様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　５ 年　 ６ 月 １６ 日現在

機関番号：１５３０１
研究種目：挑戦的研究（萌芽）
研究期間：2019～2022
課題番号：１９Ｋ２２８４６

研究課題名（和文）フェイクコンテンツ分類のためのフォレンジクス技術開発

研究課題名（英文）Multimedia Forensics for Classification of Fake Content

研究代表者
栗林　稔（Kuribayashi, Minoru）

岡山大学・自然科学学域・准教授

研究者番号：５０３４６２３５

交付決定額（研究期間全体）：（直接経費）　　4,900,000円

研究成果の概要（和文）：ある人物の顔領域を他の人物の顔との置き換えや表情を変更させて作成されるフェイクコンテンツと，敵対的生成ネットワークによって人工的に創作された画像や動画などを対象として，基本的な画像識別器の設計と評価を行った．学習時とテスト時で異なる手法で作成されたコンテンツにおいても高い識別精度を得られるように，領域単位での処理や色空間を変える手法への拡張法も提案した．また，画像識別器を誤認識させるために生成される敵対的ノイズの有無を判別する手法の開発を行った．元の画像識別器は変更せずに，前処理フィルタを設計し，90%を超える高い精度で識別できることを実験により確認できた．

研究成果の学術的意義や社会的意義
深層学習技術を用いれば，偽物とは簡単に判別できない画像や映像を生成することが可能となっており，悪用されることが懸念されている．特に，特定の人物を操った形でのコンテンツが精巧に作成され，社会的な影響を与えるような印象操作に使われる可能性も高まっている．本研究で開発した識別器は，そのような人工的に作成および加工編集されたコンテンツを機械的に判別するものであり，マルチメディアコンテンツに関連したセキュリティ技術として重要な役割を担うものと考えられる．本識別器を拡張させて更に精度を高める研究が広がることで，フェイク情報の流布を抑制できることが期待される．

研究成果の概要（英文）：We designed and evaluated a basic image classifier for fake content created by replacing a person's face with another person's face or changing facial expressions, as well as for images and videos artificially created by an adversarial generative network. We also proposed extensions to the region-based processing and color space correction methods to achieve high classification accuracy for content created with different methods during training and testing. In addition, we developed a method to identify the presence or absence of adversarial noise generated to misidentify the image classifier. We designed a preprocessing filter that does not modify the original image classifier and confirmed through experiments that it can detect adversarial images with a high accuracy of over 90%.

研究分野：マルチメディアセキュリティ

キーワード：フェイクコンテンツ　生成AI　画像識別器　敵対的サンプル

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

アナログの時代より，合成写真に代表される偽の情報によって，プロパガンダなどの情報操作が問題として挙がっている．従来の合成写真の場合，高度に経験を積んだ専門家が光や影の位置，不自然な境目の存在などを目視によりチェックして，確認を行っていた．一方，ディジタル化されたマルチメディアコンテンツにおいては，ディジタル信号処理技術により合成写真や合成音声，合成映像などの作成が可能である．更には深層学習を使った機械学習技術の発達により，実際に録音・録画されたコンテンツと遜色のない程度にまで人工的にコンテンツを創造することが可能になりつつある．悪意のある者が，これらの技術を利用してフェイクコンテンツを作成し，インターネットを介して発信した場合，多大なる影響が及ぼされる可能性がある．例えば，社会的に影響力のある人物のフェイク発言である場合，プロパガンダによる甚大な被害が広がる．この問題に対応すべく，合成技術とは反対の方向として「人工的に創造されたコンテンツ」と「正常に撮影されたコンテンツ」を判定する技術が必要である．

インターネット上でのストリーミング放送を始め，各種動画配信サイトにより，新聞やTVニュースのような既存メディアとは異なる第三のメディアが社会的な影響を与えつつある．ジャーナリズムの観点からは，既存メディアによるプロパガンダや世論誘導を監視する役割りを果たす一方，発信内容を検証することの困難性から危険性も伴っている．文字情報の場合，内容の客観的な検証が必要である認識は高いが，音声や映像では視聴覚に訴える内容であり，視聴者は真実として直ちに受け入れてしまう恐れがある．

国内の研究動向としては，音声及び音響に関係する研究は主に音声合成技術により自然な音声・音楽信号を創造するテーマに傾いている．一方，この技術が悪用される危険性については，あまり深く研究が進んでいない．信号処理技術を用いた合成や改ざんの解析については，ディジタルフォレンジクス技術において研究が進んでいるが，対応するアンチフォレンジクス技術も同時に研究が進められており，合成や改ざんの形跡を削除されることも考慮しなければならない．

