様式 C-19

科学研究費補助金研究成果報告書

平成２２年　４月２０日現在

研究種目：若手研究（Ｂ）
研究期間：2008～2009
課題番号：20760256
研究課題名（和文）　ストリーミングデータに対する適応的なデジタル署名の開発

研究課題名（英文）　A Development of Adaptive Digital Signature of Stream Data

研究代表者
酒井　正夫　　（SAKAI MASAO）
東北大学・教育情報基盤センター・准教授
研究者番号：30344740

研究成果の概要（和文）：
本研究では，ストリーミングデータに対する適応的なデジタル署名の開発に資する，ストリーミングデータに対する予測モデルの動的設計法を開発した．今回開発した手法は，対象とするストリーミングデータの特性と使用可能な計算資源量に応じた予測モデルを動的に設計することが可能である．
また，今回の開発手法は，呼吸性振動を行う悪性腫瘍に対する放射線治療の研究分野においても効果的に応用可能であることを合わせて示した．

研究成果の概要（英文）：
In this research, a new prediction method of stream data for developing adaptive digital signature was proposed. The method can design the optimized prediction model corresponding to dynamics of target stream data and available CPU resource.
In addition, the method can effectively apply real-time tracking technology of tumor motion in radiation therapy field.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	300,000	90,000	390,000
2009 年度	100,000	30,000	130,000
年度			
年度			
年度			
総　計	400,000	120,000	520,000

研究分野：工学
科研費の分科・細目：電気電子工学・システム工学
キーワード：デジタル署名，ストリーミング，時系列，予測

１．研究開始当初の背景

ストリーミングデータに対してデジタル署名を付加する場合，厳密性にこだわる従来手法を用いたのでは膨大な計算コストが必要であり，計算資源が制限される一般的な民生機器では実装が困難である．この問題に対して，研究代表者は，デジタル署名の正当性（偽造困難性）と署名作成に要する計算コストのバランスを定量的に制御できるデジタル署名技術の可能性を検討している．この新

しいデジタル署名技術をストリーミングデータに適用することで，データのビットレートやレコーダ装置の性能に最適化したデジタル署名の付加が可能になると期待できる．この場合，作成されたデジタル証明による改竄検知精度も確率的なものとなるが，別途開発する確率増幅定理のアイデアを用いた補償を行うことで，実用的なレベルでの検知精度の向上が可能と考えられる．研究代表者らは，これまでに同様な研究例として，音楽データに対して電子透かしを確率的かつ冗長に埋め込むことで，品質への改変を低減しつつ，秘匿性の高い電子透かしの埋め込みが可能であることを示している．

デジタル署名に用いる公開鍵と秘密鍵の安全な作成方法については，トラスト（秘密鍵）を複数のエージェントにより分散して作成・管理することで，トラストの漏洩リスクを完全に回避可能な手法が存在する．この手法で作成される鍵のペアは健全性が保証されるが，完全性については不十分であることが指摘されている．そのため，その実装に関する研究はまだほとんど行われていない．しかし，用途によっては，十分高い確率で正しく動作すれば，例えエラーが発生したとしても十分実用的な場合もある．研究代表者らは，これまでに同様な研究例として，トラストを複数の認証局で分散共有管理することでPKI(公開鍵基盤）の信頼性を向上させる手法を開発している．

２．研究の目的

電子デバイスや圧縮符号化技術の発展により，現代では，映像や音楽などの情報を高品質な状態でデジタルデータとして記録することが可能である．しかし，磁気テープやフィルムなどのアナログメディアにありのままに焼き付けられる情報とは異なり，圧縮符号化されたデジタルデータは，人間が認識できないレベルの多くの情報が失われており厳密な意味では正確ではない．また，デジタルデータは 0 と 1 の有限ビット列で表される情報であるため計算機を用いて容易に改変が可能であり，究極的には，いかなるものも人工的に作成可能である．したがって，デジタルカメラなどのレコーダ装置を用いて作成したデジタル情報に対して高度な改竄が施された場合，アナログ情報のようにその他の領域との比較から，それを見破ることは困難である．

デジタルデータに対する改竄の有無を検証する方法として，デジタル署名や電子透かしの技術の応用が考えられる．これらの技術によりデータにデジタル署名を付加することで，それ以降に施された改竄を検知することが可能になる．しかし，デジタル署名を付加する前段階で施された改竄を検知することは当然不可能であり，また，デジタル署名の付加処理に人の手が関わる場合は，その人物からトラスト（安全の根幹をなす情報：デジタル署名の場合は秘密鍵）が流出してしまうリスクがある．

