US 20070279969A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2007/0279969 A1

Gabelich (43) Pub. Date: Dec. 6, 2007

(54) **INTRUSION DETECTION APPARATUS AND METHOD**

(75) Inventor: **Stephen A. Gabelich**, San Pedro, CA (US)

Correspondence Address:
RAYTHEON COMPANY, (EO/E04/N119)
Intellectual Property & Licensing
2000 East El Segundo Boulevard
P.O. Box 902
El Segundo, CA 90245-0902 (US)

(73) Assignee: **RAYTHEON COMPANY**

(21) Appl. No.: **11/446,534**

(22) Filed: **Jun. 2, 2006**

Publication Classification

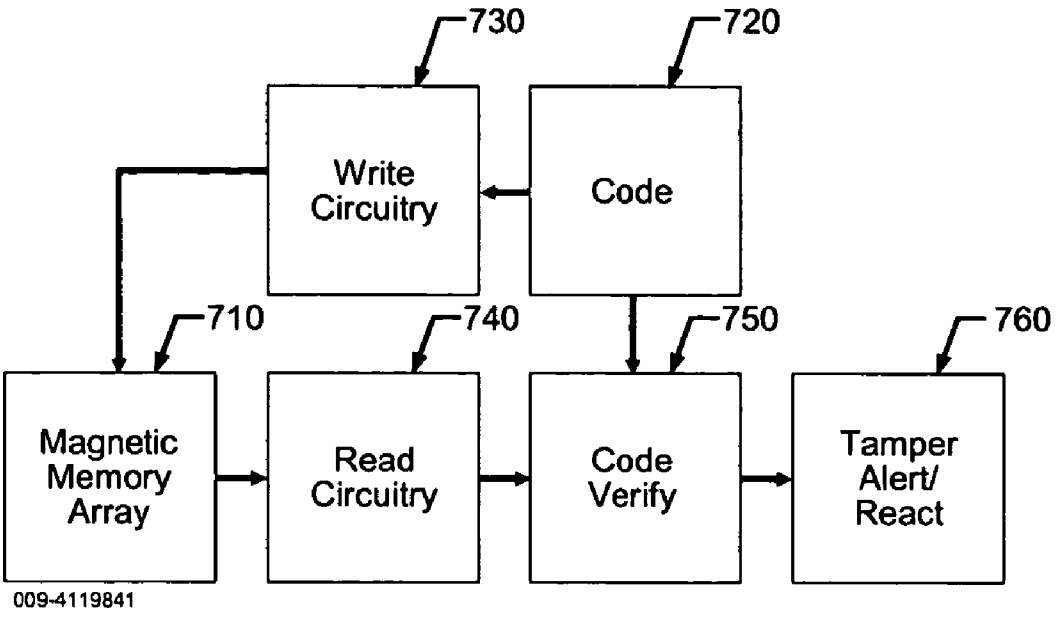
(51) **Int. Cl.**

G11C	*16/04*	(2006.01)
G11C	*11/34*	(2006.01)
G06F	*12/14*	(2006.01)
H04L	*9/32*	(2006.01)
G06F	*11/30*	(2006.01)

(52) **U.S. Cl.** **365/158**; 365/185.04; 713/193

(57) **ABSTRACT**

An apparatus and method to detect intrusion into a protected enclosure without requiring electrical power. The invention consists of an array of at least two magnetic memory elements, each of which has two electronically-readable stable states in the presence of a bias magnetic field, and a means for providing the required bias magnetic field. The magnetic memory elements and the means for providing the bias magnetic field are both located within a protected electronics enclosure and disposed such that any attempt to disassemble the enclosure will cause a change in the bias magnetic field and resultant permanent change to the content stored in the magnetic memory. Intrusion-detection functionality is initialized by electronically writing a binary code into the magnetic memory after the protected volume is completely assembled. Subsequent intrusion will automatically cause the initialization code to erase. The reaction to the detected intrusion may be an alarm or alert, or a reaction (such as erasing data or software) causing the protected equipment to lose functionality.



