(19)日本国特許庁(JP)

# (12)特許公報(B2)

(11)特許番号
特許第7309101号
(P7309101)

(45)発行日　令和5年7月14日(2023.7.14)

(24)登録日　令和5年7月6日(2023.7.6)

(51)国際特許分類
*Ｇ０６Ｎ　20/00　(2019.01)*

ＦＩ
Ｇ０６Ｎ　20/00

請求項の数　4　（全10頁）

(21)出願番号　特願2023-527359(P2023-527359)
(86)(22)出願日　令和3年6月16日(2021.6.16)
(86)国際出願番号　PCT/JP2021/022916
(87)国際公開番号　WO2022/264331
(87)国際公開日　令和4年12月22日(2022.12.22)
審査請求日　令和5年5月8日(2023.5.8)
早期審査対象出願

(73)特許権者　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　110002491
弁理士法人クロスボーダー特許事務所
(72)発明者　小関　義博
東京都千代田区丸の内二丁目７番３号
三菱電機株式会社内
審査官　福西　章人

最終頁に続く

(54)【発明の名称】　攻撃検知装置、敵対的サンプルパッチ検知システム、攻撃検知方法、及び、攻撃検知プログラム

(57)【特許請求の範囲】

【請求項１】

撮影時間範囲内の互いに異なる時刻に撮影範囲内の範囲を撮影した複数の画像データそれぞれを用いて計算された複数の認識スコアであって、前記複数の画像データそれぞれにおいて物体を検知した結果を示す複数の認識スコアを用いて生成された時系列データである時系列認識スコアに、敵対的サンプルパッチ攻撃が前記複数の画像データの少なくともいずれかに対して実施された場合において生じる異常パターンが含まれているか否かを検知する異常パターン検知部

を備える攻撃検知装置であって、

前記異常パターンは、前記時系列認識スコアが示す認識スコアの値が物体検知閾値未満異常検知閾値以上である時間が異常検知時間以上継続することを示すパターンである攻撃検知装置。

