US 20160197899A1

(19) **United States**

(12) **Patent Application Publication**

(10) **Pub. No.: US 2016/0197899 A1**

(43) **Pub. Date: Jul. 7, 2016**

Liu et al.

(54) **METHOD OF DYNAMICALLY ENCRYPTING FINGERPRINT DATA AND RELATED FINGERPRINT SENSOR**

(71) Applicant: **eMemory Technology Inc.**, Hsin-Chu (TW)

(72) Inventors: **Hsin-Chou Liu**, Kaohsiung City (TW); **Hung-Hsiang Wang**, Hsinchu County (TW)

(21) Appl. No.: **14/989,777**

(22) Filed: **Jan. 6, 2016**

Related U.S. Application Data

(60) Provisional application No. 62/100,485, filed on Jan. 7, 2015.

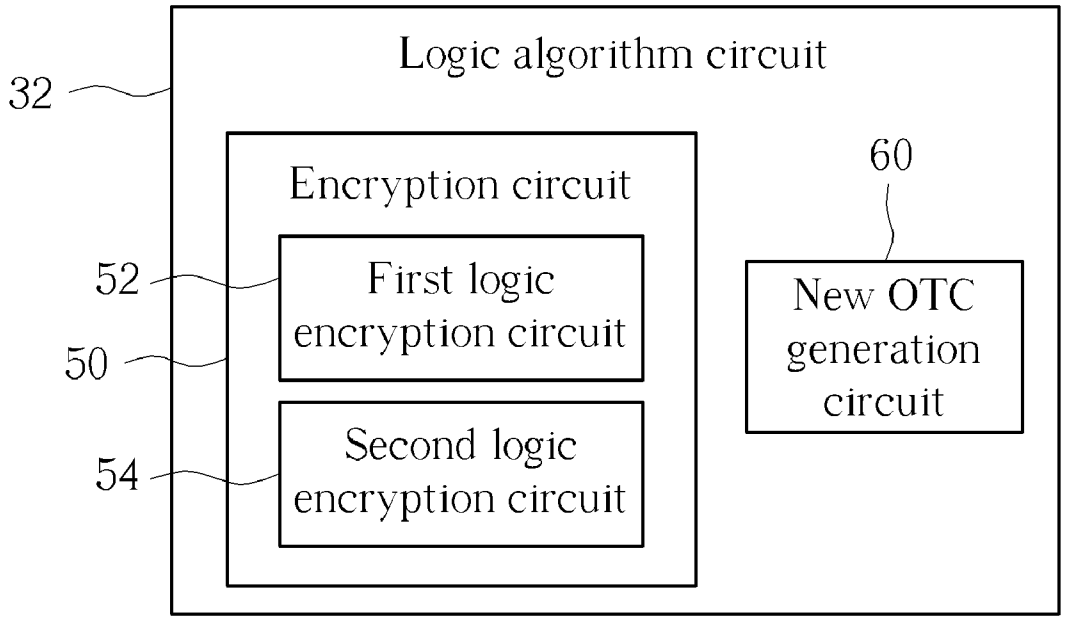
Publication Classification

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/0457*** (2013.01); ***H04L 63/0861*** (2013.01)

(57) **ABSTRACT**

A dynamic encryption type fingerprint sensor includes a capacitive array sensing fingerprints and producing fingerprint data, an embedded non-volatile memory (eNVM) storing a one-time code (OTC) and an encryption algorithm indicator, and a logic algorithm circuit encrypting the fingerprint data produced by the capacitive array according to the OTC and the encryption algorithm indicator. The logic algorithm circuit includes an encryption circuit having a plurality of logic encryption circuits selected using the encryption algorithm indicator, the encryption circuit encrypting the fingerprint data using selected logic encryption circuits of the plurality of logic encryption circuits according to the OTC. A control circuit is used for controlling operation of the capacitive array, the eNVM, and the logic algorithm circuit.



