(12) UK Patent Application (19) GB (11) 2508377 (13) A

(43) Date of A Publication 04.06.2014

(21) Application No: 1221504.2

(22) Date of Filing: 29.11.2012

(71) Applicant(s):
Crane Payment Solutions Limited
(Incorporated in the United Kingdom)
Coin House, New Coin Street, Royton, OLDHAM,
Lancashire, OL2 6JZ, United Kingdom

(72) Inventor(s):
Alex Hadley

(74) Agent and/or Address for Service:
Venner Shipley LLP
200 Aldersgate, LONDON, EC1A 4HD,
United Kingdom

(51) INT CL:
G07F 5/24 (2006.01) ***G07D 1/02*** (2006.01)
G07D 9/00 (2006.01)

(56) Documents Cited:
GB 2023902 A **US 5568854 A**
US 20030217905 A1

(58) Field of Search:
INT CL **G07D, G07F**
Other: **WPI, EPODOC, TXTE, TXTT, INSPEC, XPESP, XPESP2, XPIEE, XPIPCOM, XPI3E, XPMISC, XPLNCS, XPRD**

(54) Title of the Invention: **Preventing fraud**
Abstract Title: **Preventing fraud in a coin payout mechanism**

(57) A fraud prevention apparatus 1 for a coin payout unit 2 comprises a sensor 3a, 3b comprising an electrical oscillator for detecting coins in a coin outlet path 5 and one or more controllers configured to cause an expected change in the oscillating frequency of the sensor and to verify that the oscillating frequency has changed as expected. The controller may cause the expected change in the oscillating frequency by altering a property of an oscillator circuit in the sensor. An expected change could also be caused by altering a component configuration of the sensor. Timing elements may be altered, circuit components may be added to or removed from the sensor circuit or operation of circuit components may be varied. The controller is configured to verify that the oscillating frequency has changed as expected by determining an actual oscillating frequency of the sensor and comparing the actual frequency with an expected frequency. The invention is used to detect whether a fraudster has attempt to blind a coin sensor in the coin outlet of the apparatus and so cause the apparatus to release coins to the outlet because the sensor does not detect that coins have actually been dispensed.

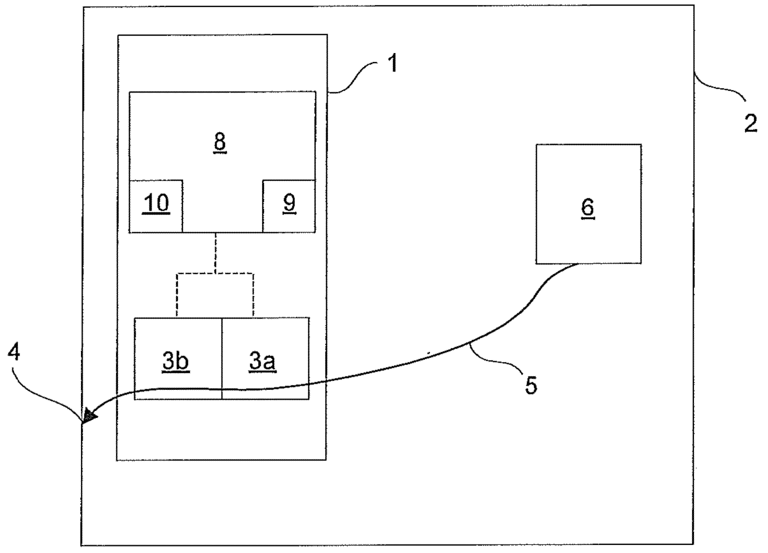

Fig. 1

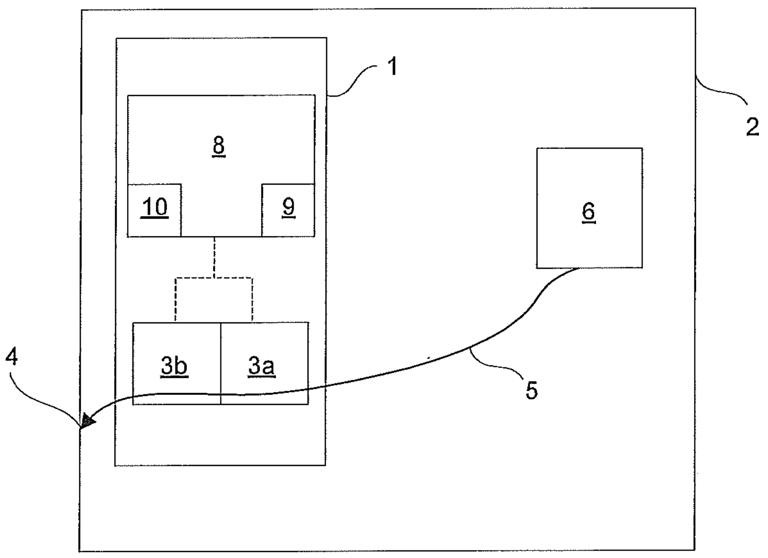
1
2
8
10
9
6
3b
3a
4
5

Fig. 1

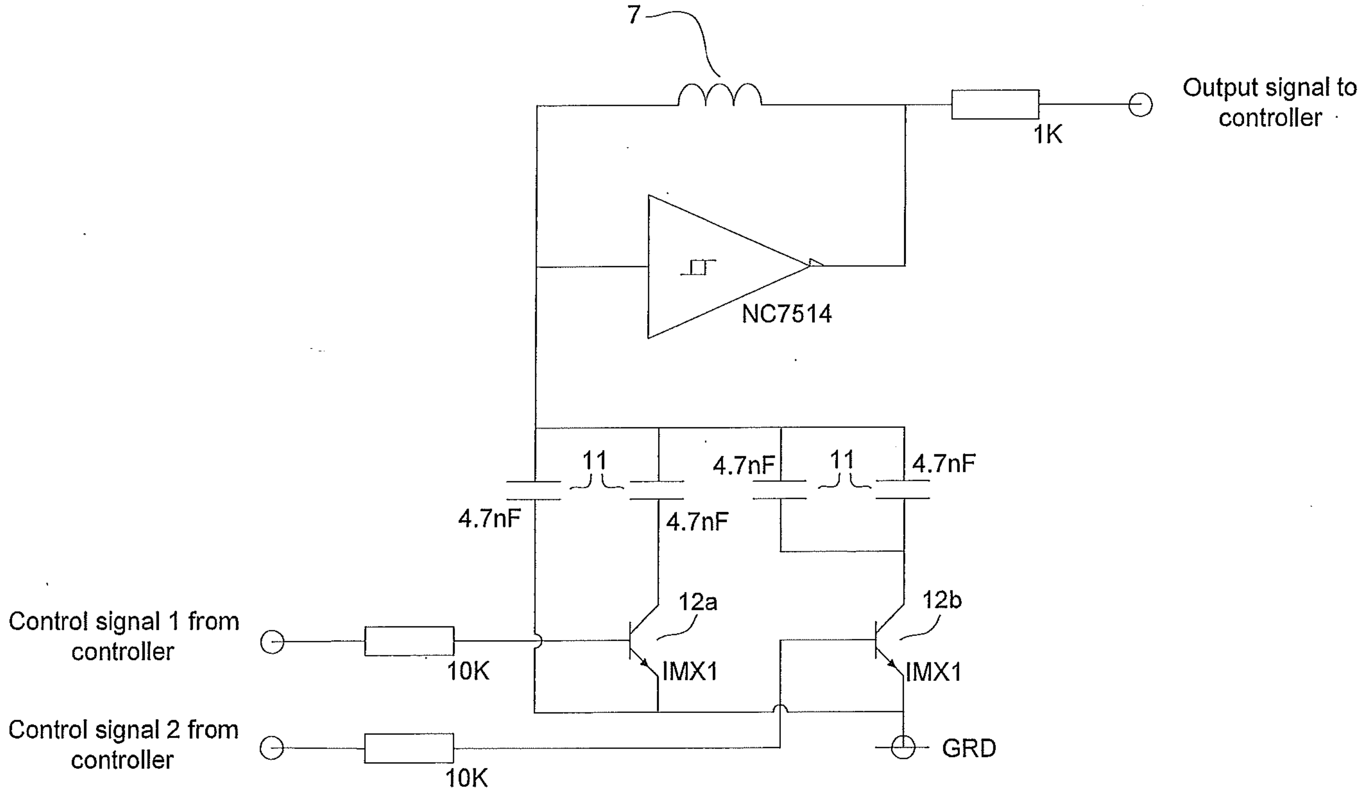
7
Output signal to controller
1K
NC7514
11
4.7nF
4.7nF
4.7nF
11
4.7nF
4.7nF
12a
12b
Control signal 1 from controller
10K
IMX1
IMX1
Control signal 2 from controller
10K
GRD