【請求項２】

請求項１に記載の攻撃検知装置と、

前記複数の画像データそれぞれを用いて前記複数の認識スコアを計算する物体検知部を備える物体検知装置と

を備える敵対的サンプルパッチ検知システム。

【請求項３】

コンピュータが、撮影時間範囲内の互いに異なる時刻に撮影範囲内の範囲を撮影した複数の画像データそれぞれを用いて計算された複数の認識スコアであって、前記複数の画像デ

ータそれぞれにおいて物体を検知した結果を示す複数の認識スコアを用いて生成された時系列データである時系列認識スコアに、敵対的サンプルパッチ攻撃が前記複数の画像データの少なくともいずれかに対して実施された場合において生じる異常パターンが含まれているか否かを検知する攻撃検知方法であって、
前記異常パターンは、前記時系列認識スコアが示す認識スコアの値が物体検知閾値未満異常検知閾値以上である時間が異常検知時間以上継続することを示すパターンである攻撃検知方法。
【請求項４】
撮影時間範囲内の互いに異なる時刻に撮影範囲内の範囲を撮影した複数の画像データそれぞれを用いて計算された複数の認識スコアであって、前記複数の画像データそれぞれにおいて物体を検知した結果を示す複数の認識スコアを用いて生成された時系列データである時系列認識スコアに、敵対的サンプルパッチ攻撃が前記複数の画像データの少なくともいずれかに対して実施された場合において生じる異常パターンが含まれているか否かを検知する異常パターン検知処理
をコンピュータである攻撃検知装置に実行させる攻撃検知プログラムであって、
前記異常パターンは、前記時系列認識スコアが示す認識スコアの値が物体検知閾値未満異常検知閾値以上である時間が異常検知時間以上継続することを示すパターンである攻撃検知プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、攻撃検知装置、敵対的サンプルパッチ検知システム、攻撃検知方法、及び、攻撃検知プログラムに関する。
【背景技術】
【０００２】
入力画像における各オブジェクトの位置をバウンディングボックスで示し、各オブジェクトの種類をラベルとして示す物体検知のタスクにおいて、ニューラルネットワークを用いた深層学習の手法が近年、非常に高い精度を達成している。非特許文献１は、電子的な摂動が加えられた画像を印刷した敵対的サンプルパッチを物理的に配置し、配置された敵対的サンプルパッチを撮影した画像を入力した際に物体検知による検知を逃れる敵対的サンプルパッチ攻撃の手法を開示している。
【先行技術文献】
【非特許文献】
【０００３】
【文献】Ｓ．Ｔｈｙｓ ｅｔ ａｌ．，“Ｆｏｏｌｉｎｇ ａｕｔｏｍａｔｅｄ ｓｕｒｖｅｉｌｌａｎｃｅ ｃａｍｅｒａｓ：ａｄｖｅｒｓａｒｉａｌ ｐａｔｃｈｅｓ ｔｏ ａｔｔａｃｋ ｐｅｒｓｏｎ ｄｅｔｅｃｔｉｏｎ”，ＣＶＰＲＷ（Ｃｏｎｆｅｒｅｎｃｅ ｏｎ Ｃｏｍｐｕｔｅｒ Ｖｉｓｉｏｎ ａｎｄ Ｐａｔｔｅｒｎ Ｒｅｃｏｇｎｉｔｉｏｎ Ｗｏｒｋｓｈｏｐｓ），ＩＥＥＥ（Ｉｎｓｔｉｔｕｔｅ ｏｆ Ｅｌｅｃｔｒｉｃａｌ ａｎｄ Ｅｌｅｃｔｒｏｎｉｃｓ Ｅｎｇｉｎｅｅｒｓ）／ＣＶＦ（Ｃｏｍｐｕｔｅｒ Ｖｉｓｉｏｎ Ｆｏｕｎｄａｔｉｏｎ），２０１９
【発明の概要】
【発明が解決しようとする課題】
【０００４】
既存技術によれば、敵対的サンプルパッチ攻撃が行われた場合に、当該攻撃を検知することが困難であるという課題がある。
【０００５】
本開示は、敵対的サンプルパッチ攻撃が行われた場合に、当該攻撃を検知することを目的とする。
【課題を解決するための手段】