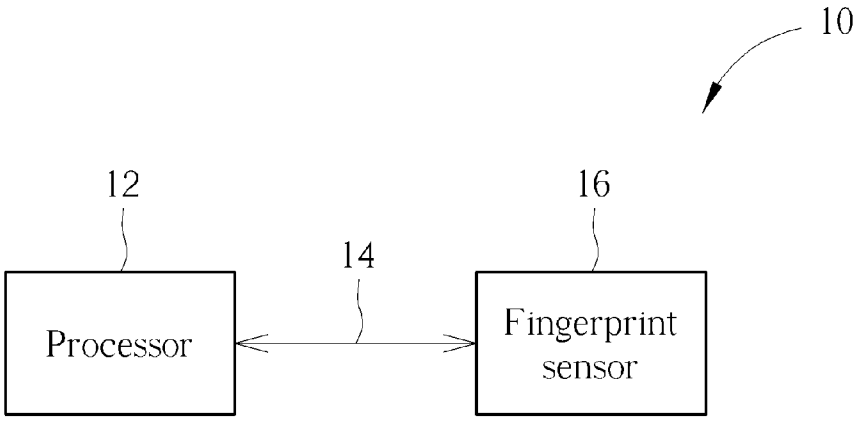


FIG. 1 PRIOR ART

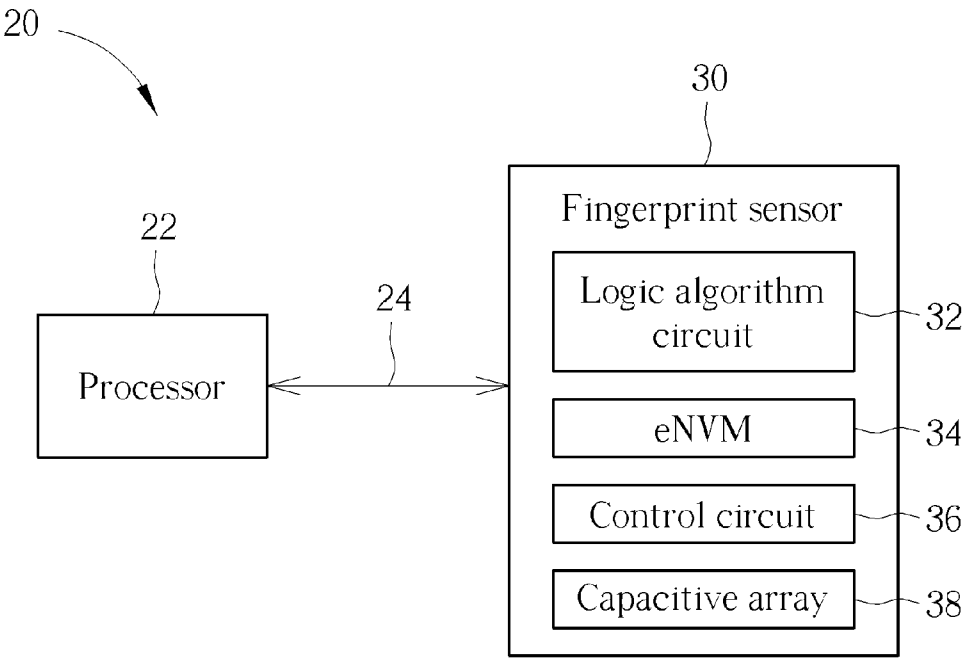


FIG. 2

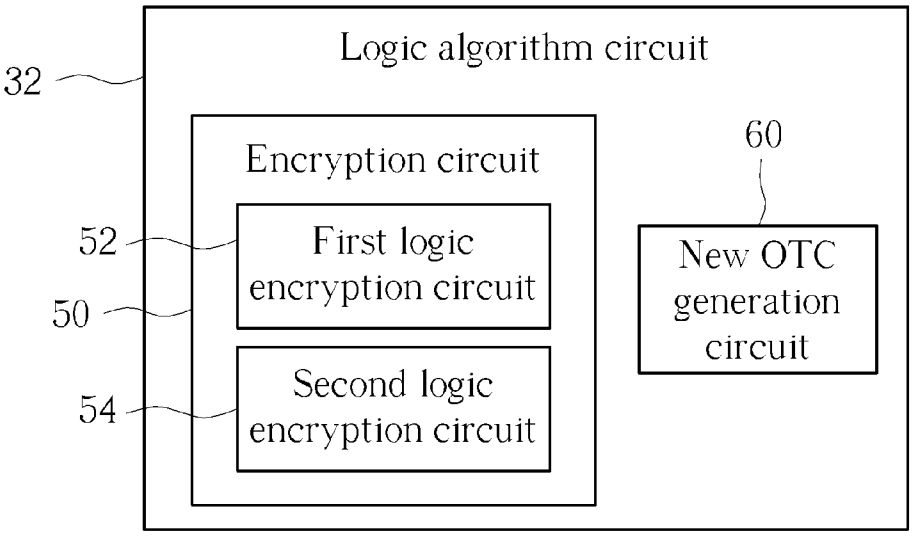

Logic algorithm circuit
32
Encryption circuit
52
First logic encryption circuit
50
54
Second logic encryption circuit
60
New OTC generation circuit