２．研究の目的

本研究では，音声・映像データの真偽判定技術により，誤った情報による大衆誘導の危険を防ぐことを目指す．正常に録画・録音されたコンテンツが加工・編集されると，元の信号からは変形されて，通常は存在する信号が削除される，もしくは存在しない信号が付加される可能性があることから，この僅かな変化を読み取って音声・映像データの真偽判定を行う．本研究では，研究者代表者がメインとして扱ってきたディジタル画像におけるフェイクコンテンツを主に扱うことにする．ただし，得られた成果を基に他のマルチメディアコンテンツにおいても適用できるように拡張させることも想定する．

最近ではサポートベクトルマシン(SVM)や畳み込みニューラルネットワーク(CNN)に関連する研究が国内外で盛んに研究されている． Pythonのコードが公開されていることもあり，多方面に渡る研究分野においてその適用範囲も多岐に渡りつつある．本研究で扱うマルチメディアコンテンツのフォレンジクス技術においては，国外では活発に研究が進みつつあるが，国内では関係する研究者，特に若手研究者が少ない．そのため，本研究を通じて国内でのフォレンジクス技術を活性化させることも本研究の目的の一つである．

３．研究の方法

最初は，現在主流となっている教師付き学習を用いたマルチメディアコンテンツにおける，人工的に想像された画像と通常の撮影された画像を分類する技術についてサーベイを行う．また，機械学習として利用可能なライブラリの利用方法を調べ，技術的に可能な処理と困難な処理について確認する．セキュリティ技術に特化した安全性の解析と，数値解析技術を用いて分類結果の信頼度を理論的に導出する．

次に敵対的ネットワークであるGAN(Generative Adversarial Network)を構築して，半教師データから開始した相互学習を通したシステムの構築を行う．学生にプログラミング技術の指導をしつつ，構築したシステムを使ったシミュレーションを行う．また学生には画像データの収集を担当し，教師データおよびテストデータとして利用するための画像データベースの構築を行ってもらう予定である．申請者はGANのモデリングを行い，画像データから特徴成分を抽出するための最適化を行う．得られたデータを用いて，人工的に想像された画像と正常に撮影された画

像の分類するためのシステムのプロトタイプを作成する．

さらに精度を高められるように特徴成分の抽出操作を再考する．シミュレーション環境への反映は，学生に作業してもらう．また，想定されるフェイクコンテンツの生成過程に応じて，提案システムを動作させて，共通する特徴成分の割り出しを行いつつ，それぞれの生成過程で作成されたコンテンツにおいて高い分類精度を得られる分類システムを構築する．

識別を回避するような対策として敵対的攻撃の問題について調べ，その対策を講じるための研究も並行して行う．意図的に誤識別を誘発するようにノイズがフェイクコンテンツに加えれた場合には，識別器が正常に判定できなくなる恐れがある．そのような敵対的攻撃に耐性を持つように識別器を学習させる方法と，識別器に入力する前に敵対的ノイズの含蓄の有無を判定する前処理フィルタの設計を検討し，その性能を評価する．

４．研究成果

フェイクコンテンツとして，ある人物の顔領域を他の人物の顔との置き換えや，表情を変更させて作成されるディープフェイク動画と，敵対的生成ネットワークによって人工的に創作された画像や動画を対象に，画像識別器の設計と評価を行った．また，画像識別器を誤認識させるために生成される敵対的ノイズの有無を判別する手法の開発を行った．

正常に撮影，録画されたコンテンツとこれらのフェイクコンテンツを識別するためにコンテンツ中に含まれる不自然な信号を解析する研究動向を広く調べ，生成方法から識別方法，現状での課題などをサーベイ論文としてまとめた．フェイクコンテンツの生成を，Entire Face Synthesis，Identity Swap，Attribute Manipulation，Expression Swap の４つの手法に分類し，その内，Entire Face Synthesis と Identity Swap を対象として，本研究では識別器の提案と評価を行った．