【０００６】
本開示に係る攻撃検知装置は、
撮影時間範囲内の互いに異なる時刻に撮影範囲内の範囲を撮影した複数の画像データそれぞれを用いて計算された複数の認識スコアであって、前記複数の画像データそれぞれにおいて物体を検知した結果を示す複数の認識スコアを用いて生成された時系列データである時系列認識スコアに、敵対的サンプルパッチ攻撃が前記複数の画像データの少なくともいずれかに対して実施された場合において生じる異常パターンが含まれているか否かを検知する異常パターン検知部
を備える。
【発明の効果】
【０００７】
本開示に係る攻撃検知装置は、物体を検知した結果を示す認識スコアから成る時系列認識スコアに、敵対的サンプルパッチ攻撃が実施された場合において生じる異常パターンが含まれているか否かを検知する異常パターン検知部を備える。従って、本開示によれば、敵対的サンプルパッチ攻撃が行われた場合に、当該攻撃を検知することができる。
【図面の簡単な説明】
【０００８】
【図１】実施の形態１に係る敵対的サンプルパッチ検知システム１００のシステム構成例を示す図。
【図２】実施の形態１に係る物体検知装置１１０の機能構成例を示す図。
【図３】実施の形態１に係る攻撃検知装置１２０の機能構成例を示す図。
【図４】実施の形態１に係る物体検知装置１１０及び攻撃検知装置１２０の各々のハードウェア構成例を示す図。
【図５】実施の形態１に係る敵対的サンプルパッチ検知システム１００の動作を示すフローチャート。
【図６】実施の形態１の変形例に係る物体検知装置１１０及び攻撃検知装置１２０の各々のハードウェア構成例を示す図。
【発明を実施するための形態】
【０００９】
実施の形態の説明及び図面において、同じ要素及び対応する要素には同じ符号を付している。同じ符号が付された要素の説明は、適宜に省略又は簡略化する。図中の矢印はデータの流れ又は処理の流れを主に示している。また、「部」を、「回路」、「工程」、「手順」、「処理」又は「サーキットリー」に適宜読み替えてもよい。
【００１０】
実施の形態１．
以下、本実施の形態について、図面を参照しながら詳細に説明する。
【００１１】
＊＊＊構成の説明＊＊＊
図１は、本実施の形態に係る敵対的サンプルパッチ検知システム１００のシステム構成例を示している。敵対的サンプルパッチ検知システム１００は、物体検知装置１１０と攻撃検知装置１２０とを有する。物体検知装置１１０と攻撃検知装置１２０とは一体的に構成されてもよい。
物体検知装置１１０は、入力画像データｘを入力として受け取り、物体検知結果である認識スコアｙを出力する。
攻撃検知装置１２０は、認識スコアｙを入力として受け取り、敵対的サンプルパッチ攻撃の検知結果ｒとして、敵対的サンプルパッチ攻撃による認識スコアの異常パターンが検知された場合には敵対的サンプルパッチ攻撃を検知したことを示す結果、それ以外の場合には敵対的サンプルパッチ攻撃を検知していないことを示す結果を出力する。敵対的サンプルパッチ攻撃は、敵対的サンプル攻撃の一種であり、特にニューラルネットワーク等を用いた物体検知を逃れる攻撃である。異常パターンは、具体例として、認識スコアの値が

、一定時間継続して物体検知の閾値を多少下回る値であるパターンである。即ち、異常パターンは、時系列認識スコアが示す認識スコアの値が物体検知閾値未満異常検知閾値以上である時間が異常検知時間以上継続することを示すパターンである。現状の敵対的サンプルパッチを用いた攻撃では、認識スコアの値を、物体検知の閾値を下回るよう抑えることができるが、完全に０にすることはできない。そのため、この異常パターンは当該攻撃の検知において有効である。ただし、異常パターンはこのパターンのみに限定されない。

【００１２】

図２は、物体検知装置１１０の機能構成例を示している。物体検知装置１１０は、データ入力部１１１と物体検知器１１２とデータ出力部１１３とを有する。

データ入力部１１１は、物体検知の対象である入力画像データｘを受け取り、受け取った入力画像データｘを物体検知器１１２に入力する。

物体検知器１１２は、入力された入力画像データｘを用いて認識スコアｙを算出し、算出した認識スコアｙをデータ出力部１１３に出力する。物体検知器１１２は、具体例としてニューラルネットワークによって構築された物体検知器１１２である。ニューラルネットワークは、具体例として、ＹＯＬＯ（Ｙｏｕ　Ｏｎｌｙ　Ｌｏｏｋ　Ｏｎｃｅ）、ＳＳＤ（Ｓｉｎｇｌｅ　Ｓｈｏｔ　Ｍｕｌｔｉｂｏｘ　Ｄｅｔｅｃｔｏｒ）、又はＦａｓｔｅｒ　Ｒ－ＣＮＮ（Ｒｅｇｉｏｎ－ｂａｓｅｄ　Ｃｏｎｖｏｌｕｔｉｏｎａｌ　Ｎｅｕｒａｌ　Ｎｅｔｗｏｒｋｓ）等である。物体検知器１１２は、入力された画像に映る各オブジェクトに対応するバウンディングボックスの位置を表す座標と、各バウンディングボックス内のオブジェクトの種類及び確信度を示す確率を認識スコアとして出力する。物体検知器１１２は、複数の画像データそれぞれを用いて複数の認識スコアを計算する。物体検知器１１２は物体検知部とも呼ばれる。