FIG. 3

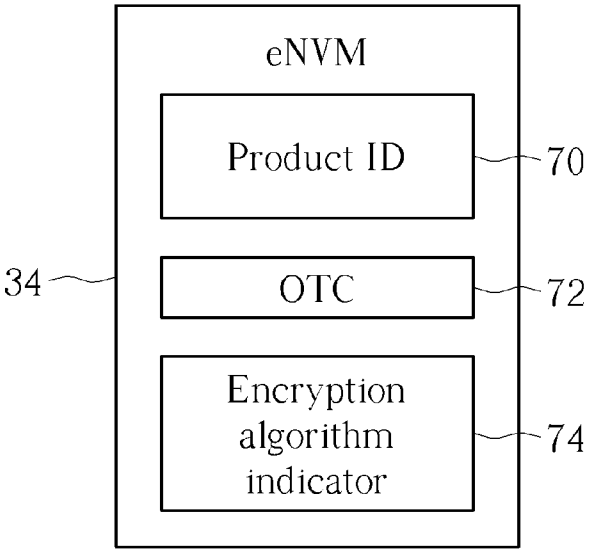

eNVM
Product ID
70
34
OTC
72
Encryption algorithm indicator
74

FIG. 4

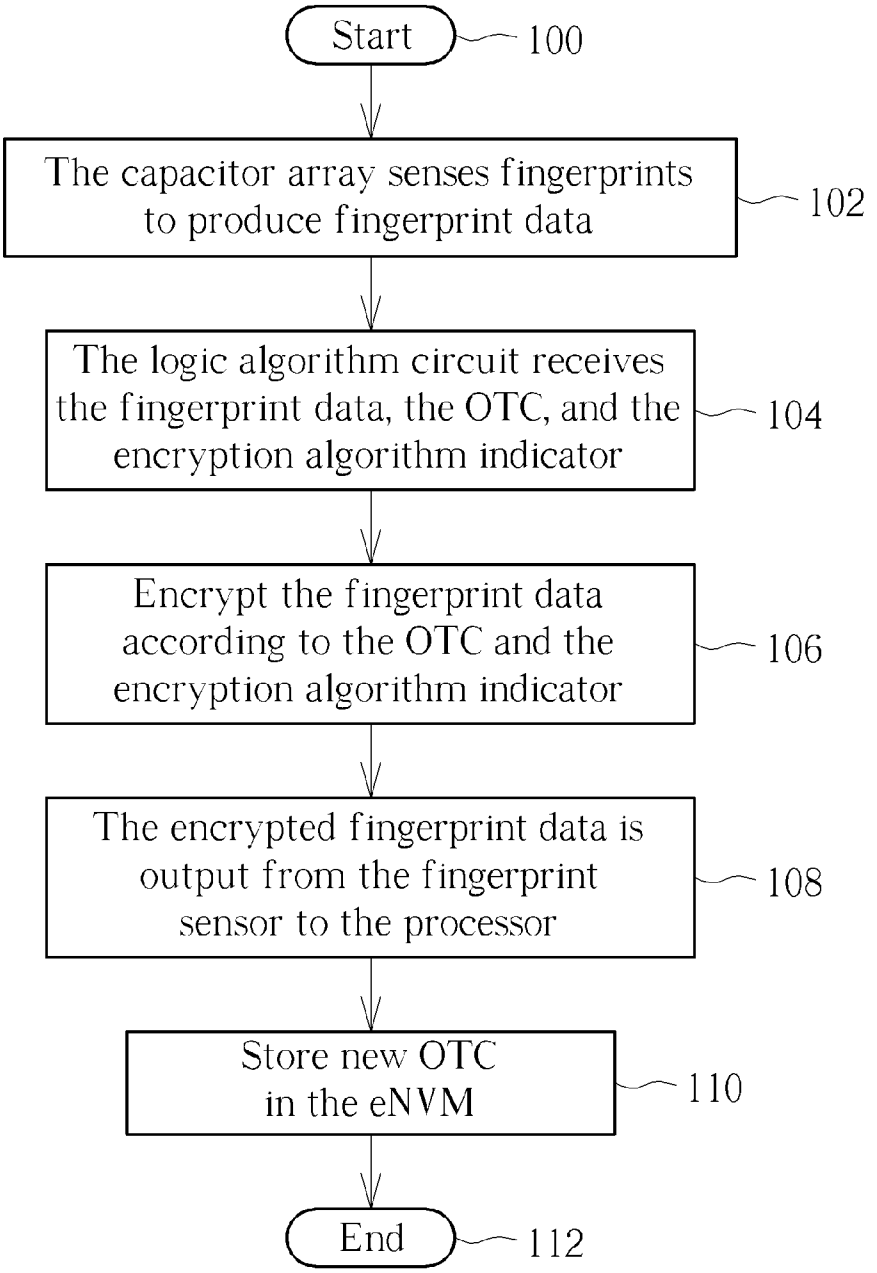

Start
100
The capacitor array senses fingerprints to produce fingerprint data
102
The logic algorithm circuit receives the fingerprint data, the OTC, and the encryption algorithm indicator
104
Encrypt the fingerprint data according to the OTC and the encryption algorithm indicator
106
The encrypted fingerprint data is output from the fingerprint sensor to the processor
108
Store new OTC in the eNVM
110
End
112

FIG. 5

METHOD OF DYNAMICALLY ENCRYPTING FINGERPRINT DATA AND RELATED FINGERPRINT SENSOR

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Application No. 62/100,485, filed on Jan. 7, 2015. The above-mentioned application is hereby incorporated by reference.

BACKGROUND OF THE INVENTION

[0002] 1. Field of the Invention

[0003] The invention relates to a fingerprint sensor, and more particularly, to a fingerprint sensor that dynamically selects an encryption type and encrypts fingerprint data using a one-time code (OTC).

[0004] 2. Description of the Prior Art

[0005] Fingerprint sensors are used to sense fingerprint data and send the fingerprint to a processor, such as an application processor or a microcontroller unit (MCU). Currently the way that sensed fingerprint data is transferred from the fingerprint sensor to the processor cannot safely protect the fingerprint data from being read and misused by unauthorized parties.

[0006] Please refer to FIG. **1**. FIG. **1** is a functional block diagram showing a system **10** for processing fingerprints according to the prior art. The system **10** comprises a processor **12** in communication with a fingerprint sensor **16** via a transmission path **14**. When fingerprint data is being transferred between the fingerprint sensor **16** and the processor **12** along the transmission path **14**, the fingerprint data can be recorded using either software or hardware. Then, the next time the processor **12** requests fingerprint data from the fingerprint