Fig. 2

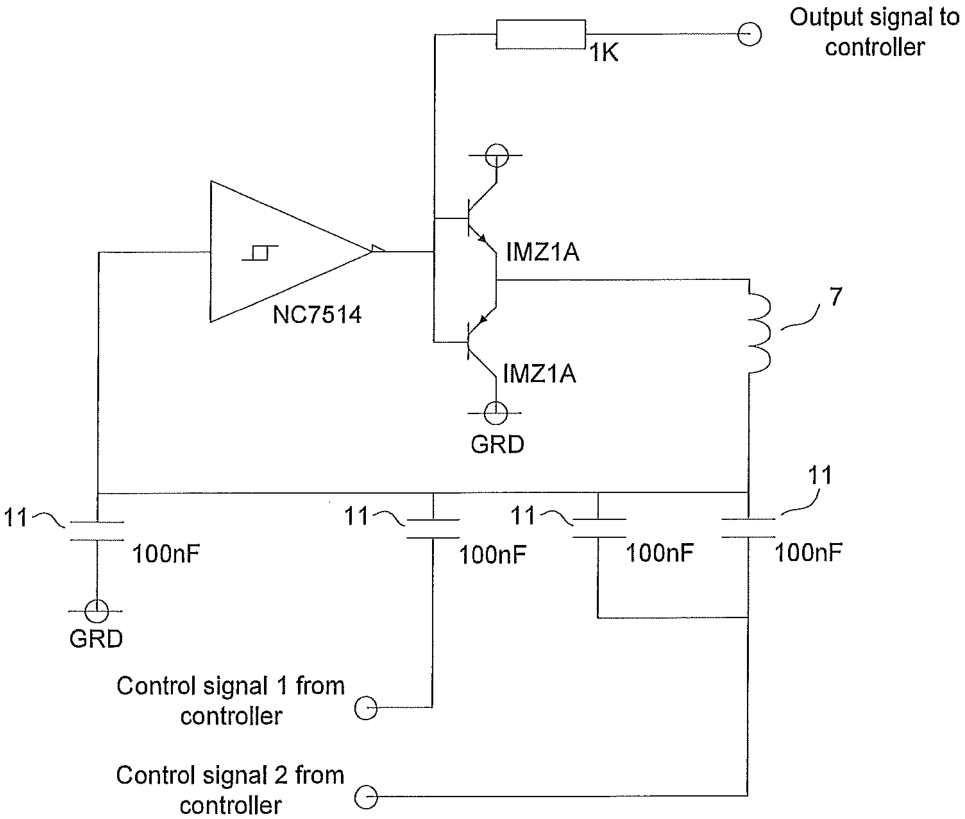
Output signal to controller
1K
IMZ1A
NC7514
7
IMZ1A
GRD
11
11
11
11
100nF
100nF
100nF
100nF
GRD
Control signal 1 from controller
Control signal 2 from controller

Fig. 3

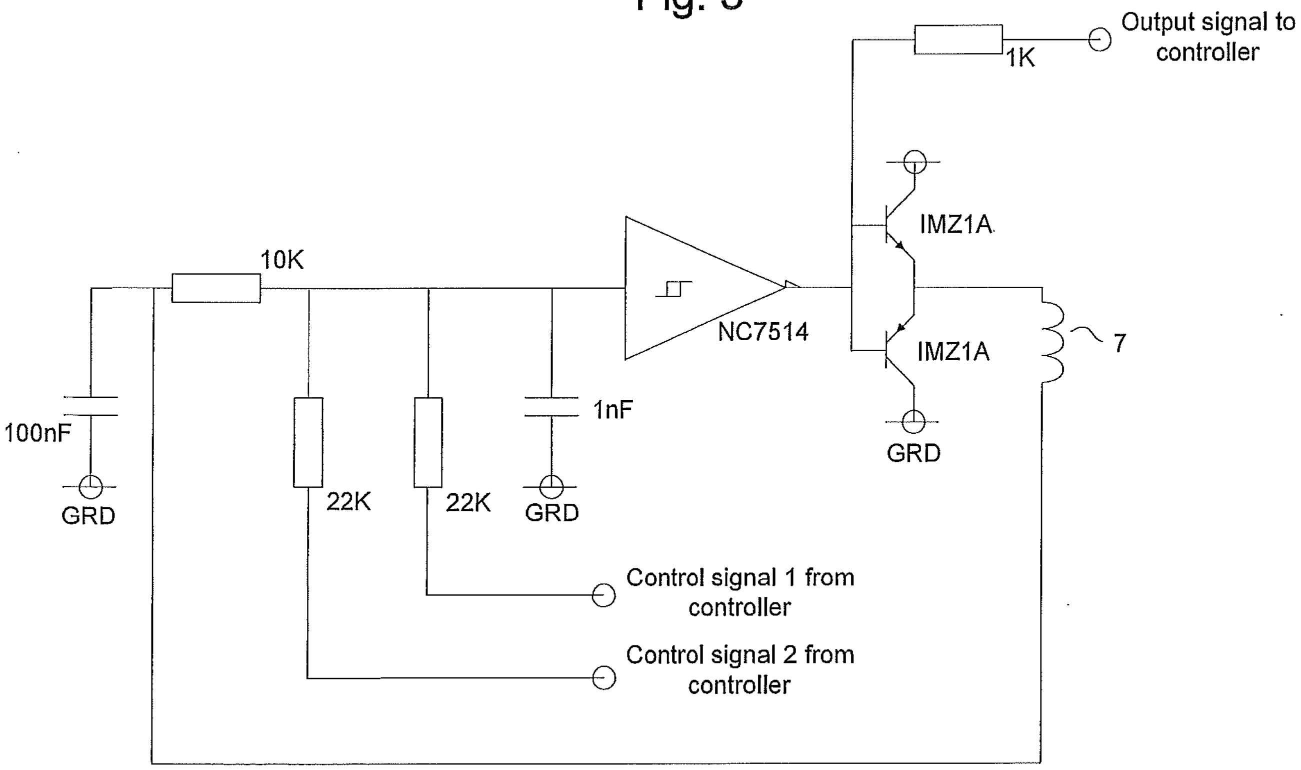
Output signal to controller
1K
IMZ1A
10K
NC7514
IMZ1A
7
100nF
1nF
GRD
22K
22K
GRD
GRD
Control signal 1 from controller
Control signal 2 from controller