データ出力部１１３は、物体検知器１１２が計算した認識スコアｙを出力する。

【００１３】

図３は、攻撃検知装置１２０の機能構成例を示している。攻撃検知装置１２０は、データ入力部１２１と認識スコア集積部１２２と異常パターン検知部１２３とデータ出力部１２４とを有する。

データ入力部１２１は、認識スコアｙを受け取り、受け取った認識スコアｙを認識スコア集積部１２２に入力する。

認識スコア集積部１２２は、入力された認識スコアｙを時系列認識スコアＹ’に追加することによって時系列認識スコアＹを生成し、生成した時系列認識スコアＹを異常パターン検知部１２３に入力する。時系列認識スコアＹは更新された時系列認識スコアＹ’に当たる。時系列認識スコアＹ’は、新たな認識スコアｙが入力されるまでに入力された認識スコアｙを集積して生成した時系列データである。認識スコア集積部１２２は、認識スコア集積部１２２に認識スコアｙが入力される度に時系列認識スコアＹを異常パターン検知部１２３に入力しなくてもよく、一定時間毎に異常パターン検知部１２３が認識スコア集積部１２２から最新の時系列認識スコアＹを取り出し、取り出した時系列認識スコアＹを用いてもよい。時系列認識スコアは、複数の認識スコアを用いて生成された時系列データである。複数の認識スコアは、撮影時間範囲内の互いに異なる時刻に撮影範囲内の範囲を撮影した複数の画像データそれぞれを用いて計算され、また、当該複数の画像データそれぞれにおいて物体を検知した結果を示す。

異常パターン検知部１２３は、時系列認識スコアＹに対して事前に指定された異常パターンとのマッチングを行う。異常パターン検知部１２３は、検知結果ｒとして、時系列認識スコアＹが異常パターンに合致する場合には検知したことを示す結果、時系列認識スコアＹが異常パターンに合致しない場合には敵対的サンプルパッチ攻撃を検知していないことを示す結果をデータ出力部１２４に入力する。異常パターン検知部１２３は、通常時の認識スコアの推移と異なる推移である異常パターンを検知した際に敵対的サンプルパッチによる攻撃が行われたと判定する。異常パターン検知部１２３は、時系列認識スコアに、敵対的サンプルパッチ攻撃が複数の画像データの少なくともいずれかに対して実施された場合において生じる異常パターンが含まれているか否かを検知する。

データ出力部１２４は、入力された検知結果ｒを出力する。

【００１４】

図４は、本実施の形態に係る物体検知装置１１０及び攻撃検知装置１２０の各々のハードウェア資源の一例を示す図である。物体検知装置１１０及び攻撃検知装置１２０の各々は、コンピュータから成り、また、複数のコンピュータから成ってもよい。

【００１５】

物体検知装置１１０及び攻撃検知装置１２０の各々は、プロセッサ１１を備えている。プロセッサ１１は、バス１２を介してＲＯＭ１３と、ＲＡＭ１４と、通信ボード１５と、表示装置であるディスプレイ５１と、キーボード５２と、マウス５３と、ドライブ５４と、磁気ディスク装置２０等のハードウェアデバイスと接続され、これらのハードウェアデバイスを制御する。プロセッサ１１は、演算処理を行うＩＣ（Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ）であり、具体例として、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）、ＤＳＰ（Ｄｉｇｉｔａｌ Ｓｉｇｎａｌ Ｐｒｏｃｅｓｓｏｒ）、又はＧＰＵ（Ｇｒａｐｈｉｃｓ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）である。物体検知装置１１０及び攻撃検知装置１２０の各々は、複数のプロセッサを備えてもよい。複数のプロセッサは、プロセッサ１１の役割を分担する。