完全にゼロから画像を作成する Face Synthesis においては，敵対的生成ネットワークによって設計された画像生成器である StyleGAN を対象として，生成された画像を領域単位で分割して不自然な信号を解析するアプローチにて識別器を設計した．画像生成器の学習過程において用いたデータセットに近いデータセットでその識別器をテストすれば，99%を超える精度で識別可能であるが，異なるデータセットを用いた場合には，その精度が大きく下がる傾向が見られた．画像を RGB 表示系から HSV 表示系に変換することで，テスト時の精度の低下を抑えることを明らかにすることができた．

ある人の顔を他の人の顔に置き換えて，その表情の変化なども視覚的に不自然とならないように精巧に作成される DeepFake 動画を対象にその識別器の設計を行った．動画からフレーム単位で静止画を抜き出し，顔領域のみを検出対象として解析する画像識別器を提案し，その評価を行った．画像識別器は，ImageNet の画像データセットで学習済みの画像識別器モデルをファインチューニングさせて，フェイクと正常で二値判別できる識別モデルを設計し，Deep Fake Detection Challenge データセットを用いて，学習させた．他のフェイク動画においても識別精度を高められるように汎用性を考慮した上で，モデルを修正しながら識別器を構築し，数量的にその性能を評価した．未知のフェイク動画に対しては，フレーム単位での識別精度は多少下がるが，動画のフレーム数が増えるに従って識別精度を高められることが確認された．

フェイクコンテンツの識別において，学習に用いるデータセットが極めて重要であり，複数の異なる方法で生成された画像や動画をできるだけ偏りなく収集しておくことが必要となる．もし，特定の生成方法に偏ったコンテンツを含むデータセットで学習させた場合，異なる方法で生成されたコンテンツに対しては，その識別精度が大幅に低下することも確認された．汎用的な識別器の設計，および学習のさせ方は難しい課題として残されており，関連研究においても，この問題への対策が検討されつつあることも分かった．将来的には，既存の生成方法の拡張や全く新しい生成方法を用いてフェイクコンテンツが作成されることも考慮して汎用的な識別器を設計する必要があり，その対策は今後の課題として残されている．

深層学習技術を用いた識別器において，意図的に誤検出を誘導するようにノイズを生成する敵対的攻撃の脅威が問題となっており，フェイクコンテンツの識別においても同様に問題として従来研究にて警鐘が鳴らされていることを発見した．そこで，本研究で対象としている識別器において，入力される画像や動画に前処理フィルタを施すことで，前もって問題となる敵対的サンプルを検出するための手法の研究も手掛けた．意図的に誤ったラベルに識別されるように生成された微小なノイズにより敵対的サンプル画像が作成されることから，そのノイズの影響を抑えることができれば，元の正しいラベルに戻すことができる．本研究では，ノイズ除去フィルタの強度を徐々に上げることで生じる上位出力ラベルの変化，およびそれらの確信度の値の変化量に着目し，特徴成分として取り出した上でニューラルネットワークによる二値分類器を構

築した.

入力画像にノイズ除去操作を行うと，CNN ベースの画像分類器から出力される確信度ベクトルが変化する．敵対的サンプルの場合，最上位のクラスラベルの確信度は大幅に低下する．適用された敵対的攻撃によって，いくつかのトップクラスラベルの確信度の変化量は異なる．特に，敵対的攻撃を受けた画像の場合は，通常の画像とは全く異なる変化をする．提案手法では，対象画像が CNN ベースの画像分類器に入力され，softmax 関数の出力である Top-α ($\alpha \geq 1$) クラスラベルとその確信度に対して，フィルタリング操作後の値の推移を観察して，敵対的サンプルを分類する．複数のフィルタ処理において支配的な役割りを果たすものを選別し，更にいくつか組み合わせることで，特徴成分を取り出す処理を軽量化しつつ，高い識別精度を保つことができるような手法を構築した．その結果，特定の結果に誘導する Target 攻撃においては 98%を超える精度で，正解の結果とは異なる他の結果に誘導する Non-Target 攻撃においても，92%を超える精度で敵対的サンプルを検出することに成功した.

また，敵対的サンプルの識別だけでなく，元の画像と同じラベルに識別されるような無毒化処理についても研究を進めている．提案のフィルタ処理を拡張させて，元の画像のラベルを高精度に推定し，そのラベルに戻す無毒化処理において，画像に与える視覚的な劣化を抑えることを現在検討中である．今後，敵対的サンプルの識別精度や計算量的な観点だけでなく，無毒化処理の性能においてこの視覚的な劣化の観点も重要な課題である.