Fig. 4

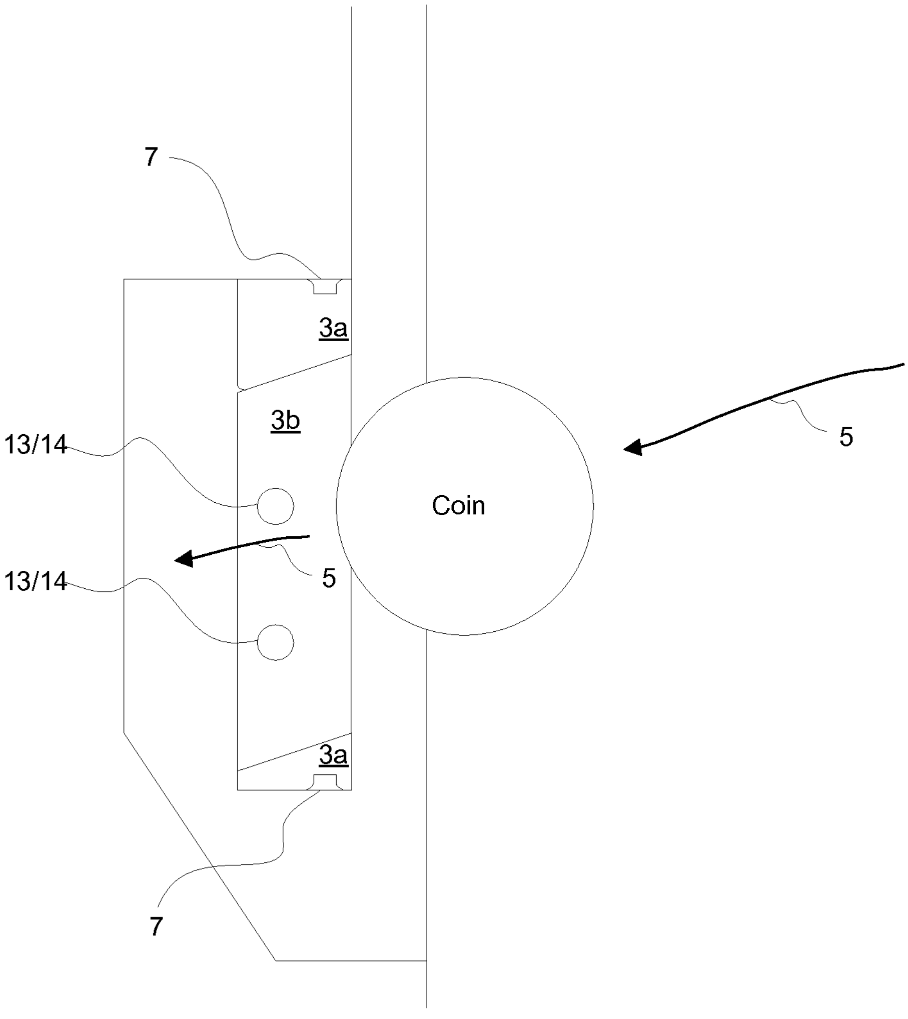

Fig. 5

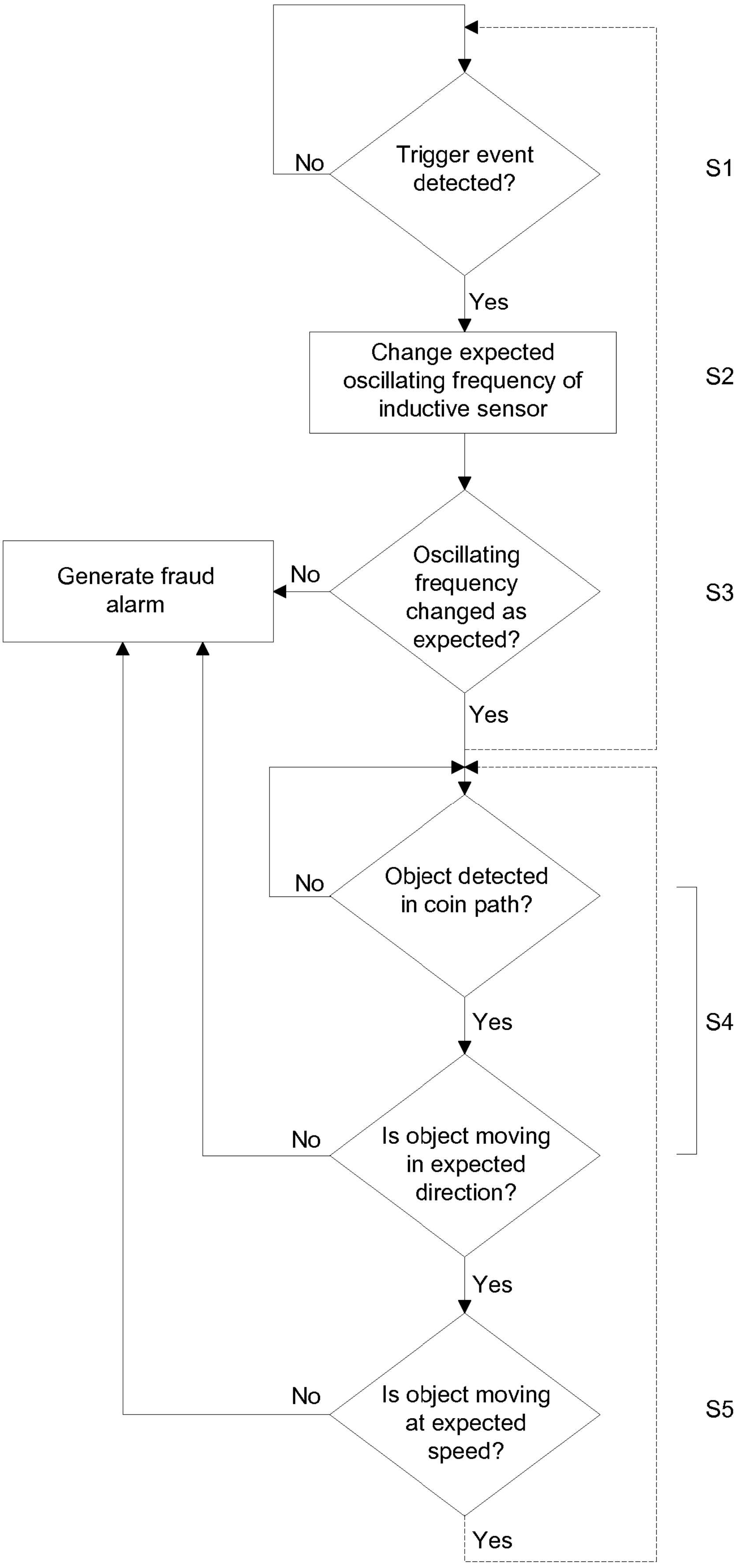
Trigger event detected?
No
Yes
S1
Change expected oscillating frequency of inductive sensor
S2
Generate fraud alarm
No
Oscillating frequency changed as expected?
Yes
S3
Object detected in coin path?
No
Yes
S4
Is object moving in expected direction?
No
Yes
Is object moving at expected speed?
No
Yes
S5

Fig. 6

Preventing Fraud

Field

This invention relates to preventing fraud by detecting fraud attempts at a payout apparatus. Particularly, but not exclusively, the invention relates to monitoring one or more coin sensors to verify correct operation.

