

論文賞贈呈

(写真：敬称略)

論文賞（第64回）は、平成18年10月から平成19年9月まで本会和文論文誌・英文論文誌に発表された論文のうちより下記の12編を選定して贈呈した。

Traitor Tracing Scheme Secure against Adaptive Key Exposure and its Application to Anywhere TV Service

(英文論文誌 A 平成19年5月号掲載)



受賞者 小川一人 受賞者 花岡悟一郎 受賞者 今井秀樹

本論文は、デジタルコンテンツの著作権保護を目的とした不正利用者追跡法(Traitor Tracing方式)を考察し、視聴場所が固定されないペイTVへの応用を提案している。Traitor Tracing方式は、コンテンツを再生する秘密鍵を管理することにより、不正な海賊版デコーダを作成したユーザを特定できるシステムである。しかし、秘密鍵が一度漏えいした場合は、過去にさかのぼってすべての情報が安全ではなくなる問題点があった。

本論文では、適応的鍵漏えい攻撃という最も強い敵を仮定した場合でも安全な方式を提案することに成功している。Kurosawa-Desmedt方式及びKey-Insulated方式を改良することにより、ユーザIDと時刻を変数に持つ2変数多項式を利用し、指定時刻に対する秘密鍵とマスター鍵の両方を有する場合のみに鍵の更新が可能な方式を構成している。つまり、秘密鍵の漏えいはシステムが事前に指定した期間のみに限られるため、想定される被害は必要最小限に抑えることが可能となる。

通常のペイTVでは、受信者に安全なデコーダ(STB)を配布することにより放送にスクランブルをかけているが、何らかの理由でSTB内部の秘密情報が漏えいした場合は、ペイTVのシステム全体が危険な状況にさらさ

れる。本提案方式では、適応的鍵漏えい攻撃という攻撃者にとって最も有利な状況を許したとしても安全なTraitor Tracing方式を提案しており、ペイTV型の課金放送における著作権保護の確立に大きく貢献している。また、衛星放送のスクランブル方式であるCAS方式の問題点を解決する実用システムも提案しており、実社会の課金放送においても十分に有効性がある。

一方、本論文で提案された方式の安全性証明に利用された数学技術は暗号学的に高度なものである。このように学術的に優れた論文が実用的な価値をも持つ方式を提案している点は非常に高く評価できる。



DCT係数の正負符号と位相限定相関との関係について

(和文論文誌 A 平成19年7月号掲載)



受賞者 伊藤 泉 受賞者 藤吉正明 受賞者 貴家仁志

2枚の画像間の幾何変換量を高精度に推定する手法の一つに、離散フーリエ変換(DFT)の位相を用いた位相限定相関法があり、生体認証やステレオ視など種々の認識技術に利用されている。これは、位相が画像の構造的特徴を保持するというフーリエ変換の性質に基づくもの

であり、振幅情報を一様化して位相のみに限定することにより、ノイズや照明変化に対してロバストな推定を可能とするものである。DFT 係数は複素数であり、位相は一般に位相項という複素平面における単位円上の値として扱われる。また、画像のデータ量は概して膨大である。したがって、この膨大なデータに対し、利用する位相項の抽出時、及び相関計算時に複素数演算を必要とする位相限定相関法は、データ量や計算量の低減が課題とされてきた。

本論文は、離散コサイン変換 (DCT) 係数の正負符号が位相情報を持つことに着眼し、DCT の正負符号を用いた新しい相関法を提案している。これは、DCT の正負符号と DFT の位相項との関係を理論的に近似なしで厳密に記述することにより導出されている。したがって、相関計算に利用する DCT 係数の正負符号は 2 値情報であり、この 2 値情報から画像間の幾何変換量が推定される。DCT 係数が実数値であること、及び利用する正負符号の抽出の容易さは課題とされたデータ量や計算量の低減に寄与する。また、振幅情報を減じる効果からノイズや照明変化に対してロバストな推定ができる。更に本論文では DCT を要素技術とする圧縮画像に対する有効性を述べ、その優位性を示している。

本論文は、DCT 係数の正負符号という 2 値情報から画像間の幾何変換量が推定されることを世界で初めて示した。本論文で導かれた DCT の正負符号と DFT の位相項の関係は、解析理論としての一般性、普遍性を有し、DCT 正負符号による位相表現が可能となり、今後種々の分野においてその応用が期待される。また、DCT 係数は画像情報圧縮との親和性が高く、画像の情報圧縮と認識理解の技術的融合の可能性を示している。