５．主な発表論文等

〔雑誌論文〕　計10件（うち査読付論文　10件／うち国際共著　7件／うちオープンアクセス　5件）

１．著者名 Minoru Kuribayashi, KokSheik Wong	４．巻 61
２．論文標題 StealthPDF: Data hiding method for PDF file with no visual degradation	５．発行年 2021年
３．雑誌名 Journal of Information Security and Applications	６．最初と最後の頁 10
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.jisa.2021.102875	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Huy H. Nguyen, Minoru Kuribayashi, Junichi Yamagishi, Isao Echizen	４．巻 E105-D
２．論文標題 Effects of image processing operations on adversarial noise and their use in detecting and correcting adversarial images	５．発行年 2022年
３．雑誌名 IEICE Transactions on Information and Systems	６．最初と最後の頁 65-77
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2021MUP0005	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Asad Malik, Minoru Kuribayashi, Sani M. Abdullahi, Ahmad Neyaz Khan	４．巻 10
２．論文標題 DeepFake Detection for Human Face Images and Videos: A Survey	５．発行年 2022年
３．雑誌名 IEEE Access	６．最初と最後の頁 18757-18775
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2022.315118	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 David Megias, Minoru Kuribayashi, A Rosales, K. Cabaj, W. Mazurczyk	４．巻 13
２．論文標題 Architecture of a fake news detection system combining digital watermarking, signal processing, and machine learning	５．発行年 2022年
３．雑誌名 Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications	６．最初と最後の頁 33-55
掲載論文のDOI（デジタルオブジェクト識別子） 10.22667/JOWUA.2022.03.31.033	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Tatsuya Yasui, Minoru Kuribayashi, Nobuo Funabiki, Isao Echizen	4．巻 15
2．論文標題 Near-Optimal Detection for Binary Tardos Code by Estimating Collusion Strategy	5．発行年 2020年
3．雑誌名 IEEE Transactions on Information Forensics and Security	6．最初と最後の頁 2069-2080
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIFS.2019.2956587	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 David Megias, Minoru Kuribayashi, Amna Qureshi	4．巻 9
2．論文標題 Survey on Decentralized Fingerprinting Solutions: Copyright Protection through Piracy Tracing	5．発行年 2020年
3．雑誌名 Computers	6．最初と最後の頁 26
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/computers9020026	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Minoru Kuribayashi and KokSheik Wong	4．巻 12022
2．論文標題 Improved DM-QIM Watermarking Scheme for PDF Document	5．発行年 2020年
3．雑誌名 Digital Forensics and Watermarking	6．最初と最後の頁 171-183
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-43575-2_14	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Minoru Kuribayashi, Tatsuya Yasui, Asad Malik	4．巻 9
2．論文標題 White Box Watermarking for Convolution Layers in Fine-Tuning Model Using the Constant Weight Code	5．発行年 2023年
3．雑誌名 Journal of Imaging	6．最初と最後の頁 117
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/jimaging9060117	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Tatsuya Yasui, Takuro Tanaka, Asad Malik, Minoru Kuribayashi	4．巻 8
2．論文標題 Coded DNN Watermark: Robustness against Pruning Models Using Constant Weight Code	5．発行年 2022年
3．雑誌名 Journal of Imaging	6．最初と最後の頁 152
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/jimaging8060152	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Minoru Kuribayashi, Kodai Kamakari, Nobuo Funabiki	4．巻 13480
2．論文標題 Classification of Screenshot Image Captured in Online Meeting System	5．発行年 2022年
3．雑誌名 Lecture Notes in Computer Science	6．最初と最後の頁 244-255
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-14463-9_16	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計49件（うち招待講演　5件／うち国際学会　22件）

1．発表者名 A. Qureshi, D. Megias, M. Kuribayashi
2．発表標題 Detecting deepfake videos using digital watermarking
3．学会等名 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC 2021)（国際学会）
4．発表年 2021年

1．発表者名 D. Takeshita, M. Kuribayashi, N. Funabiki
2．発表標題 A study of feature extraction suitable for double JPEG compression analysis based on statistical bias observation of DCT coefficients
3．学会等名 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC 2021)（国際学会）
4．発表年 2021年

１．発表者名
Y. Yamasaki, M. Kuribayashi, N. Funabiki, H. H. Nguyen, I. Echizen

２．発表標題
A study of feature extraction based on denoising auto encoder for classification of adversarial examples

３．学会等名
Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC 2021) (国際学会)