Background

In an effort to fraudulently cause a payout apparatus to payout more money than it should, a fraudster may attempt to blind a coin sensor in a coin outlet of the apparatus in order to prevent the apparatus from registering that coins are being dispensed and thus cause the apparatus to continue to release coins into the coin outlet.

Summary

According to the invention, there is provided a fraud prevention apparatus for a coin payout unit, comprising a coin sensor comprising an electrical oscillator for detecting coins in a coin outlet path; and at least one controller configured to cause an expected change in an oscillating frequency of the sensor and to verify that the oscillating frequency has changed as expected.

The controller may be configured to cause the expected change in the oscillating frequency by altering a property of an oscillator circuit in the sensor.

The controller may be configured to cause the expected change in oscillating frequency by altering a component configuration of the sensor.

Altering the component configuration of the sensor may comprise altering the configuration of one or more timing elements in the sensor.

Altering the component configuration of the sensor may comprise selectively adding at least one circuit component to the sensor.

Altering the component configuration of the sensor may comprise selectively removing at least one circuit component from the sensor.

Altering the component configuration of the sensor may comprise selectively varying the operation of at least one circuit component in the sensor.

The at least one circuit component may comprise a capacitive component.

The at least one circuit component may comprise an electrical resistor.

The at least one circuit component may comprise an electrically inductive component.

The at least one circuit component may have a value in a predetermined wide tolerance range, such as wider than average.

The controller may be configured to verify that the oscillating frequency has changed as expected by determining an actual oscillating frequency of the sensor and comparing the actual frequency with an expected frequency.

The controller may be configured to determine the expected oscillating frequency from a component configuration of the sensor.

The controller may be configured to measure the actual oscillating frequency from an output signal of the sensor.

The controller may be configured to verify that the oscillating frequency has changed as expected by searching a measured frequency profile of the sensor for a match with an expected change.

The controller may be configured to determine an expected change in oscillating frequency from an actual change to a component configuration of the sensor.

The controller may be configured to cause the expected change in oscillating frequency and verify that the oscillating frequency has changed as expected in response to the elapse of a predetermined time period, the detection of a predetermined event or the occurrence of a randomly generated time event.

If the controller determines that the oscillating frequency has not changed as expected, the controller may be configured to respond by causing an alarm signal to the generated

The sensor may be configured to detect objects at a first location in a coin path of the payout apparatus, a separate sensor may be configured to detect objects at a second location in the coin path of the payout apparatus; and at least one of the one or more controllers may be configured to compare the detections at the first and second locations and verify whether a result of the comparison is as expected.

The separate sensor may be an optical sensor.

The separate sensor may alternatively be an infra-red or ultra-violet sensor.

The result of the comparison may comprise a direction in which an object has moved in the coin path.

The result of the comparison may comprise a time gap between the detections at the first and second locations.

The coin sensor may comprise a coin sensing element whose electrical characteristics are affected by the electrical effect of a passing coin.

According to the invention, there is provided a coin payout unit comprising the fraud prevention apparatus.

According to the invention, there is provided a method of detecting fraud at a coin payout unit, comprising causing an expected change in an oscillating frequency of a coin sensor for detecting coins in the payout unit; and verifying that the oscillating frequency has changed as expected.

The method may comprise causing the expected change in the oscillating frequency by altering a property of an oscillator circuit in the sensor.

The method may comprise causing the expected change in oscillating frequency by altering a component configuration of the sensor.

Altering the component configuration of the sensor may comprise altering a configuration of at least one timing component in the sensor.

Altering the component configuration of the sensor may comprise selectively removing or adding at least one circuit component from or to the sensor.

Altering the component configuration of the sensor may comprise selectively varying the operation of at least one circuit component in the sensor.

The at least one circuit component may have a value in a predetermined tolerance range which is wider than average.

The method may comprise verifying that the oscillating frequency has changed as expected by determining an actual oscillating frequency of the sensor and comparing the actual frequency with an expected frequency.

According to the invention, there is provided a method of manufacturing a plurality of the fraud prevention apparatuses, comprising selecting wide tolerance circuit components for use in the sensors so as to cause different sensors to oscillate at different ranges of preset frequencies.

Brief description of the figures

Embodiments of the invention will now be described, for the purposes of example only, with reference to the accompanying figures in which:

Figure 1 is a schematic illustration of a coin payout apparatus in which a fraud prevention apparatus is comprised;
figure 2 is a schematic diagram of a coin sensor circuit, the expected oscillating frequency of which can be altered to verify its correct operation;
figure 3 is a schematic diagram of another coin sensor circuit, the expected oscillating frequency of which can be altered to verify its correct operation;
figure 4 is a schematic diagram of another coin sensor circuit, the expected oscillating frequency of which can be altered to verify its correct operation;
figure 5 is a schematic illustration of coin outlet region of a payout apparatus in which an optical sensor and an oscillating sensor are configured to detect the presence of coins and other objects; and
figure 6 is a flow diagram of a method of detecting fraud attacks in a monetary payout apparatus.

Detailed description

A fraud prevention apparatus 1 of a monetary payout apparatus 2 is described below. The fraud prevention apparatus 1 is configured to perform verification operations, the results of which are indicative of whether the payout apparatus 2 is operating correctly. Incorrect operation of the payout apparatus 2 may be indicative of a fraud attack on the payout apparatus 2, such as an attack in which a fraudster is attempting to cause the payout apparatus 2 to payout coins which it would not otherwise payout if operating correctly.

The verification operations which are performed by the fraud prevention apparatus 1 may comprise verifying that one or more sensors 3, which are configured to sense coins as they are being paid out via a coin outlet 4 of the payout apparatus 2, are operating correctly. Referring to figure 1, the sensor(s) 3 may be located in or adjacent to a coin outlet path 5 which directs coins released from coin storage 6 of the payout apparatus 2 to the coin outlet 4 from which the coins are available for collection. An example of suitable coin storage is a coin hopper 6 which selectively and controllably dispenses coins to the coin outlet 4 via the coin outlet path 5. In correct operation, the sensors 3 are configured to detect the presence of coins as the coins move past the sensors 3 in the coin outlet path 5 and to generate signals indicating that the coins have been detected. In this way, the coin payout apparatus 2 is able to register and count the coins into the coin outlet 4 and thus determine when to stop dispensing coins into the coin outlet path 5.