sensor **16** for verification, an unauthorized party only needs to transmit on the transmission path **14** exactly the same data that was recorded previously. Using this method, one can easily falsify fingerprint verification since the fingerprint data can easily be recorded along the transmission path **14**. One does not even need to know the content of each data transmission between the processor **12** and the fingerprint sensor **16** in order to successfully falsify the fingerprint verification. Even if the fingerprint data was encrypted before being sent from the fingerprint sensor **16** to the processor **12**, the encrypted fingerprint data can still be recorded and falsified if the encryption key is not changed frequently.

SUMMARY OF THE INVENTION

[0007] It is therefore one of the primary objectives of the claimed invention to provide a dynamic encryption method for fingerprint data in order to protect the fingerprint data from unauthorized parties. The dynamic encryption method can be integrated into a fingerprint sensor for conveniently encrypting fingerprint data sensed by the fingerprint sensor.

[0008] According to an exemplary embodiment of the claimed invention, a dynamic encryption type fingerprint sensor is disclosed. The dynamic encryption type fingerprint sensor includes a capacitive array sensing fingerprints and producing fingerprint data, an embedded non-volatile memory (eNVM) storing a one-time code (OTC) and an encryption algorithm indicator, and a logic algorithm circuit encrypting the fingerprint data produced by the capacitive array according to the OTC and the encryption algorithm indicator. The logic algorithm circuit comprises an encryption circuit comprising a plurality of logic encryption circuits selected using the encryption algorithm indicator, the encryption circuit encrypting the fingerprint data using selected logic encryption circuits of the plurality of logic encryption circuits according to the OTC. A control circuit is used for controlling operation of the capacitive array, the eNVM, and the logic algorithm circuit.