本論文は高い新規性と独創性を有し、信号処理、情報圧縮、パターン認識などの広範囲の分野に多くの示唆を与え、その価値は高く評価できる。



Construction Algorithm for Network Error-Correcting Codes Attaining the Singleton Bound

(英文論文誌 A 平成 19 年 9 月号掲載)



受賞者 松本隆太郎

喜安善市賞 (第 1 回) に別掲



ターボ等化の基礎、及び情報理論的考察

(和文論文誌 B 平成 19 年 1 月号掲載)



受賞者 松本 正



受賞者 衣斐信介

ターボ符号の発見は、一般に「ターボ概念」と呼ばれる新しい信号処理の流れを生み出した。最近、このアプローチはシングルキャリアや広帯域移動通信における符号間干渉等化の研究の流れに大きな変化を及ぼしつつある。シングルキャリアや広帯域移動通信は符号間干渉等化のための演算処理量が膨大となるために実現不可能と考えられてきた。そのことを「ターボ概念」は覆しつつある。

本論文は招待論文であるため、解説と新技術提案という、二つの目的を持っている。著者らは、これを達成するために、相互情報量の伝達特性を評価するためのツールである、EXtrinsic Information Transfer (EXIT) チャートを基盤に置いた解説を試みている。論文は、著者らが研究している Soft Cancellor followed by Minimum Mean Squared Error filter (SC-MMSE) 型ターボ等化アルゴリズムの動作の説明で開始される。ここでは、ターボ等化器の漸近特性が示されるとともに、「その構成要素である MMSE フィルタ部分とチャネル符号の復号器がど

のような役割を果たすとき、この漸近特性が得られるのか」という問題が提起されている。つまり、収束特性の解明が必要なことを明示的に述べられている。

SC-MMSE 型ターボ等化アルゴリズムの解説の後に、EXIT チャートの一般的な求め方が述べられ、これで準備段階が終了される。本論文の主題は、上記で提起された問題に解を与えることから始められる。つまり、EXIT チャート解析の手法を MMSE フィルタとチャンネル符号の復号器に適用し、繰返しごとにこれらがどのように相互情報量を増大させていくかを明らかにしている。これによって、両者の EXIT カーブを、1 に近い相互情報量が得られる以前の段階でクロスさせないとき、上述の漸近特性が得られることが明らかにされる。更に、「両者の EXIT カーブがクロスしないまま、できるだけそのギャップを少なくするように設計するとき、漸近特性が得られることを保障しながら伝送できる情報レートを最大にできる」という結論に到達する。

多次元 EXIT チャートやプリコーディングなどへの拡張について述べられた後、本論文は示唆に富む最終パラグラフで終了される。著者らは、EXIT チャートを駆使することで、解説と技術提案という二つの目的を見事に達成している。最終パラグラフからは著者らの深い熱意が感じ取れる。



通信ネットワーク故障による 社会的影響度分析法

(和文論文誌 B 平成 19 年 4 月号掲載)



受賞者 船越裕介



受賞者 松川達哉



受賞者 渡邊 均

通信網の信頼性評価の基本は、故障による社会的影響を低く抑えることにある。従来の信頼性研究においては、この社会的影響を定量化する明確な尺度と定義がなく、また、実データから通信網故障の社会的影響を定量化する試みもほとんど行われていない。著者らは、通信網における故障データとして普遍的かつはん用的なデータである故障発生時の影響規模と申告件数に対し、発生時の通信トラヒックとサービス停止時間による重み付けを行

うという斬新なアイデアにより、今まで明確な定義の存在しなかった通信網故障による社会的影響度を実データから定量化する初めての指標を提案した。更に、統計分析の手法を駆使した実際の故障データ解析を通じ、本指標が故障発生とそれに伴うメディア報道の有無の関係を定量化していることを示し、これまで抽象的な概念にとどまっていた、信頼性設計における社会的迷惑量との等質性を提示している。