The fraud prevention apparatus 1 verifies that the sensors 3 are operating correctly by monitoring the signals generated by the sensors 3 and checking that the signals are as expected. If the signals are not as expected, the fraud prevention apparatus 1 may be configured to output an alarm signal to indicate that the payout apparatus 2 is under a fraud attack. The payout apparatus 1 may be configured to respond to the alarm signal by shutting down its payout operations.

The fraud prevention apparatus 1 and the monetary payout apparatus 2 in which the fraud prevention apparatus 1 is comprised may operate under the control of a single electronic controller, or a plurality of electronic controllers, which each control the operation of both apparatuses. For example, the apparatuses 1, 2 may be implemented as a single unit in which the controller(s) may be configured to control all functions of the payout apparatus 2, including those of the fraud prevention apparatus 1.

Alternatively, the fraud prevention apparatus 1 and monetary payout apparatus 2 may operate under the control of dedicated separate electronic controllers which each control the operations of only one of the two apparatuses 1, 2.

The fraud prevention apparatus 1 comprises a sensor 3a for detecting coins in the coin outlet path 5 of the payout apparatus 2. The sensor 3a comprises an oscillator, such as an electrical oscillator circuit, which oscillates at a frequency which is dependent on the characteristics of a coin sensing element 7 coupled to the sensor 3a. The coin sensing element 7 has electrical characteristics which are temporarily varied by the electrical effect of coins as the coins move along the coin outlet path 5, as described below.

Any suitable oscillator circuit may be used. Examples include oscillator circuits in which the coin sensing element 7 is an electrically inductive element 7, such as in LC and RL oscillator circuits. The electrically inductive element 7 may comprise one or more electrically inductive coils or other windings.

Another example is an oscillator circuit in which the coin sensing element 7 is a capacitive element 7, such as in RC oscillator circuits. The capacitive element 7 may comprise one or more capacitors.

Specific examples of the sensor 3a are illustrated in figures 2 to 4. In these figures, the sensor 3a comprises an LC relaxation oscillator in which the coin sensing element 7 is an inductive element.

The oscillator may be implemented using an inverting Schmitt trigger, which may comprise either a plurality of connected discrete circuit components, for example comprising a comparator (e.g. comprising a transistor) and a plurality of resistors, or an integrated circuit (IC) as shown in the figures 2 to 4.

The coin sensing element 7 is connected in the oscillator so that the sensor 3a oscillates at a frequency which is dependent on, and which varies with, the electrical characteristics of the sensing element 7. For example, if the sensing element 7 comprises an inductor 7 as illustrated in figures 2 to 4, the sensor 3a is configured to oscillate at a frequency which is dependent on the inductance of the inductor 7.

As will be described below, the fraud prevention apparatus 1 is configured to deliberately vary the expected base oscillating frequency of the sensor 3a, for example by altering a component configuration in the sensor 3a, to enable detection of fraud attacks.

Referring to figures 1 to 4, the sensor 3a, and in particular the coin sensing element 7 referred to above, is located in the proximity of the coin outlet path 5 of the payout apparatus 2 such that coins moving along the outlet path 5 towards the coin outlet 4 effect a detectable change in the electrical characteristics, such as the inductance or capacitance, of the sensing element 7. Therefore, when the payout apparatus 2 dispenses a coin along the outlet path 5, the oscillating frequency of the sensor 3a is temporarily altered, in a manner which is related to the properties of the coin, by the electromagnetic effect of the coin moving past the sensing element 7.

The sensor 3a is configured to generate an output signal which is proportional to and/or indicative of its oscillating frequency. This output signal of the sensor 3a should be expected, in correct operation of the sensor 3a, to reflect alterations in the electrical characteristics of the sensing element 7 and thus the presence of coins in the coin outlet path 5. For example, a spike, representative of a change in the electrical characteristics of the element 7, may be observed in the output signal of the sensor 3a when a coin passes the sensing element 7 on its way to the coin outlet 4.

The output signal may comprise an output voltage signal of the sensor 3a, as shown in figures 2 to 4, and hence may oscillate at the same frequency as the sensor 3a.

The payout apparatus 2 may be configured to determine the value of the coin(s) from the characteristics of the corresponding changes(s) in the output signal and to count the coin(s) into the coin outlet 4. The apparatus 2 can thereby determine when the required value of coins has been dispensed and prevent itself from over-paying. The sensor 3a may, for example, be configured to feed the output signal of the sensor 3a to an electronic controller of the payout apparatus 2. The controller is configured to analyse the signal, for example by comparing the signal characteristics to known coin characteristics stored in a memory of the apparatus 2, to determine when the correct value of coins has been dispensed for a particular payout. In doing so, the controller may be configured to cause an outlet of the coin storage 6, which feeds into the coin outlet path 5, to be closed and thereby prevent over-payment. The apparatus 2 may alternatively be configured only to verify that the expected number of coins have been dispensed, rather than also additionally checking the value of the dispensed coins. This may require fewer circuit components.

If the sensor 3a is not operating correctly, such that the output signal fed to the controller indicates that fewer, or a lower value of, coins have been dispensed to the coin outlet 4 than is actually the case, the controller may be mislead into dispensing more coins than are required into the coin exit path 5 and thus over-paying the payout in an attempt to count the correct value of coins into the coin outlet 4. One instance in which the sensor 3a may not operate correctly is if it is fraudulently overdriven by an externally generated waveform which hides the changes in output signal which would normally be caused by coins passing the sensing element 7 on their way from the coin storage 6 to the coin outlet 4. For example, the sensor 3a might be overdriven at a frequency similar to that which indicates that no coin is present in the coin exit path 5. Alternatively, the electrical characteristics of the sensing element 7 might be altered by inserting a foreign object into the coin outlet path 5 from the exterior of the payout apparatus 2.

In these circumstances, coins may pass the sensing element 7 of the sensor 3a on their way to the coin outlet 4 without causing corresponding effects in the output signal of the sensor 3a and thus without being registered and counted by the controller.

The fraud prevention apparatus 1 is configured to detect such fraudulent acts by verifying that the sensor 3a is operating correctly. For example, the sensor 3a may be configured to feed its output signal to an electronic controller 8 of the fraud prevention apparatus 1, shown in figure 1, which is configured to cause a sensor verification operation to be carried out in relation to the sensor 3a. The controller 8 may comprise one or more processors 9 which, operating under the control of computer-readable instructions, for example comprised in computer program code stored in a memory 10 of the fraud prevention apparatus 1 or elsewhere in the payout apparatus 2, are configured to carry out the verification operation.

The verification operation for the sensor 3a comprises causing a change in the expected oscillating frequency of the sensor 3a and subsequently checking that the oscillating frequency has changed as expected. The change in the expected oscillating frequency of the sensor 3a may be caused by altering the component configuration of the oscillator. For example, as will be described in more detail below, altering the component configuration of the oscillator may comprise modifying one or more circuit components, such as by switching one or more circuit components into or out of the oscillator circuit, in order to alter the properties of the circuit. The components which are modified, e.g. switched into and/or out of the circuit, may be timing components of the oscillator, such as capacitors and/or resistors, or components of the inverter, as explained below.