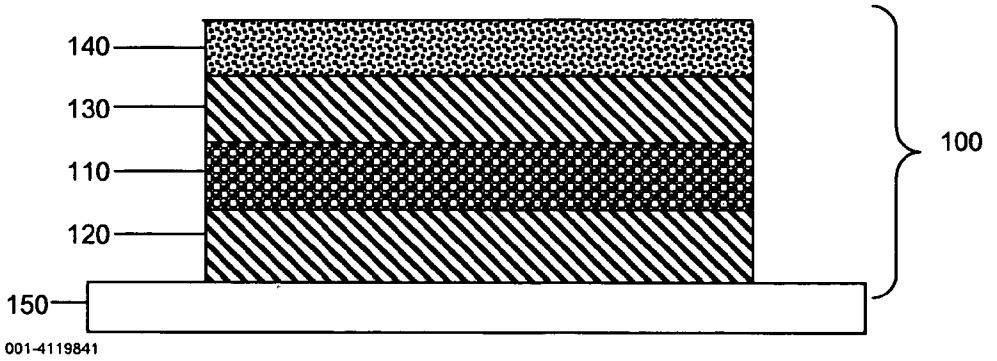


FIG 1. Prior Art

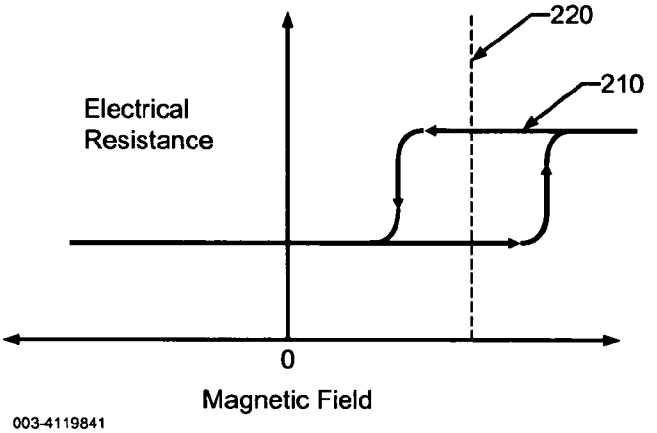


FIG. 2. Prior Art

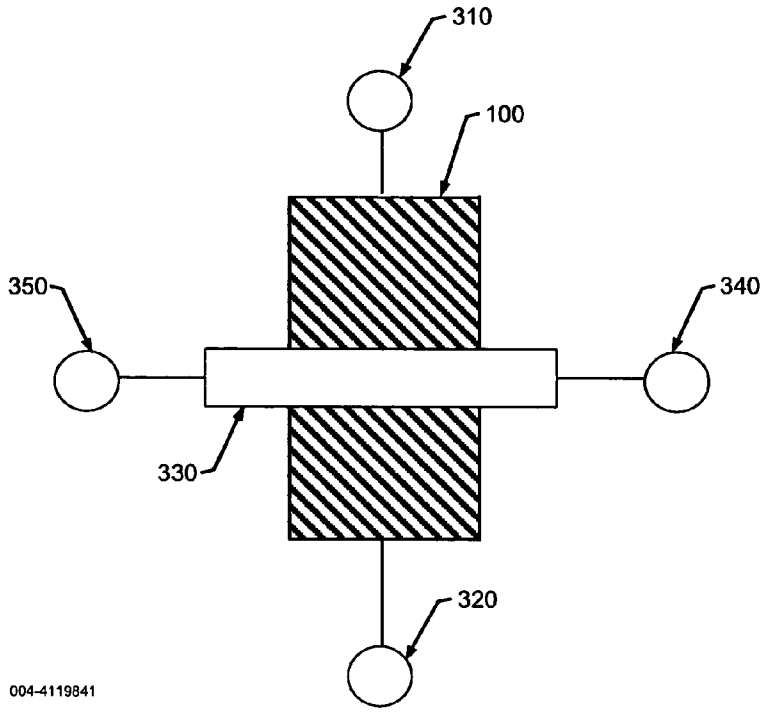


FIG. 3

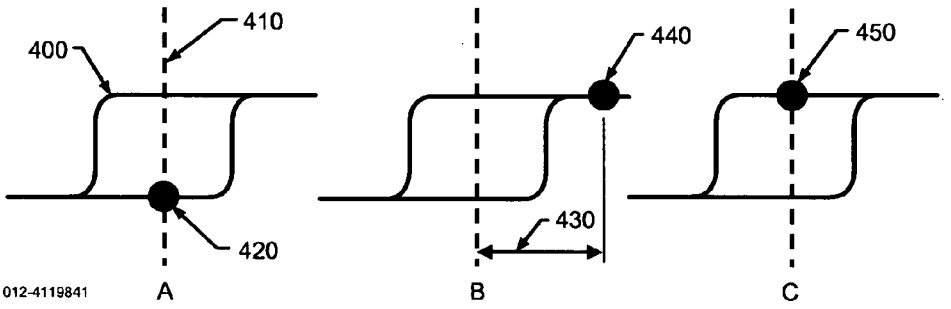


FIG. 4

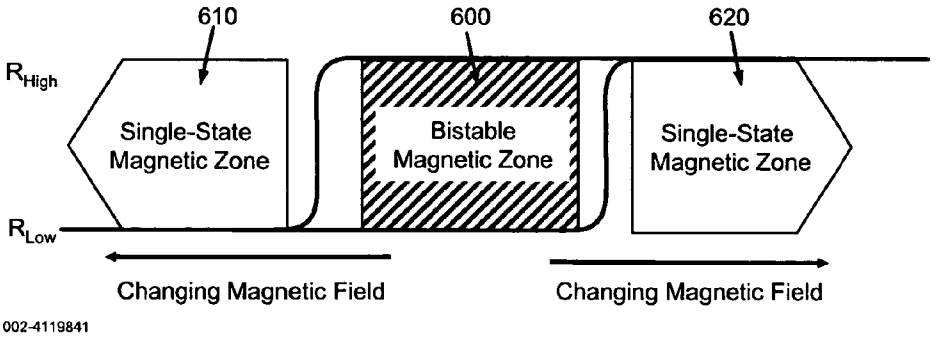


FIG. 5

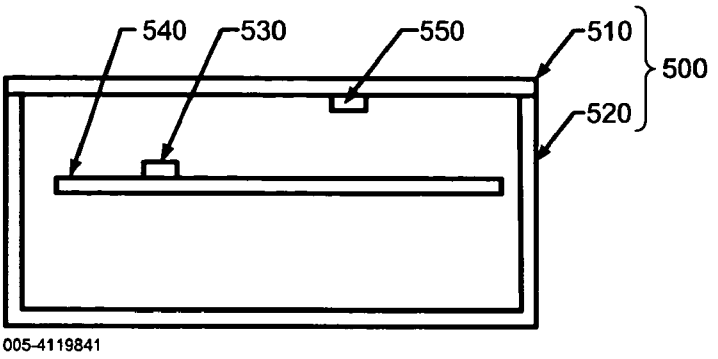


FIG. 6A

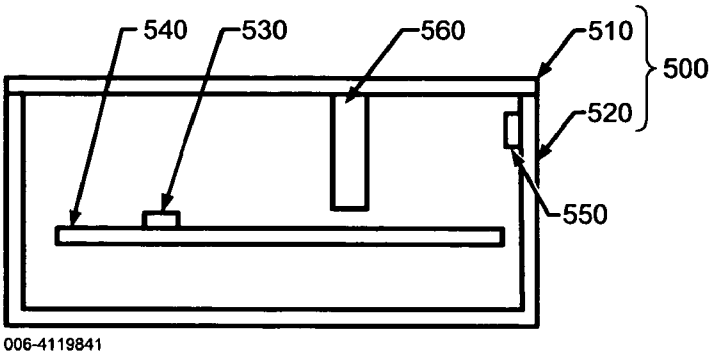


FIG. 6B

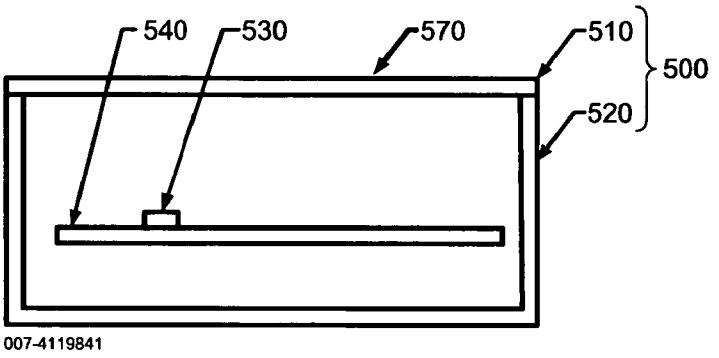


FIG. 6C

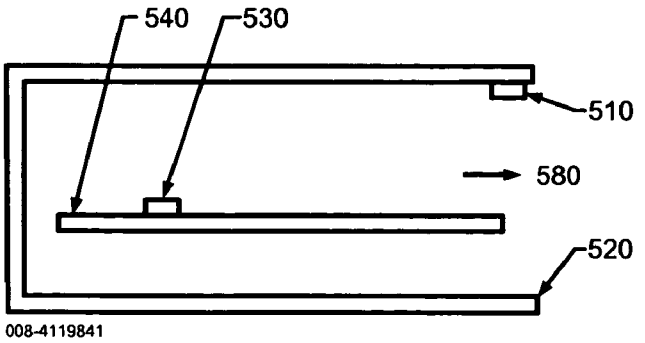


FIG. 6D

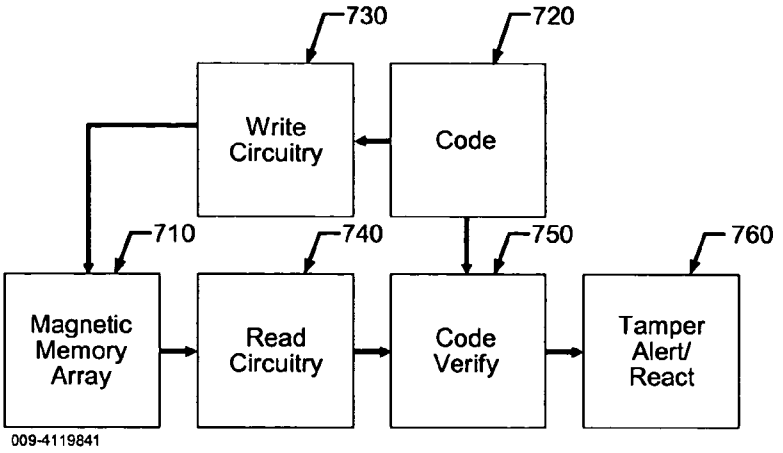


FIG. 7A

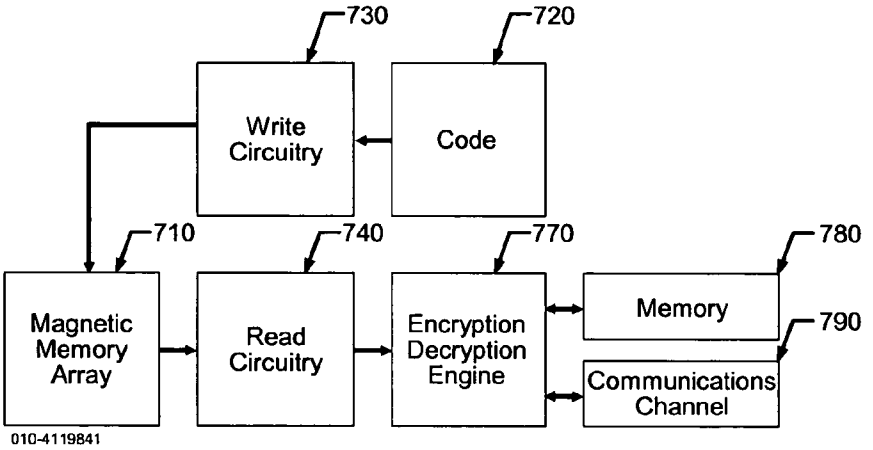


FIG. 7B