【００１６】

ドライブ５４は、ＦＤ（Ｆｌｅｘｉｂｌｅ Ｄｉｓｋ Ｄｒｉｖｅ）、ＣＤ（Ｃｏｍｐａｃｔ Ｄｉｓｃ）、又はＤＶＤ（Ｄｉｇｉｔａｌ Ｖｅｒｓａｔｉｌｅ Ｄｉｓｃ）等の記憶媒体を読み書きする装置である。

【００１７】

ＲＯＭ１３と、ＲＡＭ１４と、磁気ディスク装置２０と、ドライブ５４との各々は、記憶装置の一例である。記憶装置はコンピュータから独立していてもよい。

【００１８】

キーボード５２と、マウス５３と、通信ボード１５との各々は入力装置の一例である。ディスプレイ５１及び通信ボード１５は出力装置の一例である。

【００１９】

通信ボード１５は、有線又は無線で、ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）、インターネット、又は電話回線等の通信網に接続している。通信ボード１５は、具体例として、通信チップ又はＮＩＣ（Ｎｅｔｗｏｒｋ Ｉｎｔｅｒｆａｃｅ Ｃａｒｄ）から成る。

【００２０】

磁気ディスク装置２０は、ＯＳ（オペレーティングシステム）２１と、プログラム群２２と、ファイル群２３とを記憶している。

【００２１】

プログラム群２２は、本実施の形態において各部又は各器として説明する機能を実行するプログラムを含む。プログラムは、プロセッサ１１により読み出され実行される。即ち、プログラムは、各部又は各器としてコンピュータを機能させるものであり、また、各部又は各器の手順又は方法をコンピュータに実行させるものである。

本明細書に記載されているいずれのプログラムも、コンピュータが読み取り可能な不揮発性の記録媒体に記録されていてもよい。不揮発性の記録媒体は、具体例として、光ディスク又はフラッシュメモリである。本明細書に記載されているいずれのプログラムも、プログラムプロダクトとして提供されてもよい。

【００２２】

ファイル群２３は、本実施の形態において説明する各部又は各器で使用される各種データを含む。

【００２３】

＊＊＊動作の説明＊＊＊

物体検知装置１１０の動作手順は、物体検知方法に相当する。また、物体検知装置１１０の動作を実現するプログラムは、物体検知プログラムに相当する。攻撃検知装置１２０

の動作手順は、攻撃検知方法に相当する。また、攻撃検知装置１２０の動作を実現するプログラムは、攻撃検知プログラムに相当する。

【００２４】

図５は、本実施の形態に係る敵対的サンプルパッチ検知システム１００の処理の一例を示すフローチャートである。本図を参照して敵対的サンプルパッチ検知システム１００の処理を説明する。

【００２５】

（ステップＳ１１）

データ入力部１１１は、入力画像データｘを受け取り、受け取った入力画像データｘを物体検知器１１２に入力する。

【００２６】

（ステップＳ１２）

物体検知器１１２は、入力された入力画像データｘを用いて認識スコアｙを算出する。

【００２７】

（ステップＳ１３）

データ出力部１１３は、算出された認識スコアｙを出力する。

【００２８】

（ステップＳ１４）

データ入力部１２１は、認識スコアｙを受け取り、受け取った認識スコアｙを認識スコア集積部１２２に入力する。

【００２９】

（ステップＳ１５）

認識スコア集積部１２２は、入力された認識スコアｙを時系列認識スコアＹ’に追加することによって時系列認識スコアＹ’を時系列認識スコアＹに更新し、更新した時系列認識スコアＹを異常パターン検知部１２３に入力する。