Referring to figures 2 and 3, an example comprises altering the capacitance of an LC relaxation oscillator circuit in the sensor 3a by a known amount and subsequently verifying that the oscillating frequency of the sensor 3a has changed as would be expected following the known change in capacitance. The capacitance may be altered by replacing, adding and/or removing capacitive components to/from the oscillator circuit. In order to facilitate this, the sensor 3a may be selectively coupled to a plurality of capacitors 11 which can be selectively switched into and out of the LC relaxation oscillator by the controller 8.

More specifically, the plurality of capacitors 11 may be coupled to the LC relaxation oscillator via one or more electronic switches 12, such as one or more transistors 12a, 12b, which can be operated by the controller 8 to selectively switch each of the capacitors 11 into or out of the oscillator circuit to vary its capacitance. An example is illustrated in figure 2, in which a plurality of switches 12, each comprising a transistor 12a, 12b, are each configured to selectively switch one or more of the plurality of capacitors 11 into and out of an LC oscillator circuit under the control of the controller 8.

The controller 8 opens and closes the switches 12 by supplying control signals to the switches 12. For example, figure 2 illustrates how each of the transistors 12a, 12b referred to above may be independently coupled to the controller 8 of the fraud prevention apparatus 1 via a suitable communication coupling so that control signals, such as suitable voltage signals, can be applied by the controller 8 to cause the transistors 12a, 12b to independently switch each capacitor 11 into or out of the oscillator circuit.

It will be appreciated that in alternative implementations of the oscillator, timing components other than capacitors 11 could be selectively switched into or out of the oscillator circuit in the same manner as described above in order to cause a change in the expected oscillating frequency of the sensor 3a. For example, if an RL or RC oscillator is used, resistive components such as resistors can be selectively switched into and out of the oscillator under the control of the controller 8.

Additionally or alternatively, a change in the expected oscillating frequency of the sensor 3a may be caused by altering the component configuration of the sensor's inverter. For example, referring to figure 4, one or more discrete circuit components, such as one or more resistors, may be switched into or out of the inverter in order to vary the switching thresholds of the inverter and thereby vary the oscillating frequency of the sensor 3a.

Additionally or alternatively, changes in the expected oscillating frequency of the sensor 3a may be caused by switching additional coin sensing elements 7 into or out of the oscillator circuit. For example, the circuit may comprise a plurality of inductive or capacitive elements 7, connected in series or parallel, which can be selectively switched, individually or collectively, into or out the circuit to vary the oscillating frequency of the sensor 3a.

Referring to figures 3 and 4, as an alternative to using the switches 12 discussed above and shown in figure 2, the circuit components may be switched into and out of the oscillator circuit by control voltage signals applied directly to the components from the controller 8. This may reduce the number of components required in the oscillator circuit.

The controller 8 may be configured to change the expected base frequency of the oscillator, for example by altering the component configuration of the oscillator in one of the ways described above, in response to the elapse of preset time periods. The controller 8 may be configured to generate the new component configuration randomly, so that the new expected oscillating frequency is also randomly generated. The controller 8 may additionally or alternatively alter the expected base frequency of the oscillator at randomly generated times, or in response to particular events. For example, the controller 8 may be configured to alter the configuration of the oscillator at regular time intervals, such as every ten milliseconds, in order to vary the expected oscillating frequency of the sensor 3a. It will be appreciated that any preset number of milliseconds may be used. Additionally or alternatively, the controller 8 may be configured to alter the expected base frequency of the oscillator in response to the elapse of a relatively long time period since a coin was last detected by the sensor 3a or in response to other similar events which are consistent with the sensor 3a being fraudulently manipulated. The controller 8 may be configured to randomly generate a new component configuration for the oscillator immediately before causing a transition to a new configuration.

The exact component configuration of the oscillator is always known to the controller 8 and hence the controller 8 is always able to determine the expected oscillating frequency of the sensor 3a and to compare the expected oscillating frequency with the measured oscillating frequency to verify correct operation. The controller 8 stores the configuration in the memory 10 of the fraud prevention apparatus 1 or elsewhere in the payout apparatus 2.

As referred to above, having altered the configuration of the sensor 3a so as to expect a change in its oscillating frequency, the controller 8 of the fraud prevention apparatus 1 is configured to verify that the oscillating frequency of the sensor 3a has changed as expected. The controller 8 may be configured to make these verifications at the same regular intervals as the alterations in sensor configuration.

The controller 8 may be configured to predict the expected new oscillating frequency of the sensor 3a by mathematically calculating the frequency based on the known component configuration of the oscillator. For example, if an LC relaxation oscillator is used, the controller 8 is configured to predict the expected new oscillating frequency of the inductive sensor 3a by mathematically calculating the frequency based on the known capacitance of the LC relaxation oscillator in its new configuration and other known parameters of the oscillator circuit, including those of the inductive sensing element 7. Subsequently, the controller 8 may be configured to measure the actual oscillating frequency of the sensor 3a to check whether the measured frequency falls within a predetermined margin of the predicted frequency. The frequency measurement takes place before the controller 8 causes the oscillator to transition to another new component configuration, and hence another new expected oscillating frequency, at which time the verification process may be repeated. The size of the predetermined margin, referred to immediately below as the predetermined acceptable range, may take into account, or represent, margins of error associated with the predicted and/or measured frequencies.

If the predicted and actual operating frequencies of the sensor 3a are both within the predetermined acceptable range, the controller 8 may be configured to positively verify that the sensor 3a is operating correctly. Conversely, if the predicted and actual operating frequencies are not within the predetermined range, the controller 8 may fail to verify that the sensor 3a is operating correctly, or may make a positive determination that it is not, thereby causing the alarm signal referred to previously to be generated.

Manufacture of a plurality of the fraud prevention apparatuses 1 may comprise varying the values of components in the sensor 3a from one apparatus 1 to the next in order to ensure that the sensors 3a of different apparatuses 1 do not oscillate at the same base frequencies. For example, the values of timing components in the oscillator circuit, such as the capacitances of the individual capacitors 11 shown in figures 2 and 3 or the resistances of individual resistors, may be varied from one apparatus 1 to the next. Alternatively the values of discrete components in the inverter may be varied from one apparatus 1 to the next. This action ensures that the various possible oscillator configurations, and hence oscillating frequencies, of each sensor 3a are different, and thus causes significant variation across the plurality of manufactured apparatuses 1. The result is that there are no predefined oscillating frequencies at which all sensors 3a associated with the plurality of fraud prevention apparatuses are known to correctly operate at and, as such, in the unlikely event that a fraudster were able to successfully overdrive or otherwise fraudulently manipulate a particular sensor 3a as previously described, the fraudster would not be able to fraudulently manipulate another sensor 3a in the same way because of the difference in operating frequencies between the sensors 3a.

The variation in component values, such as capacitor or resistor values, from one apparatus 1 to the next may be achieved by selecting the components for a particular apparatus 1 from one or more pools made up of components with a large number of different stated values (e.g. capacitances or resistances) and/or by using components which have wide tolerances.

An alternative to varying the component configuration of the oscillator circuit is for the controller 8 to cut power to the oscillator and to verify that the output signal of the sensor 3a reflects this as would be expected. If the output signal does not vary as expected, the controller 8 is configured to warn of a fraud attack on the apparatus 2 as previously described.

