RF Sensor-based Liveness Detection Scheme with Loop Stability Compensation Circuit for a Capacitive Fingerprint System

Woojung Kim\(^1\), Woojin Hong\(^1\), Taekmoo Kim\(^2\), Dongwoon Kim\(^2\), and Myunghee Lee\(^1\),
Member, IEEE

\(^1\)School of Electrical & Electronic Engineering, Ulsan National Institute of Science and Technology (UNIST), Ulsan, 44919 Korea.
\(^2\)Canvasbio, Pankyoo, 13486 Korea.

Corresponding author: Myunghee Lee (e-mail: myunghee.lee@unist.ac.kr)

This work was partly supported by the HRD Program for Intelligent semiconductor Industry of KIAT(Korea Institute for Advancement of Technology) grant funded by the Korea Government [No. N0001883] and Technology development Program of MSS(Ministry of SMEs and Startups) [S2479721].

ABSTRACT A capacitive fingerprint system is the most widely used biometric identification method for smartphones. In this paper, we propose a RF sensor-based liveness detection scheme. This method solves the problem of spoofing attacks, which is a primary disadvantage to capacitive fingerprint sensors. The proposed scheme measures the inherent impedance characteristic difference of the target fingerprint caused by the eddy-current effect with an auto-balancing bridge method. The magnetic field is generated by a small form-factor inductor coil of \( \phi = 1.5 \text{mm} \). This detection scheme can be easily integrated with an existing capacitive fingerprint sensor by using the same CMOS process. The measured results demonstrate the liveness detection capability of the Si-graphite (silicone-graphite) and polyvinyl fake fingerprints that cannot be distinguished by conventional capacitive fingerprint sensors.

INDEX TERMS anti-spoofing, auto-balancing bridge, capacitive fingerprint sensor, Eddy-current, loop stability compensation, RF (Radio frequency) sensor-based liveness detection, Si-graphite (silicone-graphite) & polyvinyl fake fingerprints

I. INTRODUCTION

Fingerprint sensing technology has become the most popular biometric identification method for the latest mobile devices [1], [2]. There are several methods for fingerprint sensing, including capacitive [3], [4], optical [5], ultra-sonic [6], [7], and others [8].

Capacitive fingerprint sensing technology identifies the ridges and valleys of the fingerprint with hundreds of thousands of capacitive sensor cells, which read the capacitance between the metal plate of the sensor and the finger [3], [4]. Despite its compact size and low cost, this technology has some performance limitations due to noise, humidity or contamination, which make poor image quality. On the other hand, the optical sensor relies on the reflected light from the valleys and ridges of the fingerprint. Therefore, it can render a high-quality image despite those limitations. However, it is difficult to miniaturize due to the complexity of its sensor module, which includes a light source, an optical lens, and a CMOS image sensor. Furthermore, its 2-dimensional image information is easily spoofed [5].

Although it is more expensive than other methods, the ultrasonic fingerprint sensor, which uses MEMS (Micro Electro Mechanical Systems) technology to generate an ultrasound [6], [7], can sense fingerprint images as well as those of the internal skin tissues, and can detect fingerprints even under harsh conditions, such as contamination and humidity.

Compared to conventional ID & password authorization, biometric identification is very convenient with a low risk of loss and fast response speed. However, one of the main drawbacks for adopting these methods is their susceptibility to spoofing attacks [9]. Supreme among the fingerprint biometric identification solutions described above is capacitive fingerprint sensing technology due to its simple structure [10]. However, since fingerprint information can be easily obtained from unauthorized manners it is vulnerable to spoofing [11]. Capacitive sensors cannot distinguish a sophisticated fake fingerprint, commonly produced with Si-graphite or polyvinyl, exhibiting similar electrical properties to human skin. Fingerprint sensors - both capacitive and
ultrasonic - in all smartphones on the market, are easily spoofed by fake fingerprints.

