu University

††Youji Fukuta・Aichi University of Education

Copyright ©2011 Information Processing Society of Japan.
All Rights Reserved.

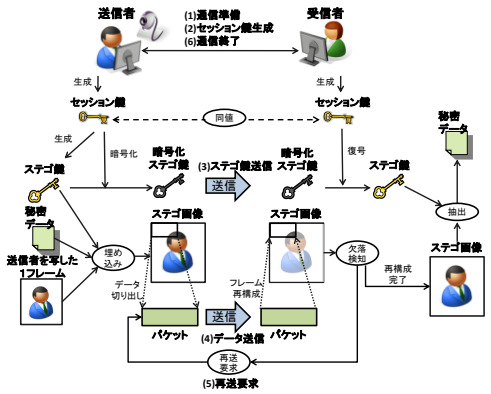


図 2 システムの全体図

(1). 通信準備段階
- 互いに SYN を送り合い，通信を確立する

(2). セッション鍵生成段階
- Diffie-Hellman 鍵共有により互いにセッション鍵を作成

(3). ステゴ鍵送信段階

[送信側]
- セッション鍵からステゴ鍵を生成
- セッション鍵を使いステゴ鍵を暗号化して送信

[受信側]
- 受信した暗号化ステゴ鍵をセッション鍵で復号して所持
- 鍵を受け取ったことを送信側に通知

(4). データ送信段階

[送信側]
- カメラから画像を 1 フレーム分取得
- 秘密データを埋め込み，ステゴ画像を作成
- パケットに切り出して 1 フレーム分送信
- 1 パケット送る毎に送信制御を行う

[受信側]
- 受け取ったパケットからデータを取り出し，バッファに格納

(5). 再送要求段階

[送信側]
- 再送要求に対するパケットを送信

[受信側]
- 欠落したパケットを検知して再送要求を行う

(6). 通信終了段階
- 秘密データが残っている場合は，(3). ステゴ鍵送信段階に戻る
- 秘密データの共有が終わった場合は，互いに FIN を送り合い，通信を終了する

4. 実装

実装したシステムの開発環境を表 1 に示す．

表 1　開発環境，使用機器

開発言語	Java
利用した API	Java Media Framework 2.1.1e
Web カメラ	Logicool® HD Pro Webcam C910

また，ステガノグラフィの手法として EDS-MBNS 法[1]を用いてステゴ画像の作成を行った．EDS-MBNS 法とは，埋め込みデータを多基底表記し，カバー画像に埋め込む手法である MBNS 法[2]を拡張した手法である．

5. 評価実験

送信制御の有効性を確認するために 2 台の PC 間で UDP 通信を行い，送信制御有りと無しの場合について，

I. スループット
II. パケットロス率

の 2 つの比較を行った．実験機の構成を表 2 に，実験時のパラメータを表 3 に示す．また，結果を表 4 に示す．

結果から送信制御が有る場合，パケットロスを大幅に削減でき，スループットが向上することが確認できた．

表 2　実験機の構成

	送信側 PC	受信側 PC
CPU	Intel® Core i5 650 @3.20GHz	Intel® Core Duo T2300 @1.66GHz
GPU	NVIDIA GeForce 8400GS	NVIDIA Quadro NVS 110M
メモリ	4GB	1GB
OS	Windows7 Professional 64bit	Windows XP

表 3　パラメータ

送信制御の待機時間	200[ns]
画像サイズ	200×200
1 パケットサイズ	1500[byte]
1 フレームに埋め込むデータサイズ	1000[byte]

表 4　実験結果

	送信制御有り	送信制御無し
スループット[Mbps]	2.67	0.08
パケットロス率[%]	1.96	40.82

6. おわりに

本稿では Web カメラを用いたステガノグラフィによる送信者確認機能付きデータ秘匿伝送方式を提案した．本方式は送信者が確認可能なデータに対して共有する秘密データを埋め込んで送信することで，事前準備や検証処理に時間をかけずにデータの送信者の確認が簡易に可能なデータ伝送方式である．

本方式を実装したシステムにおいて，データ送受信時に送信側が送信制御を行うことで，パケットロスを削減でき，スループットが向上することを確認した．

参考文献

[1]. 宅間勇太，福田洋治，白石善明，“埋め込み量を制限したステガノグラフィにおける未使用領域の利用に関する一考察”，電子情報通信学会総合大会，A-7-20，2007 年 3 月．

[2]. Xinpeng Zhang, Shuozhong Wang, “Steganography Using Multiple-Base Notational System and Human Vision Sensitivity”, IEEE Signal Processing Letters, Vol.12, pp.67-70, Jan. 2005.

Copyright ©2011 Information Processing Society of Japan.
All Rights Reserved.