[0009] According to another exemplary embodiment of the claimed invention, a method of dynamically encrypting fingerprint data with a fingerprint sensor is disclosed. The method includes sensing fingerprints with a capacitive array of the fingerprint sensor and producing corresponding fingerprint data, receiving an encryption algorithm indicator and a one-time code (OTC) , selecting one or more logic encryption circuits of a plurality of logic encryption circuits using the encryption algorithm indicator, and encrypting the fingerprint data produced by the capacitive array with the one or more selected logic encryption circuits according to the OTC.

[0010] It is an advantage that the present invention provides a way to dynamically select an encryption type that is used to encrypt fingerprint data using the OTC. This encryption method provides two layers of protection. First, using the OTC for encryption makes it harder for an unauthorized party to decrypt the fingerprint data. Second, dynamically selecting the logic encryption circuits using the encryption algorithm indicator for performing the encryption also adds a second layer of protection. One would have to know both the OTC and the selected logic encryption circuits that were used for encrypting the fingerprint data in order to decrypt the corresponding encrypted fingerprint data.

[0011] These and other objectives of the present invention will no doubt become obvious to those of ordinary skill in the art after reading the following detailed description of the preferred embodiment that is illustrated in the various figures and drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] FIG. **1** is a functional block diagram showing a system for processing fingerprints according to the prior art.

[0013] FIG. **2** is a functional block diagram showing a system for processing fingerprints according to the present invention.

[0014] FIG. **3** is a functional block diagram showing details of the logic algorithm circuit of the present invention.

[0015] FIG. **4** is a functional block diagram showing details of the eNVM of the present invention.

[0016] FIG. **5** is a flowchart describing the method of encrypting fingerprint data using the fingerprint sensor of the present invention.

DETAILED DESCRIPTION

[0017] The present invention seeks to encrypt fingerprint data in a manner that provides solid protection and prevents the encrypted fingerprint data from being viewed by unauthorized parties.

[0018] Please refer to FIG. **2**. FIG. **2** is a functional block diagram showing a system **20** for processing fingerprints according to the present invention. The system **20** comprises a processor **22** in communication with a fingerprint sensor **30** via a transmission path **24**. The fingerprint sensor **30** comprises a logic algorithm circuit **32**, an embedded non-volatile memory (eNVM) **34**, a control circuit **36** for controlling

operation of the fingerprint sensor **30**, and a capacitive array **38** for sensing fingerprints and producing fingerprint data. The fingerprint data produced by the capacitive array **38** will vary depending on where the fingerprint is located on the capacitive array **38**.

[0019] Please refer to FIG. **3**. FIG. **3** is a functional block diagram showing details of the logic algorithm circuit **32** of the present invention. The logic algorithm circuit **32** comprises both an encryption circuit **50** and a new one-time code (OTC) generation circuit **60**. The encryption circuit **50** comprises a plurality of logic encryption circuits including a first logic encryption circuit **52** and a second logic encryption circuit **54**. The number of logic encryption circuits **52**, **54** included in the encryption circuit **50** should be at least two, and may contain any number of logic encryption circuits **52**, **54** greater than two. One or a combination of multiple logic encryption circuits **52**, **54** may be used for encrypting fingerprint data, as will be explained in greater detail below. The new OTC generation circuit **60** is used for generating an initial OTC and for generating an updated OTC after a previous OTC has been used. The logic algorithm circuit **32** can be built using simple logic gates, and does not need to be a general purpose processor or MCU.

[0020] Please refer to FIG. **4**. FIG. **4** is a functional block diagram showing details of the eNVM **34** of the present invention. The eNVM **34** stores a product identification **70** for identifying the particular model of the fingerprint sensor **30**, stores the OTC **72**, and stores an encryption algorithm indicator **74**. The encryption algorithm indicator **74** is used for indicating which of the logic encryption circuits **52**, **54** should be used for encrypting the fingerprint sensor **30** while using the OTC **72** as a key for the encryption. The encryption algorithm indicator **74** may indicate that the first logic encryption circuit **52**, the second logic encryption circuit **54**, or a combination of the first logic encryption circuit **52** and second logic encryption circuit **54** should be used for encrypting the fingerprint data. If more than two logic encryption circuits are contained in the encryption circuit **50**, then there will be more possibilities for the logic encryption circuits that can be used for encrypting the fingerprint data.