通信網における信頼性は、従来、網計画・構築時における信頼性設計に重点が置かれており、いったん構築された通信網の運用段階における信頼性を実データで評価する手法については、十分に研究されてきたとは言い難い。本研究は、そのような状況に重要な一石を投じるものである。今まで理論的土台となる研究の存在しなかった、通信網の運用フェーズにおける実データと社会的影響度に基づいた信頼性管理技術という新たな領域を開拓するものであり、正に先駆的研究であるといえよう。

通信網の信頼性管理は、設計フェーズの検討だけでは十分ではなく、むしろ運用中の通信網の信頼性を的確に把握し、必要な対処を迅速に行うことこそが重要である。本論文はそのような、運用フェーズにおける信頼性管理技術の確立に向けた重要な基礎理論を提案したものであり、信頼性理論としての独創性と、信頼性管理技術としての有用性の両面において、高く評価できる。

以上の理由から、今回の受賞は適切なものであり、また、今後も著者らが本分野のパイオニアとして研究を継続、発展させることを願ってやまない。



電波伝搬特性を活用した秘密情報の 伝送・共有技術

(和文論文誌 B 平成 19 年 9 月号掲載)



受賞者 岩井誠人



受賞者 笹岡秀一

本論文は、無線通信における電波伝搬特性を活用した秘密情報の伝送・共有技術、すなわち、無線セキュリティ技術に関する招待論文である。特に電波伝搬の立場から本技術について述べている。電波伝搬特性をセキュリ

ティ技術に応用しようという試みは、海外においても Physical Layer Security などと称して近年研究が盛んになっている。著者らはこれらにも先駆けてこの分野の研究を進め、実用に供することが可能なレベルにまでその技術を築き上げてきた。

著者らが検討する電波伝搬特性を活用する無線セキュリティ技術は、移動通信環境におけるマルチパスフェージングの場所依存性に基づいている。すなわち、マルチパスフェージングに起因する種々の特性—信号強度や位相の変動・マルチパス遅延・デジタル伝送特性など—は、ある2地点の送受信伝搬路に特異なものであり他地点では得ることができない。この特性を秘密鍵の生成などセキュリティ技術に応用しようというアプローチである。受賞論文では、この基本原理を示し、これに基づいて鍵情報を配送することなく離れた送受2地点間で秘密鍵を生成・共有可能な具体的実現方法を提示している。また、実用的な観点のみならず、情報理論における相互情報量を用いた解析を行い安全に共有可能な秘密情報量に関する理論的根拠も示した。更に、電波伝搬的なアプローチによる情報盗聴の試み（アタック）の方法を検討し、それに対する耐性についても評価している。

著者らが進めてきた電波伝搬特性を活用した無線セキュリティ技術は、セキュリティ対策としてはある意味「異端」ともいえるものである。すなわち、暗号や認証などという高度な安全性の保証が必要な技術分野において、ランダム性の高い電波伝搬という自然現象的なものを礎とすることは常識とは異なる。それに対して著者らは、電波伝搬・無線通信・誤り制御などの種々の無線通信の技術を駆使し、セキュリティ的に成り立つレベルにまで本技術を磨き上げてきた。この点に大きな価値がある。

特に、ユビキタスネットワークなど今後小形化・分散化する将来の通信形態との親和性は高く、今後の新しい研究分野を切り開くことが期待される。



A 130-nm CMOS 95-mm² 1-Gb Multilevel AG-AND-Type Flash Memory with 10-MB/s Programming Throughput

(英文論文誌 C 平成 18 年 10 月号掲載)



受賞者 倉田英明



受賞者 佐伯俊一



受賞者 小林 孝



受賞者 笹子佳孝



受賞者 有金 剛



受賞者 吉田敬一



受賞者 高瀬賢順



受賞者 吉竹貴之



受賞者 土屋 修



受賞者 池田良広



受賞者 鳴海俊一



受賞者 金光道太郎



受賞者 伊澤和人



受賞者 古沢和則

フラッシュメモリは、デジタルカメラ、USBメモリや音楽プレーヤなどの大容量データストレージとして急速に普及してきた。フラッシュメモリの急速な普及を支えたのは、ムーアの法則を上回るペースで進展した大容量化である。フラッシュメモリの大容量化には、セルの微細化に加えて、一つのセルに2bit以上の情報を記