これらの問題を根本的に解決するためには，レコーダ装置の圧縮符号化処理の過程にデジタル署名を付加する機能を実装し，はじめからデジタル署名付きのデータを書き出すことが有効と考えられる．しかし，ストリーミングデータに対するデジタル署名の作成処理は，一般的に膨大な計算コストが必要でありリアルタイム処理を行うことが困難である．また，トラストの漏洩リスクを回避するために，その作成と管理の自動化も考慮すべきである．

そこで，本研究では，ストリーミングデータに対する実用的なデジタル署名技術を開発し，最終的には，それをデジタルカメラなどのレコーダ装置に安全に実装する方法を開発することを目的とする．

３．研究の方法

ストリーミングデータに対してリアルタイムでデジタル署名を作成する場合，用いる手法によってはその計算コストが必ずしも常時一定ではなく，例えば，ストリーミングデータの直近のダイナミクスなどに依存して変化する．また，そのデジタル署名作成の処理を，ハードウェアで実現しようとする場合，想定される最悪値に耐えうるように性能（単位時間当たりの計算資源）を設計する必要がある．つまり，ハードウェアによるリアルタイム処理においては，逐次，計算資源に余剰が生じることになる．

もしこの余剰な計算資源を用いて，ストリーミングデータの正確な将来予測が可能だとすると，その予測結果を活用することで，本来はリアルタイムで処理されるデジタル署名作成を，準リアルタイムで行うことが可能になる．そこで，本研究では，動的に変化する計算資源を用いた適応的なデジタル署名の作成技術の開発に資することを目的に，ストリーミングデータに対する予測モデルの動的設計法の開発を行った．

本研究で対象とするストリーミングデータには，放射線治療の際に観測された肺腫瘍マーカの時間変動データを用いた（図１，２を参照）．

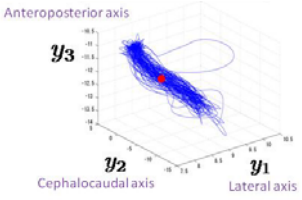

図 1 肺腫瘍マーカのダイナミクス

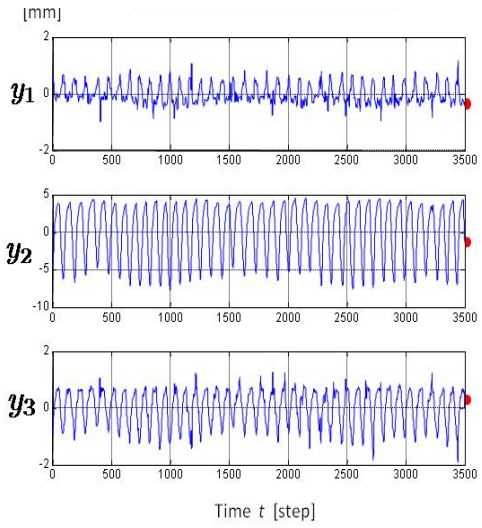

図２　肺腫瘍マーカの各軸方向の時間変動

図２が示すように，肺腫瘍マーカの各軸方向の時間変動は，呼吸性の比較的単純な周期運動であり，その予測は容易なようにも思える．しかし一方で，生体特有のカオス的性質を含むことから，本研究に適した実用的なストリーミングデータと言える．

本研究では，周期運動ダイナミクスを考慮した近似モデル Seasonal AutoRegressive Integrated Moving-Average (SARIMA)モデル

$$\phi(B)\Phi(B^s)(1-B)^d(1-B^s)^D y(t) = \theta(B)\Theta(B^s)e(t)$$

$$\phi(z) = 1-\phi_1 z-\phi_2 z^2-\cdots-\phi_p z^p$$

$$\Phi(z) = 1-\Phi_1 z-\Phi_2 z^2-\cdots-\Phi_P z^P$$

$$\theta(z) = 1+\theta_1 z+\theta_2 z^2+\cdots+\theta_q z^q$$

$$\Theta(z) = 1+\Theta_1 z+\Theta_2 z^2+\cdots+\Theta_Q z^Q$$

を基に，新しい予測モデルとその設計アルゴリズムを開発した．SARIMA モデルはモデル次数(p, P, q, Q, d, D)を変更することで，計算コストや同定精度を，容易にかつ即時に調整できるという特徴があり，動的に変化する計算資源量に応じて予測モデルを動的に設計するという本研究の目的に適している．

また，本研究では，ストリーミングデータの周期ダイナミクスの時間変動が，予測精度に及ぼす影響を解析し，その悪影響を回避するための改良も行った．本研究で開発した予測システムの概略を図３に示す．