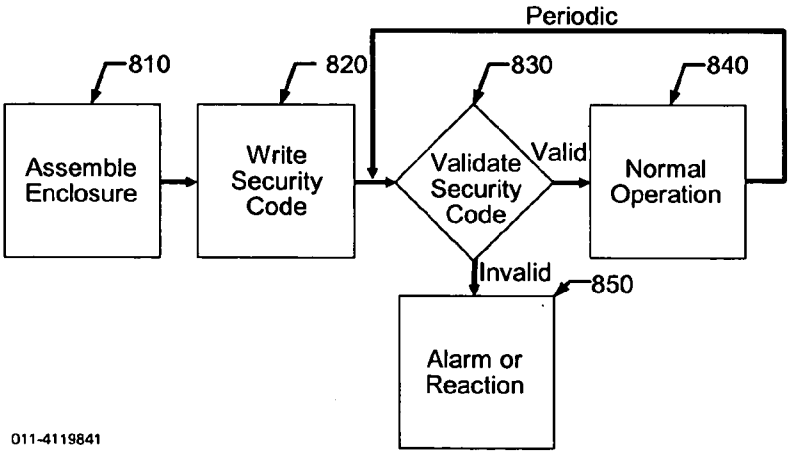


FIG. 8

INTRUSION DETECTION APPARATUS AND METHOD

[0001] This invention was made with government support. The government has certain rights in this invention.

BACKGROUND OF THE INVENTION

[0002] This invention relates to an apparatus to detect hardware intrusion into a protected enclosure without requiring electrical power.

[0003] There are numerous applications where it is desirable to be able to detect intrusion into a protected enclosure. The "intrusion" could be unauthorized opening, disassembly, or other attempt to gain access to the protected enclosure. The protected enclosure could contain, for example, proprietary hardware, security equipment, or fee collection or metering equipment. To provide protection to portable equipment or equipment without applied power (such as during storage or shipment), the intrusion detection means must also operate without electrical power. Thus there is a need for a cost-effective, reliable, digitally-compatible, non-reversible sensor that can detect intrusion without the need for battery or other electrical power. This invention satisfies all of these requirements.