憶する多値技術が必要不可欠であるが、多値技術を適用すると、セルのしきい値状態を高精度に制御しなければならず、特に書込み速度が大幅に低下するという問題があった。

本論文は、多値でも高速な大容量フラッシュメモリを実現する手法を提言し、実チップによる検証を行ったものである。著者らは、①セル速度の向上、②セル間の特性ばらつき抑制、③書込み単位の増大の三つのアプローチで書込み速度向上を図っている。まず AG-AND 型セルを用いて、ホットエレクトロン注入による高速なセル書込みを実現した。また、ビット線に蓄積した一定量の電荷をホットエレクトロン注入に用いる定電荷注入方式を提案し、セル間の特性ばらつきを従来の 40% 程度に抑制している。更に、4 バンク構成を採用し、書込み単位を従来の 4 倍とした。以上の技術により、これまでの多値 (2 bit/セル) フラッシュメモリに対して約 5 倍の書込み速度を実現している。

一方、低コスト化のためにはチップ面積の縮小が必須となる。提案された AG-AND 型セルでは、阻止分離用 STI が不要であり、ビット線ピッチを従来の 4F から 3.1F に低減することができる。また、4 バンク構成採用によるバッファ面積の増加を抑制するため、センスラッチへのデータ転送をパラレルからシリアルとし、バッファを SRAM に組み込むことで、面積増加を約半分に抑えている。

著者らは、0.13 μm プロセスを用いて 1GByte 多値フラッシュメモリを製造し、チップ面積 95mm² を実現するとともに 10MByte/s の高速書込み性能を確認した。

このように本論文は、高速な書込み性能を有する多値フラッシュメモリの先導的な提案及び実チップによる検証を行ったものであり、その内容は高く評価できる。



OFDM Error Vector Magnitude Distortion Analysis

(英文論文誌 C 平成 18 年 12 月号掲載)



受賞者 山之内慎吾 受賞者 國弘和明 受賞者 樋田 光

OFDM (直交周波数分割多重) は良好なスペクトル効率とフェージング耐性を持つことから、無線 LAN、UWB (Ultra-Wide Band)、地上デジタル放送など、多くの無線通信方式に適用されている。その一方で、OFDM 用の無線送信機では EVM (Error Vector Magnitude ; 誤差ベクトル強度) で代表される変調精度特性に厳しい制約が課される。送信機の特性は最終段の電力増幅器の特性に大きく左右される。特に所望の変調精度を得るには電力増幅器の非線形性を抑制することが設計上の重要課題であり、集中的に研究が進められている。

OFDM 変調波入力時の電力増幅器の特性設計には、システムレベルシミュレーション及びハーモニクバランス (HB : Harmonic Balance) 法による回路シミュレーションが併用される。この方法では二つのシミュレーション法を併用するためツール費用や工程数などの設計コストが増大する。HB 法によるシミュレーション単独であれば設計コストが大幅に削減できるものの、HB 法は入力信号が離散スペクトルの場合のみ適用可能であり、OFDM 変調波のような連続スペクトルの場合は直接の取扱いが不可能であった。

本論文では、電力増幅器の非線形指標である振幅ひずみ (AM-AM) 特性及び位相ひずみ (AM-PM) 特性と EVM との関係式を解析的に導出した。AM-AM 及び AM-PM 特性は HB 法で計算できるので、導出した関係式を適用すれば、システムレベルシミュレーションによる変調波解析を介することなく、HB 法シミュレーション単独で EVM 特性の計算が可能になる。また、解析的に厳密な関係式を用いることで、提案手法は従来のシステムレベルシミュレーションと同等の精度を実現している。更に、この技法では変調波解析を介さないことで、EVM 特性の計算時間を従来のシステムシミュレーションの約 1/10 にまで短縮している。これらにより、電力増幅器の設計コストと開発効率は大きく改善される。

本論文は、非線形指標間関係式を解析的に導出した点で高い学術的な価値を持つとともに、電力増幅器設計の低コスト化と開発効率の向上を図るという実用面でも大きく貢献するものであり、その内容は高く評価される。

Light-Induced Self-Written Optical Waveguides

(英文論文誌 C 平成 19 年 5 月号掲載)



受賞者 各務 学



受賞者 山下達弥



受賞者 米村正寿



受賞者 松井崇行

インターネットやネットワーク制御の急速な高速化に伴い、民生や移動体等の比較的低コストシステムへも光通信の普及が始まっている。これらの巨大な応用分野では小形集積、省配線、超低コストといった特徴的な要件が強い。