なお，本研究では，予測システムの開発やその性能評価などのすべてを，技術計算ソフトウェア Matlab を用いてオフラインにて行った．

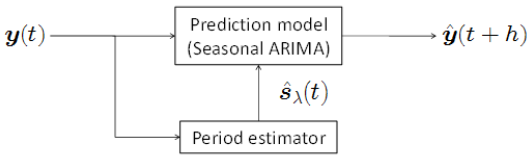

図３　開発した予測システムの概略図

４．研究成果

動的に変化する計算資源量に応じて，ストリーミングデータに対する予測モデルを適応的に設計する予測システム（近似モデルとアルゴリズム）を開発した．

将来，投入する計算資源量に応じて，その正当性（偽造困難性）を調整可能なデジタル署名作成の技術が出現した場合，今回開発した予測システムが，そのハードウェア化の際の性能向上や低コスト化に役立つと期待できる．

また，今回開発した予測システムは，自然界で観測される一般的な時系列データを対象とする汎用システムとしても高い性能が期待できる．実際，放射線治療の分野で求められる肺腫瘍マーカ位置の変動予測において，既存の予測手法に比べて高い予測精度が実現できることを示した(図４参照)．このように，本研究の成果は，情報セキュリティの分野に限らず，幅広い分野への応用が期待できるものである，

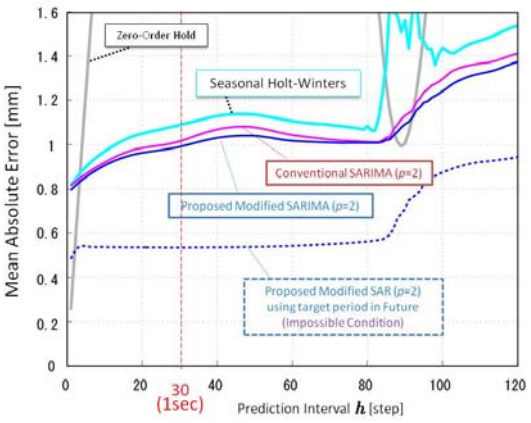

図４　本研究で開発した予測システムと既存の予測手法との，肺腫瘍マーカの変動予測精度の比較．横軸が予測区間長(h)，縦軸が平均絶対誤差，

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計２件）

1.　N. Homma, S. Kato, T. Goto, Masao Sakai,

N. Sugita, M. Yoshizawa, Y. Sassa et al., Human Brain Activities Related to Manual Control of a Nonholonomic System: An F-MRI Study, IJACE International Journal of Advanced Computer Engineering, 査読有, Vol.2, 2009, 129-133

2. N. Homma, M. Sakai, H. Endo, M. Motsuya, Y. Takai, M. Yoshizawa, A new motion management method for lung tumor tracking radiation therapy, WSEAS TRANSACTIONS on SYSTEMS, 査読有, Vol.8, No.4, 2009, 471-480

〔学会発表〕(計 5 件)

1. 酒井正夫, 本間, 高井, 追跡照射放射線治療のための肺腫瘍位置の呼吸性変動予測モデル, 第 51 回 自動制御連合講演会, 2008 年 11 月 22 日, 山形大学

2. 遠藤, 酒井正夫, 本間, 高井, 吉澤, 追跡照射放射線治療のための腫瘍位置の呼吸性変動予測法, 計測自動制御学会東北支部 第 249 回研究集会, 2009 年 3 月 13 日, 東北大学

3. 市地, 酒井正夫, 本間, 高井, 吉澤, 放射線治療のための肺腫瘍位置変動の周期ダイナミクス予測に関する一考察, 計測自動制御学会東北支部 45 周年記念学術講演会資料, 2009 年 9 月 7 日, 岩手大学

4. K. Ichiji, M. Sakai, N. Homma, Y. Takai and M. Yoshizawa, A Time Variant Seasonal ARIMA Model for Lung Tumor Motion Prediction, The Fifteenth International Symposium on Artificial Life and Robotics 2010(AROB 15th '10), February 5, 2010, B-Con Plaza, Beppu, Oita, Japan

5. Masao Sakai, Prediction Method of Unsteady Periodic Tumor Motion for Readiotherapy, 5th International Symposium on Medical, Bio- and Nano-Electoronics, February 25, 2010, Senda Japan

〔図書〕(計 0 件)

〔産業財産権〕
○出願状況 (計 0 件)

○取得状況 (計 0 件)

〔その他〕
ホームページ等

６. 研究組織
(1)研究代表者
酒井　正夫 (MASAO SAKAI)
東北大学・教育情報基盤センター・准教授

研究者番号：30344740

(2)研究分担者
(　　)

研究者番号：

(3)連携研究者
(　　)

研究者番号：