【００３０】

（ステップＳ１６）

異常パターン検知部１２３は、入力された時系列認識スコアＹが事前に指定された異常パターンに合致するか否かを判定する。

異常パターンが時系列認識スコアＹに合致する場合、攻撃検知装置１２０はステップＳ１７に進む。それ以外の場合、攻撃検知装置１２０はステップＳ１８に進む。

【００３１】

（ステップＳ１７）

データ出力部１２４は、検知結果ｒとして、敵対的サンプルパッチ攻撃を検知したことを示す結果を出力する。

【００３２】

（ステップＳ１８）

データ出力部１２４は、検知結果ｒとして、敵対的サンプルパッチ攻撃を検知していないことを示す結果を出力する。

【００３３】

＊＊＊実施の形態１の効果の説明＊＊＊

以上のように、本実施の形態によれば、時系列認識スコアが異常パターンに合致するか否かを判定することによって敵対的サンプルパッチ攻撃を検知することができる。

【００３４】

＊＊＊他の構成＊＊＊

＜変形例１＞

図６は、本変形例に係る物体検知装置１１０及び攻撃検知装置１２０の各々のハードウェア構成例を示している。

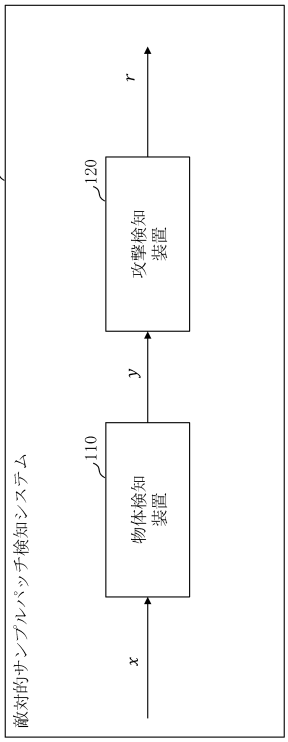
物体検知装置１１０及び攻撃検知装置１２０の各々は、プロセッサ１１、プロセッサ１１とＲＯＭ１３、プロセッサ１１とＲＡＭ１４、あるいはプロセッサ１１とＲＯＭ１３と

ＲＡＭ１４とに代えて、処理回路１８を備える。
　処理回路１８は、物体検知装置１１０及び攻撃検知装置１２０の各々が備える各部の少なくとも一部を実現するハードウェアである。
　処理回路１８は、専用のハードウェアであってもよく、また、磁気ディスク装置２０に格納されるプログラムを実行するプロセッサであってもよい。
【００３５】
　処理回路１８が専用のハードウェアである場合、処理回路１８は、具体例として、単一回路、複合回路、プログラム化したプロセッサ、並列プログラム化したプロセッサ、ＡＳＩＣ（Ａｐｐｌｉｃａｔｉｏｎ Ｓｐｅｃｉｆｉｃ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ）、ＦＰＧＡ（Ｆｉｅｌｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ）又はこれらの組み合わせである。
　物体検知装置１１０及び攻撃検知装置１２０の各々は、処理回路１８を代替する複数の処理回路を備えてもよい。複数の処理回路は、処理回路１８の役割を分担する。
【００３６】
　物体検知装置１１０及び攻撃検知装置１２０の各々において、一部の機能が専用のハードウェアによって実現されて、残りの機能がソフトウェア又はファームウェアによって実現されてもよい。
【００３７】
　処理回路１８は、具体例として、ハードウェア、ソフトウェア、ファームウェア、又はこれらの組み合わせにより実現される。
　プロセッサ１１とＲＯＭ１３とＲＡＭ１４と処理回路１８とを、総称して「プロセッシングサーキットリー」という。つまり、物体検知装置１１０及び攻撃検知装置１２０の各々の各機能構成要素の機能は、プロセッシングサーキットリーにより実現される。
【００３８】
＊＊＊他の実施の形態＊＊＊
　実施の形態１について説明したが、本実施の形態のうち、複数の部分を組み合わせて実施しても構わない。あるいは、本実施の形態を部分的に実施しても構わない。その他、本実施の形態は、必要に応じて種々の変更がなされても構わず、全体としてあるいは部分的に、どのように組み合わせて実施されても構わない。各部又は各器として説明するものは、ファームウェア、ソフトウェア、ハードウェア又はこれらの組み合わせのいずれで実装されても構わない。
　なお、前述した実施の形態は、本質的に好ましい例示であって、本開示と、その適用物と、用途の範囲とを制限することを意図するものではない。フローチャート等を用いて説明した手順は、適宜変更されてもよい。
【符号の説明】
【００３９】
　１１　プロセッサ、１２　バス、１３　ＲＯＭ、１４　ＲＡＭ、１５　通信ボード、１８　処理回路、２０　磁気ディスク装置、２１　ＯＳ、２２　プログラム群、２３　ファイル群、５１　ディスプレイ、５２　キーボード、５３　マウス、５４　ドライブ、１００　敵対的サンプルパッチ検知システム、１１０　物体検知装置、１１１　データ入力部、１１２　物体検知器、１１３　データ出力部、１２０　攻撃検知装置、１２１　データ入力部、１２２　認識スコア集積部、１２３　異常パターン検知部、１２４　データ出力部。