本論文は、各種光部品間の光インタコネクションを光導波路作製と同時に行うユニークなプロセスの提案と、光通信モジュールへの応用に関しまとめられている。骨子となる技術は光硬化性樹脂中に放射された光の自己集束効果を利用した光導波路の自己形成であり、著者らにより初めて均一直径光導波路の実現と、三次元構造光回路の一括形成技術が示された。本技術はコア直径が $9\mu\text{m}$ の単一モード光ファイバから 1mm の大口徑プラスチック光ファイバまで対応が可能である。また、自己形成光導波路は無調心実装が可能で、更に、光導波路のダイシングや研磨プロセスが不要となる初めての光回路形成法であり、実装コストの大幅な低減が期待できる。研究初期において、本技術の弱点とされた光導波路以外の実装誤差に起因する接続トレランスの低下、及び、クラッド部の固形化方法について本論文は異領域技術を持ち込み見事に解決している。前者に関しては、光物理における空間ソリトンの重ね合わせによる『光はんだ』効果を用いて各部品の軸ずれを補正しながら自己組織的に経路(光回路)構成を行うことを実証している。また、後者に関しては、高分子化学における材料的及び空間的選択重合により、モノマー混合液中で特定のモノマーのみ重合させ、三次元導波路構造を得ることを可能とした。これにより、単一モードのような極細三次元構造物においても光回路が形成できるようになった。

以上のように、本論文は複雑な光回路の量産と低コスト化に適した作製法を提案しており極めてはん用性が高

い。自動車分野以外にも、既に多くの研究機関において、アクセス系ネットワーク、民生分野の機器、計算機や光電子混載ボードなどの光配線といった適用研究が始まっており、今後の他分野への波及も楽しみである。光通信技術のすそ野を広げる提案型研究として高く評価される。



マルコフ連鎖モデルに基づく移動ヒストグラムの動的構築法

(和文論文誌 D 平成 19 年 2 月号掲載)



受賞者 石川佳治



受賞者 町田陽二



受賞者 北川博之

近年の無線ネットワーク技術や GPS などの位置測定技術の普及により自動車などの移動オブジェクトの追跡が容易になってきている。多数の移動オブジェクトの移動状況データを集積しリアルタイムに集約することにより、移動状況の分析や予測を行うことが可能となり、的確な交通情報の発信や交通制御等、今後社会に有益なサービスを提供する基盤となることが期待される。

本論文では、大量の移動オブジェクトをリアルタイムに集約する移動ヒストグラムの構築手法を提案している。ここでは、移動パターンを表現するためのモデルとしてマルコフ連鎖モデルを採用している。また、移動ヒストグラムの論理表現としてデータキューブを採用し、分析処理にかかわる操作をデータキューブの概念を用いて分かりやすい形で可能としている。一方、データキューブの物理的な実現方法として木構造を採用し、記憶容量の削減を図っている。また、適応的に木構造の伸張を行う近似的な手法を採用することにより、リアルタイムの分析処理のためにストリーミング的に配信される移動状況を継続的に集約する移動ヒストグラムの動的構築を実現している。更に、実際の都市における道路ネットワーク上での多数の移動オブジェクトの移動をシミュレートするデータを用いた実験により、移動ヒストグラムのサイズ、構築時間、問合せ処理時間、移動ヒストグラムの精度について評価を行い、提案手法の特性を明らかにするとともに有効性を示している。

このように、本論文は、大量の移動オブジェクトの移動軌跡データをコンパクトに要約するための移動ヒストグラムの構築手法として論理表現と物理表現を分離した実現方法を提案している。高水準の論理表現により利用者に分かりやすく機能を提供しつつ、物理表現をリアルタイムの集約にも耐え得るように効率的に実現し、また、その有効性を十分に示している。独創性に優れ、記述も親切かつ丁寧であり、高く評価できる。



隠れマルコフモデルデータベースの 高速ゆう度検索

(和文論文誌 D 平成 19 年 2 月号掲載)