４．発表年
2021年

１．発表者名
K. Nakai, M. Kuribayashi, N. Funabiki

２．発表標題
A study of privacy protection of photos taken by wide-angle surveillance camera

３．学会等名
Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC 2021) (国際学会)

４．発表年
2021年

１．発表者名
D. Megias, M. Kuribayashi, A. Rosales, and W. Mazurczyk

２．発表標題
DISSIMILAR: Towards fake news detection using information hiding, signal processing and machine learning

３．学会等名
The 16th Int. Conf. Availability, Reliability and Security (ARES2021) (国際学会)

４．発表年
2021年

１．発表者名
M. Kuribayashi, T. Tanaka, S. Suzuki, T. Yasui, and N. Funabiki

２．発表標題
White-box watermarking scheme for fully-connected layers in fine-tuning model

３．学会等名
9th ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec'21) (国際学会)

４．発表年
2021年

１．発表者名
角森健太，山﨑裕真，栗林稔，舩曳信生，越前功

２．発表標題
JPEG圧縮由来の歪み信号に対する応答特性に基づくAdversarial Examples検知手法

３．学会等名
2022年暗号と情報セキュリティシンポジウム（SCIS2022）

４．発表年
2022年

１．発表者名
鎌苅康大，栗林稔，舩曳信生

２．発表標題
オンライン会議システム上の画面キャプチャによる情報漏洩の対策の一検討

３．学会等名
2022年暗号と情報セキュリティシンポジウム（SCIS2022）

４．発表年
2022年

１．発表者名
田中拓朗，安井達哉，栗林稔，舩曳信生

２．発表標題
埋め込みロス関数なしのDNN電子透かしの収束に関する考察

３．学会等名
信学技報，EMM 11月

４．発表年
2021年

１．発表者名
山﨑裕真，栗林稔，舩曳信生，グエン フイ ホン，越前功

２．発表標題
複数のAuto Encoderに対する応答特性を用いた敵対的事例の検出法

３．学会等名
信学技報，EMM 5月

４．発表年
2021年

１．発表者名
竹下大地，栗林稔，舩曳信生

２．発表標題
DCT係数の統計的な偏り観測における二重JPEG圧縮履歴解析に適した特徴成分選出に関する考察

３．学会等名
信学技報，EMM 5月

４．発表年
2021年

１．発表者名
M. Kuribayashi, T. Tanaka, Nobuo Funabiki

２．発表標題
DeepWatermark: embedding watermark into DNN model

３．学会等名
Asia-Pacific Signal and Information Processing Association Anual Sumit and Conf. (APSIPA ASC 2020)（国際学会）

４．発表年
2020年

１．発表者名
M. Kuribayashi, K. Kamakari, K. Kawata, N. Funabiki

２．発表標題
Classification of video recaptured from display device

３．学会等名
Asia-Pacific Signal and Information Processing Association Anual Sumit and Conf. (APSIPA ASC 2020)（国際学会）

４．発表年
2020年

１．発表者名
A. Higashi, M. Kuribayashi, N. Funabiki, H. Nguyen, I. Echizen

２．発表標題
Detection of adversarial examples based on sensitivities to noise removal filter

３．学会等名
Asia-Pacific Signal and Information Processing Association Anual Sumit and Conf. (APSIPA ASC 2020)（国際学会）