Figure 5 shows an example location of an optical sensor 3b, together with the oscillating sensor 3a described above, for detecting coins in the coin outlet path 5 of the payout apparatus 2. The optical sensor 3b comprises one or more optical emitters 13, such as one or more LEDs 13, and one or more optical detectors 14, such as one or more phototransistors 14. The optical emitters 13 are configured to emit light in the direction of the optical detectors 14 so that the emitted light is detected by the detectors 14 when the optical path between the emitters 13 and detectors 14 is not blocked.

The optical emitter(s) 13 and detector(s) 14 are located in the proximity of the coin exit path 5 in locations which cause coins travelling to the coin outlet 4 via the coin exit path 5 to block the optical path between the emitter(s) 13 and detector(s) 14. For example, an emitter 13 and a corresponding detector 14 in the optical path of the emitter 13 may be located on opposite sides of the coin exit path 5 or coin outlet 4.

The optical sensor 3b is communicatively coupled to the controller 8 of the fraud prevention apparatus 1 and the controller 8 is configured to monitor the status of the optical sensor 3b in order to detect coins being dispensed from the coin storage 6 to the coin outlet 4. More specifically, an output signal of the optical sensor 3b indicates to the controller 8 whether the optical path between the emitter(s) 13 and the detector(s) 14 referred to above is blocked. The output signal of the optical sensor 3b also indicates the time at which the optical path of the sensor 3b was blocked. For example, the output signal may indicate the times at which the blockage or interruption of the optical path of the sensor 3b begun and ended, and also the duration for which the optical path was blocked. A similar indication is also present in the output signal of the oscillating sensor 3a described above.

The oscillating sensor 3a and optical sensor 3b may be physically separated in the coin outlet path 5 by a predetermined distance so that a coin moving along the coin outlet path 5 to the coin outlet 4 is first detected by the oscillating sensor 3a and subsequently detected by the optical sensor 3b. It will be appreciated that the sensors 3a, 3b could alternatively be located such that the coin is first detected by the optical sensor 3b and subsequently by the oscillating sensor 3a.

The order in which the sensors 3a, 3b detect the coin allows the fraud prevention apparatus 1 to determine the direction in which coins are moving along the coin outlet path 5. For example, if a first detection is made by the sensor 3a which is located furthest from the coin outlet 4 and a subsequent second detection is made by the sensor 3b which is located closer to the coin outlet 4, the controller 8 may determine that an object has moved from the coin storage 6 to the coin outlet 4 as would be expected by the dispensation of coins. The order of detection also allows the apparatus 1 to determine the direction in which foreign objects, such as inductive fraudulent sensor manipulation devices, are moving in the coin path 5 and thus to identify a potential fraud attack by identifying an unexpected event.

If the order indicated by the sensors 3a, 3b is not as expected, for example because a comparison of the sensor output signals indicates that the sensor 3b which is located closer to the coin outlet 4 detected the object before the sensor 3a which is located further from the coin outlet 4, then the controller 8 may determine that an object has been inserted into the coin outlet path 5 from the exterior of the payout apparatus 2. Such a determination is indicative of a fraud attack, such as an attempt to insert a device to manipulate the oscillating frequency of the oscillating sensor 3a as described above, and may cause the controller 8 to generate the alarm signal referred to previously.

In addition to indicating the direction in which objects (e.g. coins) have moved along the coin outlet path 5, a comparison of the sensor output signals also allows the controller 8 to determine the time gap between the object being detected by the sensors 3a, 3b. The controller 8 may be configured to compare these measured time gaps with those which would be expected in normal operation of the apparatus 2. For example, the controller 8 may be configured to compare a measured time gap between an object first passing the oscillating sensor 3a and subsequently the optical sensor 3b with an expected time gap which is stored in a memory of the fraud prevention apparatus 1. The expected time gap may be derived from the expected speed of a coin in the coin outlet 5 under normal operating conditions and the known distance between the sensors 3a, 3b. Additionally or alternatively, the expected time gap may be based on configuration measurements made during manufacture of the apparatus 2.

A measured time gap which does not closely match the corresponding expected time gap stored in memory is indicative of a fraud attack on the payout apparatus 2 and may cause the controller 8 to generate the alarm signal referred to previously.

A method of preventing fraud, in accordance with the apparatus and operations described above, is detailed below in relation to figure 6.

In a first step S1, the controller 8 of the fraud prevention apparatus 1 is configured to detect a trigger event which indicates that the operating frequency of the oscillating sensor 3a should be changed. The trigger event may be the elapse of a predetermined time period since a previous event, or the detection or occurrence of a particular event as previously described. In a second step S2 of the method, the controller 8 is configured to cause the change in the operating frequency of the sensor 3a, for example by altering the configuration of the oscillator circuit. In a third step S3 of the method, the controller 8 of the fraud prevention apparatus 1 is configured to check whether the operating frequency of the sensor 3a has changed as expected and, if it has not, may be configured to cause a fraud alarm signal to be generated.

In a fourth step S4, in response to detection of an object in the coin outlet path 5 by one or both of the separately located coin sensors 3a, 3b, the controller 8 is configured to determine the direction in which the object has moved along the outlet path 5 by determining the order in which the object was detected by the sensors 3a, 3b. If the direction of travel is not as expected, the controller 8 may be configured to cause the fraud alarm signal to be generated.

In a fifth step S5 of the method, the controller 8 is configured to determine whether a measured time gap between the object being independently detected by the coin sensors 3a, 3b is as would be expected for a coin being dispensed from the coin storage 6 under normal operating conditions. If the time gap is not as expected, the controller 8 may be configured to cause the fraud alarm signal to be generated.

It will be appreciated that various modifications can be made to the implementation described above and shown in the figures without departing from the scope of the appended claims. For example, although the oscillator illustrated in the figures is for a Frequency Modulation (FM) sensor, the oscillating sensor 3a could alternatively comprise an FM and Amplitude Modulation (AM) sensor as an additional layer of security. In such an implementation, a demodulated AM signal would provide an analogue signal to the controller 8 which is responsible for causing changes in the expected oscillating frequency of the sensor 3a. The controller 8 would be configured to determine changes in the FM and AM signals output by the sensor 3a and to verify that the changes, for example from a default value, are in one direction only until a peak signal is received, followed by changes in the opposite direction, for example back to the default value. The peak values in the output signals may occur when the coin is centrally located in or adjacent the coin sensing element 7. Changes in signal direction which occur at an unexpected time, such as one which does not correspond to the peak signal deviation from the default value, may be indicative of a fraud attack.

The controller 8 may also be configured to determine the magnitude of the peak signal deviations and to verify that the magnitudes fall within expected limits, which may be stored in the memory 10.

A high Quality Factor circuit design ensures a relatively large variation in AM signal for a small change in the oscillating frequency of the sensor 3a and thus puts in place an extra variable that a would-be fraudster must attempt to manipulate when making a fraud attack. Such a design would also provide a high level of variation in the operational (e.g. frequency) characteristics of the sensor 3a for relatively small changes in component values, thus adding to the complexity and difficulty of successfully manipulating a plurality of sensors 3a in the same manner.