受賞者 藤原靖宏



受賞者 櫻井保志



受賞者 山室雅司

隠れマルコフモデル (Hidden Markov Model, 以下 HMM) は確率密度関数に基づく状態遷移によりデータ系列を表現するデータモデルであり、音声認識、自然言語処理、遺伝子解析など多くの分野で用いられている。本論文で扱う問題は、与えられた離散型 HMM 集合から、あるデータ系列 (問合せシーケンス) に対してゆう度の高い順に K 個のモデルを出力するというものである。この問題にはビタビアルゴリズムによるナイーブな手法 (以下, Naive Viterbi) が存在する。しかし, HMM モデルの状態数や探索対象の HMM モデル数が多い場合には, Naive Viterbi ではばく大な計算コストが必要となってしまう。

この問題に対し, 著者らは SCREW という手法を提案している。SCREW は Naive Viterbi に比べて計算コストが極めて小さい。また, 探索漏れのないことが理論的に保証されている。SCREW の特徴は 3 点ある。まず, ビタビアルゴリズムの計算に用いられるデータ構造であるトレリス構造の縮退による計算量削減である。縮退後の近似ゆう度が厳密なゆう度より小さくならないように工夫されており, 縮退後のトレリス構造でも探索漏れのないことが保証されている。次に, 探索処理が進むに従って徐々にトレリス構造の縮退を緩め, ゆう度の近似精度を上げていく点である。すなわち, ゆう度の大きなモデ

ルについてのみ近似精度を上げてゆう度の再計算を行う。最後に, 厳密なゆう度計算を行う際に状態遷移の枝刈りを効率的に行う点である。

著者らは, 実際のビデオデータによるシーンのクラスタリングについて SCREW の性能評価実験を行っている。その結果, Naive Viterbi に比べてエルゴディック HMM で約 985 倍, left-right HMM で約 127 倍の性能向上が見られたと報告している。

離散型 HMM のモデル探索において, 高速性と解の厳密性を両立した研究は他に類がない。また本論文の成果は特定の分野に限定されておらず, 広範囲への応用が期待できる。なお本論文は, 本会データ工学研究専門委員会主催による第 17 回データ工学ワークショップ (DEWS 2006) にて優秀論文賞を受賞した研究を基にしたものであり, 同委員会の推薦論文であることを付記する。



人間の視覚特性を考慮した投影画像の 光学的補正

(和文論文誌 D 平成 19 年 8 月号掲載)



受賞者
マーク アッシュダウン



受賞者 佐藤いまり



受賞者 岡部孝弘



受賞者 佐藤洋一

PC の画面などを投影するプロジェクタは, 小形化, 低価格化, 高輝度化が進み広く使われるようになっていく。利用が進むにつれ, 照明を暗くした部屋に設置した専用のスクリーンのような場所ではなく, 明るいオフィスや居間の壁などに投影して使われることも多くなっていく。このような理想的とはいえない場所への投影を実現する技術に注目が集まっている。従来の技術は, 投影

された画像をカメラで撮影し、プロジェクタへの入力画像と比較してずれがないように入力画像を補正する方法が主流であった。この方法では、投影面の一部の反射率が大きく異なる場合や環境光の影響が大きい場合には補正に必要な輝度や色がプロジェクタの出力可能範囲を超えてしまい、補正の誤差が大きくなるばかりか、誤差のパターンが見えてしまう問題も抱えていた。

本論文で著者らは、不均一な反射率の投影面や環境光の影響だけでなく、入力される画像の内容も考慮して良好な投影画像が得られるような補正手法を提案している。提案手法は、反射率が低い部分への入力画像の明るさが元々低ければ補正の誤差は小さくなる、といった判断により入力画像全体の明るさを制限せずにコントラストを十分に持った画像を投影することを可能にする。更

に、人間の視覚特性に基づいた補正により観察者に違和感を与えない範囲でずれを認めることで更に高いコントラストでの投影を実現している。提案手法を実装したシステムによりユーザ評価を行うことで有効性を明確にしている。

本論文の技術は、実際にプロジェクタを利用するオフィス環境などを想定した提案であり、実システムとしても十分運用可能であり、社会的な貢献度が高い。また、従来法にはない人間の視覚特性も考慮した補正法を提案しており、独創性にも優れており高く評価できる。なお、本論文は本会パターン認識・メディア理解 (PRMU) 研究専門委員会主催による画像の認識・理解シンポジウム (MIRU 2006) において、優秀論文賞を受賞した研究を基にしたものであることを付記しておく。