SUMMARY OF THE INVENTION

[0004] A first embodiment of the invention consists of an array of at least two magnetic memory elements, each of which has two electronically-readable stable states in the presence of a bias magnetic field, and a means for providing the required bias magnetic field. The term "bias magnetic field" is intended to describe a magnetic field having a strength and direction within predetermined limits that will sustain the states of the magnetic memory elements. The predetermined limits on field strength may be centered about some finite value or may be centered about zero. In the latter case, the magnetic memory elements are configured to maintain two stable states in the absence of an applied magnetic field, and to change states if the applied magnetic field exceeds some threshold value.

[0005] The magnetic memory elements and the means for providing the bias magnetic field are both located within a protected electronics enclosure and disposed such that any attempt to disassemble the enclosure will cause a change in the bias magnetic field and resultant permanent change to the content stored in the magnetic memory.

[0006] Intrusion detection functionality is initialized by electronically writing a binary code into the magnetic memory after the protected volume is completely assembled. Subsequent disassembly will automatically cause the initialization code to erase. Attempted intrusion can be detected by comparing the memory content with the known value of the code at initialization. The reaction to the detected intrusion may be an alarm or alert, or a reaction (such as erasing data or software) causing the protected equipment to lose functionality.

[0007] In a preferred embodiment, the binary code stored in the magnetic memory at initialization is used as the key to encrypt or decrypt stored data or communications. In this case, loss of the encryption code due to attempted intrusion is sufficient to cause the protected equipment to lose functionality.

[0008] In a preferred embodiment of the invention, the magnetic memory is an array of spin-valve magnetoresistive sensor elements. Spin-valve sensors are described in U.S. Pat. No. 5,159,513 and have been extensively developed for use in read heads for magnetic disc memory devices.

[0009] In the case where a finite bias magnetic field is required to maintain the memory states, the means for providing the bias magnetic field will preferably be a small permanent magnet. The magnetic memory and the magnet must be mounted within the protected enclosure such that they physically move with respect to each other (in any direction) if the enclosure is non-destructively disassembled.

[0010] In the case where the magnetic memory is configured to maintain stable states in the absence of an applied magnetic field (i.e., the bias field strength limits are centered on zero), the protected enclosure is designed to shield the magnetic memory array from external or ambient magnetic fields. Disassembly causes the magnetic memory to be exposed to magnetic fields (e.g., the earth's magnetic field), resulting in changes to the memory content.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] FIG. **1** is a schematic cross-sectional view of a prior art spin-valve magnetic sensor.

[0012] FIG. **2** is a diagram of the electric resistance versus applied magnetic field for a prior art spin-valve magnetic sensor.

[0013] FIG. **3** is a schematic plan view of a prior art spin-valve magnetic memory element.

[0014] FIG. **4** is a diagram illustrating the method of changing the state of a spin-valve magnetic memory element.

[0015] FIG. **5** is a diagram illustrating the operation of the invention.

[0016] FIGS. **6**A, **6**B, **6**C, and **6**D are schematic cross-sectional views of embodiments of the invention.

[0017] FIGS. **7**A, **7**B are block diagrams of embodiments of the invention.

[0018] FIG. **8** is a flow chart of the process of using the invention.

DETAILED DESCRIPTION

[0019] FIG. **1** is a schematic cross-sectional view of an exemplary prior art spin-valve magnetic sensor suitable for use in the present invention. The magnetic sensor **100** is comprised of a number of layers deposited onto a substrate **150**. Two thin film magnetic layers **120**, **130** are separated by a non-magnetic layer **110**. In the traditional spin-valve device, the non-magnetic layer **110** is a metal such as copper. A similar magnetic sensor, commonly called a spin-tunneling device, is known to employ a dielectric layer **110** between the magnetic layers **120**, **130**. An additional layer of antiferromagnetic material **140** is deposited directly in contact with one of the magnetic layers. All of these layers are physically very thin and may be only a few 10's of angstroms in thickness.

[0020] It must be understood that the device illustrated in FIG. **1** is an example of a sensor suitable for use in the

invention. The asymmetric layer structure of this example device is typical of spin-valve devices configured for use with a non-zero bias magnetic field. Alternative magnetic sensor constructions are known, including an inverted device wherein the antiferromagnetic material is disposed between the lower magnetic film and the substrate. The use of additional magnetic or antiferromagnetic layers, deposited over or along side of the spin-valve device, is a known technique to tailor the characteristics of the spin valve. The characteristics of such devices may be tailored to include stable memory function with zero bias magnetic field.

[0021] The effect of the antiferromagnetic layer **140** is to "pin" the adjacent magnetic layer **130** such that the magnetization of layer **130** does not change in the presence of magnetic field (up to very high levels; thousands of Gauss), but instead always points in one direction along the long axis of the spin-valve device.