[0021] Please note that the processor **22** will also need to store its own identical copy of both the OTC **72** and the encryption algorithm indicator **74** that are stored in the eNVM **34**. That is, in order for the processor **22** to be able to decrypt the encrypted fingerprint data received from the fingerprint sensor **30** along the transmission path **24**, the processor **22** will need to have the same OTC **72** and encryption algorithm indicator **74** for being able to successfully perform decryption. In an embodiment, the processor can provide the OTC **72** to the fingerprint sensor **30** instead of the new OTC generation circuit **60** being used for generating a new OTC **72** to replace the previous OTC **72**. The OTC **72** can either be encrypted or non-encrypted when it is stored in the eNVM **34** or when it is received from the processor **22**.

[0022] Please refer to FIG. **5**. FIG. **5** is a flowchart describing the method of encrypting fingerprint data using the fingerprint sensor **30** of the present invention. Steps in the flowchart will be explained as follows.

[0023] Step **100**: Start.

[0024] Step **102**: The capacitive array **38** of the fingerprint sensor **30** senses fingerprints to produce fingerprint data.

[0025] Step **104**: The capacitive array **38** supplies the fingerprint data to the logic algorithm circuit **32**, and the eNVM **34** supplies both the OTC **72** and the encryption algorithm indicator **74** to the logic algorithm circuit **32**.

[0026] Step **106**: The encryption circuit **50** of the logic algorithm circuit **32** encrypts the fingerprint data according to the OTC **72** and the encryption algorithm indicator **74**. The encryption circuit **50** selects one or more logic encryption circuits **52**, **54** according to the encryption algorithm indicator **74** and uses the selected logic encryption circuits **52**, **54** for encrypting the fingerprint data according to the OTC **72**.

[0027] Step **108**: The encrypted fingerprint data is output from the fingerprint sensor **30** to the processor **22** via the transmission path **24**.

[0028] Step **110**: A new OTC **72** is generated using the new OTC generation circuit **60** or is received from the processor **22**, and the new OTC **72** is stored in the eNVM **34**. The OTC **72** is only used once, so after the OTC **72** is used for encrypting fingerprint data, a new OTC **72** is stored in the eNVM **34**. If the new OTC generation circuit **60** is used for generating the OTC **72**, the new OTC generation circuit **60** can generate the new OTC **72** randomly or based on a previous value of the OTC **72**. For example, if the new OTC **72** is generated based on a previous value of the OTC **72**, the previous value of the OTC **72** can be altered using simple logic operations in order to create the new OTC **72**. Meanwhile, the processor **22** will create the same new OTC **72** that is created by the new OTC generation circuit **60**.

[0029] Step **112**: End.

[0030] The encryption algorithm indicator **74** stored in the eNVM **34** can be updated as often as desired. The update can take place periodically, such as every week or every day, or can take place after each time the logic algorithm circuit **32** is used for encrypting fingerprint data. When the encryption algorithm indicator **74** is updated, the processor **22** sends the updated encryption algorithm indicator **74** to the fingerprint sensor **30**, and the updated encryption algorithm indicator **74** is stored in the eNVM **34**.

[0031] Since the processor **22** maintains a copy of the same OTC **72** and encryption algorithm indicator **74** that are used in the fingerprint sensor **30**, the processor **22** is able to successfully decrypt the encrypted fingerprint data that the processor **22** receives from the fingerprint sensor **30** in order to verify the fingerprint data. The encryption algorithm indicator **74** will indicate to the processor **22** which of the logic encryption circuits **52**, **54** were used for encrypting the fingerprint data. The processor **22** does not necessarily need to have its own logic encryption circuits **52**, **54** since the processor **22** can be a general purpose processor capable of executing a variety of varying and complex instructions. The processor **22** is able to perform the same logic operations as the logic encryption circuits **52**, **54** in reverse for decrypting the encrypted fingerprint data.

[0032] In summary, the present invention provides away to dynamically select an encryption type that is used to encrypt fingerprint data using the OTC **72**. Since the OTC **72** is only used a single time, this makes it harder for an unauthorized party to decrypt the fingerprint data. Also, dynamically selecting the logic encryption circuits **52**, **54** using the encryption algorithm indicator **74** for performing the encryption also adds a second layer of protection. One would have to know both the OTC **72** and the selected logic encryption circuits **52**, **54** that were used for encrypting the fingerprint data in order to decrypt the corresponding encrypted fingerprint data. Furthermore, the fingerprint sensor **30** can be formed on a single chip, making it simple for product manu-

facturers to take advantage of the dynamic encryption functions of the fingerprint sensor **30** when designing products that make use of the fingerprint sensor **30**.