It will be appreciated that the embodiments and alternatives described above can be used either singly or in combination. It will also be appreciated that alternatives which are not explicitly discussed above are within the scope of the invention. For example, as briefly described, although the oscillator circuit is described above principally in relation to an LC oscillator, other types of oscillator could alternatively be used. The oscillating frequencies of such alternative oscillators can be varied by altering the component configuration of the oscillator in a similar manner to the LC examples. A specific example of an alternative oscillator is an RL or RC oscillator, in which a resistance value of the circuit is varied under the control of the controller 8 to cause a change in the oscillating frequency of the sensor 3a. Resistive components such as one or more resistors can be switched in and out of the circuit in a similar manner to capacitive components in order to alter the oscillating frequency. In particular, the verification operation for the oscillating sensor 3a may comprise altering the resistance of an RL or RC oscillator in the sensor 3a by a known amount and subsequently verifying that the oscillating frequency of the sensor 3a has changed as would be expected following the known change in resistance. The resistance may be altered by replacing, adding and/or removing resistive components to/from the oscillator circuit. In order to facilitate this, the sensor 3a may be selectively coupled to a plurality of resistors which can be selectively switched into and out of the oscillator by the controller 8, for example using one or more switches 12 as described previously or by applying control signals to the components from the controller 8.

It will also be appreciated that the specific components and component values illustrated in figures 2 to 4 can be replaced with alternative components and component values to achieve the same effects as the illustrated circuits.

Furthermore, as an alternative to switching components into or out of the oscillator, as described above, the controller 8 may be configured to adjust the values of variable components in the oscillator, such as one or more variable resistors, in order to alter the oscillating frequency of the sensor 3a.

Claims

1. A fraud prevention apparatus for a coin payout unit, comprising:

a coin sensor comprising an electrical oscillator for detecting coins in a coin outlet path; and

at least one controller configured to cause an expected change in an oscillating frequency of the sensor and to verify that the oscillating frequency has changed as expected.

2. An apparatus according to claim 1, wherein the controller is configured to cause the expected change in the oscillating frequency by altering a property of an oscillator circuit in the sensor.

3. An apparatus according to claim 1 or 2, wherein the controller is configured to cause the expected change in oscillating frequency by altering a component configuration of the sensor.

4. An apparatus according to claim 3, wherein altering the component configuration comprises altering the configuration of one or more timing elements in the sensor.

5. An apparatus according to claim 3 or 4, wherein altering the component configuration of the sensor comprises selectively adding at least one circuit component to the sensor.

6. An apparatus according to claim 3, 4 or 5, wherein altering the component configuration of the sensor comprises selectively removing at least one circuit component from the sensor.

7. An apparatus according to any of claims 3 to 6, wherein altering the component configuration of the sensor comprises selectively varying the operation of at least one circuit component in the sensor.

8. An apparatus according to any of claims 5 to 7, wherein the at least one circuit component comprises a capacitive component.

9. An apparatus according to any of claims 5 to 8, wherein the at least one circuit component comprises an electrical resistor.

10. An apparatus according to any of claims 5 to 9, wherein the at least one circuit component comprises an electrically inductive component.

11. An apparatus according to any of claims 5 to 10, wherein the at least one circuit component has a value in a predetermined wide tolerance range, such as wider than average.

12. An apparatus according to any preceding claim, wherein the controller is configured to verify that the oscillating frequency has changed as expected by determining an actual oscillating frequency of the sensor and comparing the actual frequency with an expected frequency.

13. An apparatus according to claim 12, wherein the controller is configured to determine the expected oscillating frequency from a component configuration of the sensor.

14. An apparatus according to claim 12 or 13, wherein the controller is configured to measure the actual oscillating frequency from an output signal of the sensor.

15. An apparatus according to any of claims 12 to 14, wherein the controller is configured to verify that the oscillating frequency has changed as expected by searching a measured frequency profile of the sensor for a match with an expected change.

16. An apparatus according to any preceding claim, wherein the controller is configured to determine an expected change in oscillating frequency from an actual change to a component configuration of the sensor.

17. An apparatus according to any preceding claim, wherein the controller is configured to cause the expected change in oscillating frequency and verify that the oscillating frequency has changed as expected in response to the elapse of a predetermined time period, the detection of a predetermined event or the occurrence of a randomly generated time event.

18. An apparatus according to any preceding claim, wherein if the controller determines that the oscillating frequency has not changed as expected, the controller is configured to respond by causing an alarm signal to the generated

19. An apparatus according to any preceding claim, wherein:

the sensor is configured to detect objects at a first location in a coin path of the payout apparatus;

a separate sensor is configured to detect objects at a second location in the coin path of the payout apparatus; and

at least one of the one or more controllers is configured to compare the detections at the first and second locations and verify whether a result of the comparison is as expected.

20. An apparatus according to claim 19, wherein the separate sensor is an optical sensor.

21. An apparatus according to claim 19 or 20, wherein the result of the comparison comprises a direction in which an object has moved in the coin path.

22. An apparatus according to any of claims 19 to 21, wherein the result of the comparison comprises a time gap between the detections at the first and second locations.

23. An apparatus according to any preceding claim, wherein the coin sensor comprises a coin sensing element whose electrical characteristics are affected by the electrical effect of a passing coin.

24. A coin payout unit comprising a fraud prevention apparatus according to any preceding claim.

25. A method of detecting fraud at a coin payout unit, comprising:

causing an expected change in an oscillating frequency of a coin sensor for detecting coins in the payout unit; and

verifying that the oscillating frequency has changed as expected.

26. A method according to claim 25, comprising causing the expected change in the oscillating frequency by altering a property of an oscillator circuit in the sensor.

27. A method according to claim 25 or 26, comprising causing the expected change in oscillating frequency by altering a component configuration of the sensor.

28. A method according to claim 27, wherein altering the component configuration comprises altering a configuration of at least one timing component in the sensor.

29. A method according to claim 27 or 28, wherein altering the component configuration of the sensor comprises selectively removing or adding at least one circuit component from or to the sensor.

30. A method according to any of claims 27 to 29, wherein altering the component configuration of the sensor comprises selectively varying the operation of at least one circuit component in the sensor.

31. A method according to claim 29 or 30, wherein the at least one circuit component has a value in a predetermined tolerance range which is wider than average.

32. A method according to any of claims 25 to 31, comprising verifying that the oscillating frequency has changed as expected by determining an actual oscillating frequency of the sensor and comparing the actual frequency with an expected frequency.

33. A method of manufacturing a plurality of fraud prevention apparatuses according to any of claims 1 to 23, comprising selecting wide tolerance circuit components for use in the sensors so as to cause different sensors to oscillate at different ranges of preset frequencies.

Application No:	GB1221504.2	**Examiner:**	Andrew Hole
Claims searched:	1 to 33	**Date of search:**	28 March 2013

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
A	-	GB 2023902 A (PRÜMM) Please see abstract and drawings.
A	-	US 5568854 A (HAYES et al.) Please see abstract and drawings.
A	-	US 2003/0217905 A1 (SPEAS et al.) Please see abstract and drawings.

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^{X} :

Worldwide search of patent documents classified in the following areas of the IPC

G07D; G07F

The following online and other databases have been used in the preparation of this search report

WPI, EPODOC, TXTE, TXTT, INSPEC, XPESP, XPESP2, XPIEE, XPIPCOM, XPI3E, XPMISC, XPLNCS, XPRD

International Classification:

Subclass	Subgroup	Valid From
G07F	0005/24	01/01/2006
G07D	0001/02	01/01/2006
G07D	0009/00	01/01/2006