[0022] The other magnetic layer **120**, called the "free" layer, is not pinned, and the direction of magnetization of layer **120** can vary in the presence of a magnetic field. However, layer **120** will exhibit a natural tendency to become magnetized in either of two stable states with the direction of magnetization either parallel to and antiparallel to that of the "pinned" layer **130**.

[0023] The relative magnetization of the two magnetic layers **120**, **130** with respect to each other determines the resistance of the nonmagnetic layer **110**. When the magnetization of the free layer **120** points in the same direction as that of the pinned layer **130**, the electrical resistance of layer **110** is reduced. Conversely, when the magnetization of layers **120**, **130** are pointing in opposite directions, the electrical resistance of layer **110** is increased. Thus, in general, two stable resistance states are possible.

[0024] The degree of resistance change between states depends on the type of magnetic sensor and design parameters such as layer thicknesses. Spin-valve sensor devices typically exhibit a resistance change of approximately 5%, measured along the long axis of the nonmagnetic film **110**. Spin-tunneling devices are reported to exhibit resistance changes greater than 40%, measured across the thickness of the nonmagnetic film **110**.

[0025] FIG. **2** is a graph of the electric resistance versus applied magnetic field for a spin-valve magnetic sensor. The resistance versus magnetic field plot **210** exhibits the hysteresis typical of magnetic devices. However, because of the asymmetric structure of the spin-valve device, the hysteresis is centered about a bias magnetic field indicated by dashed line **220**. There are two stable values for the resistance in the presence of a suitable bias magnetic field, but only one value of resistance outside the suitable range of magnetic field. The combination of a spin-valve sensor and a means for providing a suitable bias magnetic field constitutes a magnetic memory element capable of "storing" one of two stable states that can be "read" by measuring the resistance of the conductive layer within the spin-valve device.

[0026] FIG. **3** is a schematic plan view of a prior art spin-valve magnetic memory element suitable for use in the invention. The spin-valve device **100** should be understood to be the top view of the stacked layers previously shown in cross-section in FIG. **1**. Terminals **310**, **320** connect to opposing ends of the non-magnetic layer **110** and can be used to measure the resistance of that layer. Terminals **340**, **350** connect to opposing ends of conductor **330**. Conductor **330** crosses over the spin-valve device **100** such that a sufficient electrical current passed through conductor **330** will create a magnetic field along the length of spin-valve **100** for the purpose of "writing" the state of the spin-valve memory. It should be understood that the memory element also comprises a means, not shown in FIG. **3**, for providing the bias magnetic field required to maintain two stable states of the spin-valve device. In an actual spin-valve memory, terminals **310**, **320**, **340**, **350** would be replaced by conductors connecting the circuitry required to read and write the memory content.

[0027] FIG. **4** is a diagram illustrating a method of changing the state of a spin-valve magnetic memory element. Curve **400** represents the hysteresis characteristic of the spin-valve device as previously discussed in conjunction with FIG. **2**. In FIG. **4**A, the spin-valve is in the low resistance state as indicated by point **420**. This state is maintained by the presence of the bias magnetic field with a field strength indicated by dashed line **410**. In FIG. **4**B, the magnetic field has been changed by an amount indicated by arrow **430**. This changed magnetic field has driven the spin valve to its high resistance state as indicated by point **440**. In FIG. **4**C, the magnetic field has been restored to the original value and the spin valve is maintained in the high resistance state as indicated by point **450**. The spin valve can be "written" back to the low resistance state by changing the magnetic field in the opposing direction to the field used to write the high resistance state.

[0028] FIG. **3** and FIG. **4** are representative examples of the structure and operation of a magnetic memory element suitable for use in the invention. Magnetic memory elements and magnetic random access memories (MRAM) are well known in the art. U.S. Pat. No. 5,949,707, U.S. Pat. No. 5,966,322, U.S. Pat. No. 6,021,065, U.S. Pat. No. 6,275,411, and U.S. Pat. No. 6,349,053 all describe memory elements using spin-valve (or giant magneto restrictive effect) or spin-tunneling devices. Any magnetic memory device may be suitable for use in the invention so long as the device exhibits two stable states in the presence of a magnetic field having strength and direction falling within predetermined, finite, controllable limits.

[0029] The invention leverages the magnetic memory element's hysteretic behavior. The interrelationship between a magnetic memory element's magnetic field surroundings (external magnetic field parameters at any given moment in time) and its electrical resistance (and the number of resistance values possible) is illustrated in FIG. **5**.