[0033] Those skilled in the art will readily observe that numerous modifications and alterations of the device and method may be made while retaining the teachings of the invention. Accordingly, the above disclosure should be construed as limited only by the metes and bounds of the appended claims.

What is claimed is:

1. A dynamic encryption type fingerprint sensor, comprising:

a capacitive array sensing fingerprints and producing fingerprint data;

an embedded non-volatile memory (eNVM) storing a one-time code (OTC) and an encryption algorithm indicator;

a logic algorithm circuit encrypting the fingerprint data produced by the capacitive array according to the OTC and the encryption algorithm indicator, the logic algorithm circuit comprising:

an encryption circuit comprising a plurality of logic encryption circuits selected using the encryption algorithm indicator, the encryption circuit encrypting the fingerprint data using selected logic encryption circuits of the plurality of logic encryption circuits according to the OTC; and

a control circuit for controlling operation of the capacitive array, the eNVM, and the logic algorithm circuit.

2. The dynamic encryption type fingerprint sensor of claim **1**, wherein one or more of the plurality of logic encryption circuits is selected using the encryption algorithm indicator, and the one or more selected logic encryption circuits encrypt the fingerprint data according to the OTC.

3. The dynamic encryption type fingerprint sensor of claim **1**, wherein the encryption algorithm indicator is updated periodically, and an updated encryption algorithm indicator is stored in the eNVM.

4. The dynamic encryption type fingerprint sensor of claim **1**, wherein the encryption algorithm indicator is updated after every time the logic algorithm circuit is used for encrypting fingerprint data, and an updated encryption algorithm indicator is stored in the eNVM.

5. The dynamic encryption type fingerprint sensor of claim **1**, wherein the OTC is encrypted.

6. The dynamic encryption type fingerprint sensor of claim **1**, wherein the OTC is received from outside the dynamic encryption type fingerprint sensor.

7. The dynamic encryption type fingerprint sensor of claim **1**, wherein the logic algorithm circuit further comprises a new OTC generation circuit for generating a new OTC after the OTC has been used for encrypting fingerprint data.

8. The dynamic encryption type fingerprint sensor of claim **7**, wherein new OTC is generated randomly or generated based on a previous value of the OTC.

9. The dynamic encryption type fingerprint sensor of claim **1**, wherein the dynamic encryption type fingerprint sensor is formed on a single chip.

10. The dynamic encryption type fingerprint sensor of claim **1**, wherein the eNVM further stores a product identification of the dynamic encryption type fingerprint sensor to identify the dynamic encryption type fingerprint sensor.

11. A method of dynamically encrypting fingerprint data with a fingerprint sensor, the method comprising:

sensing fingerprints with a capacitive array of the fingerprint sensor and producing corresponding fingerprint data;

receiving an encryption algorithm indicator and a one-time code (OTC);

selecting one or more logic encryption circuits of a plurality of logic encryption circuits using the encryption algorithm indicator; and

encrypting the fingerprint data produced by the capacitive array with the one or more selected logic encryption circuits according to the OTC.

12. The method of claim **11**, wherein the OTC and the encryption algorithm indicator are stored in an embedded non-volatile memory (eNVM) of the fingerprint sensor.

13. The method of claim **12**, wherein the encryption algorithm indicator is updated periodically, and an updated encryption algorithm indicator is stored in the eNVM.

14. The method of claim **12**, wherein the encryption algorithm indicator is updated after every time the logic algorithm circuit is used for encrypting fingerprint data, and an updated encryption algorithm indicator is stored in the eNVM.

15. The method of claim **12**, wherein the eNVM further stores a product identification of the fingerprint sensor to identify the fingerprint sensor.

16. The method of claim **11**, wherein the OTC is encrypted.

17. The method of claim **11**, wherein the OTC is received from outside the fingerprint sensor.

18. The method of claim **11**, further comprising generating a new OTC after the OTC has been used for encrypting fingerprint data.

19. The method of claim **18**, wherein new OTC is generated randomly or generated based on a previous value of the OTC.

20. The method of claim **11**, wherein the fingerprint sensor is formed on a single chip.

* * * * *