４．発表年
2020年

１．発表者名
Minoru Kuribayashi

２．発表標題
Adversarial Examples of Deep Learning System and Its Defense

３．学会等名
IEEE Computational Intelligence Society Chapter（招待講演）（国際学会）

４．発表年
2021年

１．発表者名
中井康貴，栗林稔，舩曳信生，藤井爽平，石原洋之

２．発表標題
監視カメラにおける映り込み領域に対する顔検出とプライバシ保護に関する考察

３．学会等名
信学技報，EMM 3月

４．発表年
2021年

１．発表者名
東亮憲，栗林稔，舩曳信生，Huy Hong Nguyen，越前功

２．発表標題
複数のフィルタ強度によるCNN画像分類器の応答特性を用いた敵対的事例の検出法

３．学会等名
信学技報，EMM 3月

４．発表年
2021年

１．発表者名
河田健斗，栗林稔，舩曳信生

２．発表標題
顔領域に注目してファインチューニングした事前学習済みCNNモデルに基づくディープフェイク動画検出法

３．学会等名
2021年暗号と情報セキュリティシンポジウム（SCIS2021）

４．発表年
2021年

１．発表者名
中嶋直也，栗林稔，舩曳信生

２．発表標題
ブロックサイズの違いがDCT係数の頻度分布を利用したJPEG画像圧縮履歴解析に与える影響

３．学会等名
信学技報，EMM 11月

４．発表年
2020年

１．発表者名
田中拓朗，栗林稔，舩曳信生

２．発表標題
DM-QIMによるDNNモデルの全結合層に対する電子透かし法

３．学会等名
信学技報，EMM 9月

４．発表年
2020年

１．発表者名
Minoru Kuribayashi and KokSheik Wong

２．発表標題
Improved DM-QIM Watermarking Scheme for PDF Document

３．学会等名
International Workshop on Digital-forensics and Watermarking (IWDW2019)（国際学会）

４．発表年
2019年

１．発表者名
田中拓朗，安井達哉，栗林稔，舩曳信生

２．発表標題
DM‐QIMによるディープニューラルネットワークの重みに対する電子透かし法

３．学会等名
信学技報，EMM 11月

４．発表年
2020年

１．発表者名
小浦啓太郎，栗林稔，舩曳信生

２．発表標題
DCT係数のヒストグラムを利用したJPEG画像のCNNに基づく編集履歴解析

３．学会等名
信学技報，EMM 3月

４．発表年
2020年

１．発表者名
鎌苅康大，河田健斗，栗林稔，舩曳信生

２．発表標題
ビデオカメラを用いたディスプレイ再撮により作成された違法動画の検出法

３．学会等名
信学技報，EMM 3月

４．発表年
2020年

１．発表者名
東亮憲，栗林稔，舩曳信生，Huy Hong Nguyen，越前功

２．発表標題
非可逆圧縮の圧縮率の変化に伴う挙動解析に基づく敵対的事例の検知法

３．学会等名
信学技報，EMM 3月

４．発表年
2020年

１．発表者名
小浦啓太郎，栗林稔，舩曳信生

２．発表標題
DCT係数のヒストグラムの偏りを利用したJPEG画像の編集履歴解析

３．学会等名
コンピュータセキュリティシンポジウム（CSS2019）

４．発表年
2019年

１．発表者名
東亮憲，栗林稔，舩曳信生，Nguyen Huy H.，越前功

２．発表標題
JPEG圧縮による画像分類器の識別結果の変動解析に基づく敵対的事例の検知法

３．学会等名
コンピュータセキュリティシンポジウム（CSS2019）

４．発表年
2019年

１．発表者名
安井達哉，栗林稔，舩曳信生

２．発表標題
電子指紋符号の結託攻撃パラメータ推定のための特徴ベクトル導出及びその次元削減

３．学会等名
コンピュータセキュリティシンポジウム（CSS2019）

４．発表年
2019年

１．発表者名
A. H. Zim, A. Ashraf, A. Iqbal, A. Malik, M. Kuribayashi

２．発表標題
A Vision Transformer-Based Approach to Bearing Fault Classification via Vibration Signals

３．学会等名
Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC 2022)（国際学会）

４．発表年
2022年

１．発表者名
A. Malik, A. Ashraf, H. Wu, M. Kuribayashi

２．発表標題
Reversible Data Hiding in Encrypted Text Using Paillier Cryptosystem

３．学会等名
Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC 2022)（国際学会）

４．発表年
2022年

１．発表者名
K. Tsunomori, Y. Yamasaki, M. Kuribayashi, N. Funabiki, I. Echizen

２．発表標題
Detection and Correction of Adversarial Examples Based on JPEG-Compression-Derived Distortion

３．学会等名
Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC 2022) (国際学会)

４．発表年
2022年

１．発表者名
M. S. Raval, M. Roy, M. Kuribayashi

２．発表標題
Survey on Vision Based Fake News Detection and Its Impact Analysis

３．学会等名
Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC 2022) (国際学会)

４．発表年
2022年

１．発表者名
P. Raval, H. Khakhi, M. Kuribayashi, M. S. Raval

２．発表標題
Defense Against Adversarial Examples Using Beneficial Noise

３．学会等名
Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC 2022) (国際学会)

４．発表年
2022年

１．発表者名
H. Takiwaki, M. Kuribayashi, N. Funabiki, M. S. Raval

２．発表標題
Privacy Protection Against Automated Tracking System Using Adversarial Patch

３．学会等名
Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC 2022) (国際学会)