【図面】

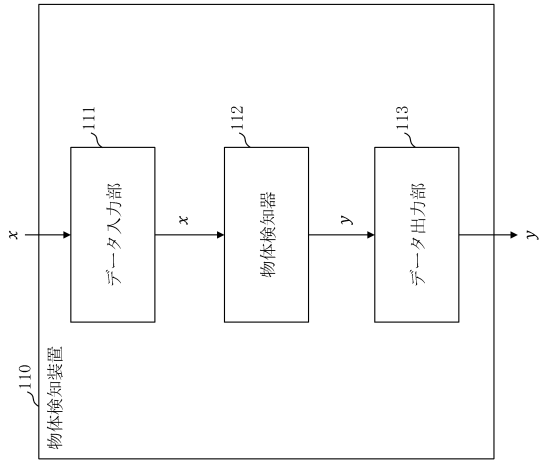
【図１】

図1



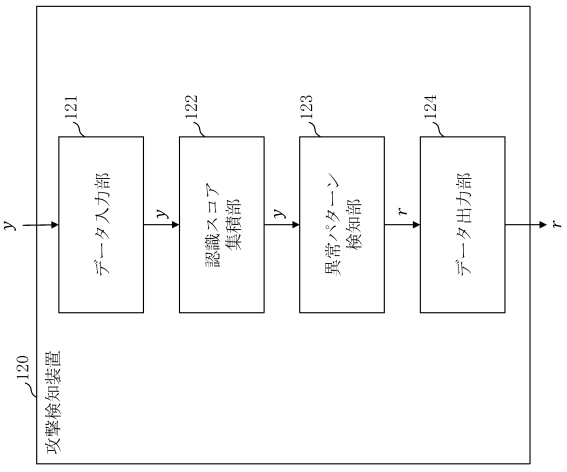

【図２】

図2



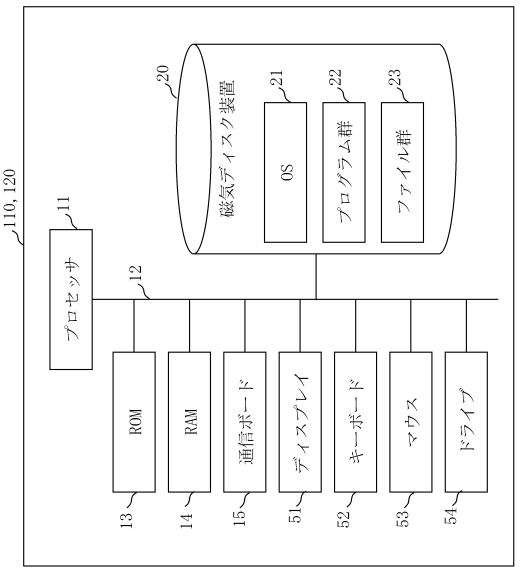

【図３】

図3



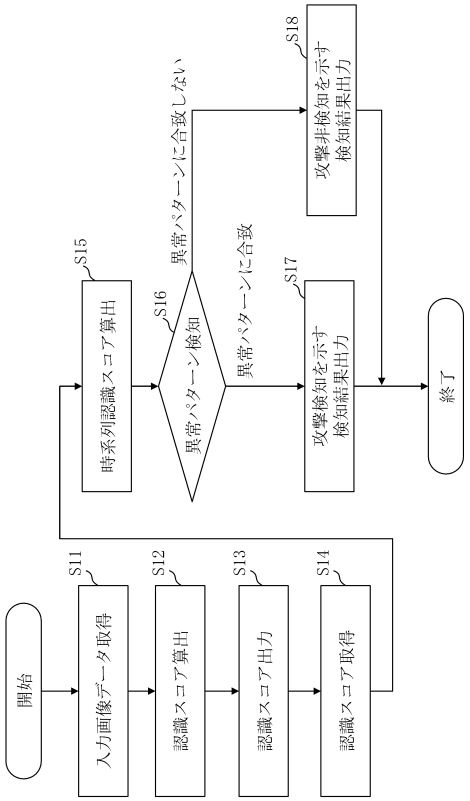

【図４】

図4



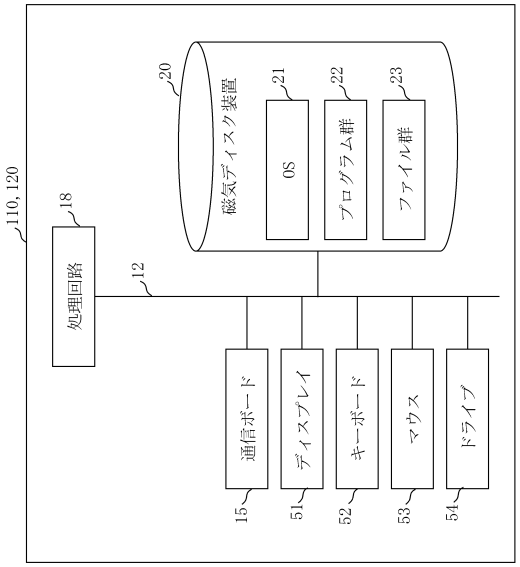
【図５】

図5


開始
入力画像データ取得
S11
認識スコア算出
S12
認識スコア出力
S13
認識スコア取得
S14
時系列認識スコア算出
S15
異常パターン検知
S16
異常パターンに合致
異常パターンに合致しない
攻撃検知を示す
検知結果出力
S17
攻撃非検知を示す
検知結果出力
S18
終了

【図６】

図6


110, 120
処理回路
18
12
磁気ディスク装置
20
OS
21
プログラム群
22
ファイル群
23
通信ボード
15
ディスプレイ
51
キーボード
52
マウス
53
ドライブ
54

フロントページの続き

(56)参考文献 特開２０１９－１２５８６７（ＪＰ，Ａ）
JI, N., et al.，Adversarial YOLO: Defense Human Detection Patch Attacks via Detecting Adversarial Patches，arXiv.org [online]，arXiv:2103.08860，2021年03月16日，Retrieved from the Internet: 〈URL: https://arxiv.org/abs/2103.08860〉 [Retrieved on 2021-08-31]
XIAO, C., et al.，AdvIT: Adversarial Frames Identifier Based on Temporal Consistency in Videos，Proceedings of 2019 IEEE/CVF International Conference on Computer Vision (ICCV)，2019年10月27日，pp. 3967-3976，Retrieved from the Internet: 〈URL: https://ieeexplore.ieee.org/document/9010733〉 [Retrieved on 2021-08-31]，DOI: 10.1109/ICCV.2019.00407
DOSHI, K. et al.，Continual Learning for Anomaly Detection in Surveillance Videos，arXiv.org [online]，arXiv:2004.07941，2020年04月15日，Retrieved from the Internet: 〈URL: https://arxiv.org/abs/2004.07941〉 [Retrieved on 2021-08-31]

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／００－２１／８８
Ｇ０６Ｎ ３／００－９９／００