[0030] In essence, the magnetic memory element's hysteresis notionally divides the magnetic field range into three zones: two single-state conditions **610**, **620** and one "bistable" zone **600**. The suitable zone represents the design level for the bias magnetic field plus margin for magnetic variations; two stable binary resistance values are possible in this zone. The field strength in the "bistable" zone may be centered about zero, or may be centered on a predetermined non-zero value. The single-state zones represent the external magnetic field direction and strength caused by intrusion events; one and only one resistance value is possible in each of these zones.

[0031] In practice, an intrusion detection sensor will contain a minimum of two magnetic memory elements. Upon

hardware initialization, predetermined resistance values can be written to individual spin valves to store a binary resistance security code or encryption key. In the case where the memory has only two elements and can only store two binary bits, the possible useful security code values are 01 and 10 (either the high or low resistance states can be arbitrarily defined as binary 0). This code will persist if, and only if, the applied magnetic field for all spin valves is maintained in the bistable zone. If at any time the applied magnetic field changes into either of the single-state zones, the security code is erased (either all "0s" or all "1s" depending on which of the two intrusion zones was applied last). The change in the stored security code will occur whether or not power is applied.

[0032] FIG. **6**A is a schematic cross-sectional view of an exemplary embodiment of the invention. Enclosure **500**, comprised of a box **520** and a cover **510**, encloses electronic equipment **540**, which must be protected from intrusion or unauthorized access. Magnetic memory array **530**, comprised of two or more spin-valve or other magnetic memory elements, is disposed within the enclosure as part of electronic equipment **540**. A means for providing a magnetic field **550**, such as a permanent magnet, is disposed on and permanently attached to the cover **510**. The means for providing a magnetic field **550** is designed and positioned to create the desired bias magnetic field (required for magnetic memory operation) at the magnetic memory array **530**. Thus the magnetic memory array **530** can stably store a security code so long as the cover **510** is in place and the magnetic field at the memory array is within the bistable zone. Any motion of the cover **510** with respect to the memory array **530** (such as would occur during disassembly of enclosure **500**) will change the magnetic field at the memory array into either of the "single-state" zones and permanently erase the security code stored therein.

[0033] FIGS. **6**B, **6**C, **6**D are schematic cross-sectional views of additional exemplary embodiments of the invention. Like elements have the same reference designators used in FIG. **6**A.

[0034] In FIG. **6**B, a magnetic shield **560** attached to cover **510** is disposed between the magnetic memory array **530** and magnet **550**. Removing cover **510** displaces the shield **560**, changing the magnetic field at memory array **530** and thus changing the security code stored therein.

[0035] In FIG. **6**C, the magnetic memory array **530** is adapted to stably store a security code in the absence of a magnetic field, and cover **510** and box **520** are constructed of a magnetic shielding material. Removing cover **510** exposes the magnetic memory array **530** to environmental magnetic fields, depicted by arrow **570**, thus changing the security code stored in the magnetic memory array.

[0036] In FIG. **6**D, electronic equipment **540** bearing magnetic memory array **530** is disposed within box **520** and can only be removed by motion in the direction indicated by the arrow **580**. Electronic equipment **540** could be a circuit card or module conventionally mounted in card guides. Removing electronic equipment **540** in direction **580** causes the magnetic memory array **530** to pass in proximity to magnetic **550**, thus changing the content stored in memory array **530**.

[0037] It should be understood that FIGS. **6**A, **6**B, **6**C, and **6**D illustrate simplistic embodiments of the invention and that many variations are possible within the scope of the invention. The magnetic memory array and the means for providing a magnetic field may be disposed anywhere within the enclosure so long as attempted intrusion results in relative motion between these elements. This relative motion could be caused by removing a cover, opening a drawer or door, or sliding a circuit module from a rack. Additionally, multiple memory arrays, magnets, or shields could be disposed such that intrusion is detected by relative motion of at least one memory array with respect to at least one magnet or one shield.

[0038] FIG. **7**A is a block diagram of a further embodiment of the invention, which is comprised of a magnetic memory array **710** including means (not illustrated) for establishing a suitable bias magnetic field, circuitry for writing **730** and reading **740** the magnetic memory content, means for establishing **720** and verifying **750** a security code, and means **760** for reacting to an intrusion event if detected. The security code can be established by a variety of means **720**, including permanently storing the code in a memory, generating the code through some random process, or acquiring the code from an external source via a secure datalink. Once the code is established, the write circuitry **730** copies the code into magnetic memory array **710** by sending pulses of electrical current through the write conductors of the magnetic memory elements. Note that the code can only be written into the magnetic memory array in the presence of the appropriate bias magnetic field. So long as the bias magnetic field is maintained, the security code is stored in magnetic memory **710** and can be read by read electronics **740**. In typical applications, the code will be read periodically and verified by comparison with the pre-established security code. Any change in the code will activate the means **760** for reacting to the intrusion event, which may range from a simple alarm to self-destruction of the functionality of the protected equipment (by means of erasure of internal firmware, for example).