４．発表年
2022年

１．発表者名
M. Kuribayashi, K. Kamakari, N. Funabiki

２．発表標題
Classification of Screenshot Image Captured in Online Meeting System

３．学会等名
International IFIP Cross Domain Conference for Machine Learning & Knowledge Extraction (CD-MAKE2022)（国際学会）

４．発表年
2022年

１．発表者名
R. Parmar, M. Kuribayashi, H. Takiwaki, M. S Raval

２．発表標題
On Fooling Facial Recognition Systems using Adversarial Patches

３．学会等名
The 2022 International Joint Conference on Neural Networks (IJCNN 2022)（国際学会）

４．発表年
2022年

１．発表者名
瀬尾亮太，田中千奈月，栗林稔，舩曳信生

２．発表標題
プライバシ保護に向けたOpenPose骨格推定を用いた人の頭部位置検出

３．学会等名
信学技報，EMM 3月

４．発表年
2023年

１．発表者名
田中千奈月，栗林稔，舩曳信生

２．発表標題
OpenPoseで検出した特徴点における動作特性に注目した歩容認証

３．学会等名
信学技報，EMM 3月

４．発表年
2023年

１．発表者名
赤井怜音，栗林稔，舩曳信生

２．発表標題
Federated Learningにおいて悪意のある分散ノードを除外するための一検討

３．学会等名
信学技報，EMM 3月

４．発表年
2023年

１．発表者名
浦晃暢，栗林稔，舩曳信生

２．発表標題
敵対的生成ネットワークによって生成されたシンセティックメディア識別のための画像処理解析の検討

３．学会等名
2023年暗号と情報セキュリティシンポジウム（SCIS2023）

４．発表年
2022年

１．発表者名
笠井健太郎，栗林稔，舩曳信生，越前功

２．発表標題
ブロックチェーン技術によるコンテンツの加工編集履歴を管理するコンテンツクレデンシャル機能の一考案

３．学会等名
2023年暗号と情報セキュリティシンポジウム（SCIS2023）

４．発表年
2022年

１．発表者名
安井達哉，Malik Asad，栗林稔

２．発表標題
重み一定符号を用いたDNN電子透かしの検出法

３．学会等名
2022年情報科学フォーラム(FIT2022)

４．発表年
2022年

１．発表者名
瀧脇大登，栗林稔，舩曳信生

２．発表標題
顔識別回避のためのパッチ型敵対的事例の生成及び堅牢性の検証

３．学会等名
信学技報，EMM 5月

４．発表年
2022年

１．発表者名
角森健太，山﨑裕真，栗林稔，舩曳信生，越前功

２．発表標題
敵対的ノイズとJPEG圧縮由来の歪みの相関を用いた敵対的事例検出の研究

３．学会等名
信学技報，EMM 5月

４．発表年
2022年

１．発表者名
Minoru Kuribayashi

２．発表標題
Multimedia Forensics for Fake Content Classification

３．学会等名
International Conference on Emerging Computational Intelligence (ICECI 2023)（招待講演）（国際学会）

４．発表年
2023年

１．発表者名
Mehul S. Raval, Mohendra Roy, Minoru Kuribayashi

２．発表標題
Fake News Detection and its impact analysis

３．学会等名
Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC 2022)（国際学会）

４．発表年
2022年

１．発表者名
栗林稔

２．発表標題
人工知能に関する問題その対策

３．学会等名
岡山地方裁判所（招待講演）

４．発表年
2022年

１．発表者名
栗林稔

２．発表標題
ディープフェイクを見破れ!

３．学会等名
兵庫県立豊岡高等学校 【STEAM講演会】（招待講演）

４．発表年
2021年

１．発表者名
Minoru Kuribayashi

２．発表標題
Adversarial Examples of Deep Learning System and Its Defense

３．学会等名
IEEE Computational Intelligence Society Chapter and Ahmedabad University（招待講演）（国際学会）

４．発表年
2021年

〔図書〕　計1件

１．著者名	４．発行年
D. Megias, W. Mazurczyk, M. Kuribayashi	2022年
２．出版社	５．総ページ数
MDPI	234
３．書名	
Data Hiding and Its Applications: Digital Watermarking and Steganography	

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関			
スペイン	カタルーニャ・オベルタ大学			
ポーランド	ワルシャワ工科大学			
マレーシア	モナーシュ大学マレーシア			
インド	アーメダバード大学			