[0039] While read circuitry **740** will most likely be located in the immediate proximity of magnetic memory array **710**, the other elements shown in FIG. **7** do not need to be located within the protected enclosure. For example, the write circuitry could be external to the enclosure and connected to the magnetic memory array only temporarily to write the security code after the enclosure is assembled. Any or all of the means for establishing the security code **720**, the means for verifying the code **750**, and the means for reacting to an intrusion event **760** could be located within the protected enclosure or could be external to the protected enclosure and connected by a secure data link.

[0040] FIG. **7**B is a block diagram of a preferred embodiment of the invention. As previously described, means **720** establish a security code that is stored in magnetic memory array **710** by write circuitry **730**. The stored security code is read from magnetic memory array **710** by read circuitry **740** and provided to encryption/decryption engine **770**. Encryption/decryption engine **770** uses the security code as an encryption key to encrypt or decrypt information to be stored in or read from memory **780**, or information to be transmitted or received via communications channel **790**. Requiring the read circuitry **740** to read the content of magnetic memory **710** every time an encryption or decryp-

tion operation is performed will ensure that loss of the magnetic memory content causes immediate loss of function of the protected equipment.

[0041] FIG. **8** illustrates the process of using the invention. After the enclosure is assembled at step **810**, the security code is written into the magnetic memory array at step **820**. The code read from the memory is validated at step **830**. The step of validating the security code may be accomplished by comparing the code to a known value, or by using the code to decrypt data previously encrypted using the same code. The protected electronic equipment operates normally **840** if the security code is valid, and reacts in some predetermined manner **850** if the code is invalid. The security code is revalidated periodically, either at fixed time intervals, every time an encryption or decryption operation is performed, or after some event, such as every time power is applied to the protected electronics.

Claims:

1. An apparatus for detecting attempted intrusion into a protected enclosure, comprising:

a magnetic memory array comprising at least two magnetic memory elements, each adapted to store a binary value only in the presence of a bias magnetic field having a magnetic field strength and direction within predetermined limits; and

means for providing said bias magnetic field.

2. The apparatus of claim 1, wherein said magnetic memory array and said means for providing said bias magnetic field are disposed such that any attempt to intrude into said enclosure alters said bias magnetic field sufficiently to change at least one of the binary values stored in said memory array.

3. The apparatus of claim 1, wherein said magnetic memory elements comprise spin-valve devices.

4. The apparatus of claim 1, wherein said magnetic memory elements comprise spin-tunneling devices.

5. The apparatus of claim 1, wherein said means for providing said bias magnetic field comprises at least one permanent magnet.

6. The apparatus of claim 5, wherein said means for providing said bias magnetic field comprises a plurality of permanent magnets.

7. The apparatus of claim 5, wherein said magnetic memory array and said at least one permanent magnet are disposed such that any attempt to intrude into said enclosure causes relative motion between said magnetic memory array and at least one permanent magnet.

8. The apparatus of claim 1, wherein said means for providing said bias magnetic field comprises at least one magnetic shielding element.

9. The apparatus of claim 9, wherein said magnetic memory array and said at least one magnetic shielding element are disposed such that any attempt to intrude into said enclosure causes relative motion between said magnetic memory and at least one magnetic shielding element.

10. The apparatus of claim 1, further comprising:

means for storing a code in said magnetic memory array; and

means for reading said stored code.

11. The apparatus of claim 10, further comprising:

means to use said code as an encryption key.

12. A method for detecting attempted intrusion into a protected enclosure, comprising:

providing a magnetic memory array disposed within said protected enclosure, said magnetic memory array operable to store a binary number of at least two bits in the presence of a bias magnetic field having magnetic field strength and direction within predetermined limits; and

providing said bias magnetic field at said magnetic memory array;

wherein said magnetic memory array is disposed within said enclosure such that any attempt to intrude into said enclosure alters the magnetic field at said memory array sufficiently to change the state of at least one bit of said binary number.

13. The method of claim 12, further comprising:

storing a predetermined binary number into said magnetic memory array after said enclosure is assembled; and

comparing the binary number stored in said array with said predetermined binary number to determine if attempted intrusion has occurred.

14. The method of claim 12, further comprising:

storing a binary number into said magnetic memory array after said enclosure is assembled;

periodically reading the binary number stored in said magnetic memory array; and

using the binary number read from said magnetic memory array as an encryption/decryption key.

15. The method of claim 14, wherein the step of reading the binary number stored in said magnetic memory array is performed every time the encryption/decryption key is used.

* * * * *