Anti-spoofing solutions are generally classified as either hardware- or software-based. The software-based method detects liveness using data processing or algorithms [11], [12], [13]. This method can be implemented with existing capacitive fingerprint sensors without extra hardware. However, once the fake fingerprint is authenticated, the software-based method is spoofed by having learned the additional features of the fake fingerprint image. The hardware-based method depends on biometric information, such as epidermic temperature [14], optical properties [15], pulse oximetry [16] and others [17]. This offers more accurate liveness detection at the increased cost of additional hardware [18].

This paper introduces a RF sensor-based liveness detection scheme. With a small form-factor inductor coil, the scheme can be implemented without a significant increase in cost or size compared to other hardware-based methods. This scheme can be easily integrated with existing capacitive fingerprint sensors by using the same CMOS process. It senses the impedance characteristic difference of fingerprints using the Eddy-current effect. The detection technique is described in Section II. Section III discusses the proposed RF sensor-based liveness detection sensor circuit design. Sections IV and V show the measurement results and conclusion.

II. PROPOSED RF SENSOR-BASED LIVENESS DETECTION TECHNIQUE

The proposed scheme uses the principle of ECPS (Eddy-Current Position Sensor) to detect the impedance characteristic difference of the target object. The ECPS accurately measures the position of a metallic target using the principle of the Eddy-current effect [19], [20]. A typical ECPS senses the distance of a target with the same conductivity. However, the proposed scheme senses the conductivity difference of multiple targets with the same distance. Fig. 1 shows the principle of the proposed RF sensor using a small form-factor inductor coil. The Eddy-current, characterized by its high frequency, is formed primarily within the skin from the surface of the conductor due to the skin effect [19]. The conductivity difference between a live and a fake fingerprint induces a different amount of Eddy-current: the inductance decreases, while the resistance increases.

![FIGURE 1. Principle of RF sensor-based liveness detection scheme using Eddy-current with live and fake fingerprint.](image)

![FIGURE 2. Proposed liveness detection inductive sensor (a) Series resistance and (b) Parallel resistance equivalent circuits model.](image)

![FIGURE 3. Impedance measurement result](image)

The equivalent circuit of the proposed inductive sensor consists of a lossy inductance (Series R-L circuit) with a parallel parasitic capacitance, $C_p$, as shown in Fig. 2(a). The series resistance model is equivalent to the parallel resistance model near the resonant frequency [21]. The resonance frequency, $\omega_0$, of each model is equal to $(L_{coil}C_p)^{1/2}$.

In Fig. 2(b), the maximum impedance of the inductive sensor, $|Z(s)|_{max}$, at the resonance frequency is represented by the parallel resistance, $R_p = L_{coil}/(R_pC)$. The impedance $Z(s)$ of the proposed RF sensor is

$$Z(s) = \left(\frac{1}{sR_p} + sC_p + \frac{1}{sL_{coil}}\right)^{-1} \tag{1}$$

The scheme senses the impedance characteristics of a fingerprint, which has an inherent resonance frequency, $\omega_0$, and the maximum impedance value $|Z(s)|_{max}$ = $R_p$. The higher conductivity by a live fingerprint causes a higher resistance, $R_p$, than that of a fake one made from such materials as silicon-graphite and polyvinyl material due primarily to a higher Eddy-current. The impedance measurement results are shown in Fig. 3. Live fingerprints have a higher maximum impedance value than that of fakes. The maximum impedance values of each target sample show the conductivity with the order of $|Z(\omega)|_{max, air} < |Z(\omega)|_{max, fake} < |Z(\omega)|_{max, live}$. Any object between the highest maximum impedance value of air and the lowest maximum impedance value of the live fingerprints is identified as a fake fingerprint. $(R_p+L)$ measurement [21] and the auto-balancing bridge method [22], [23] are typical impedance measurement methods. In Fig. 4(a), the $(R_p+L)$ measurement method senses the $R_p$ by monitoring...
the value of negative resistance \( -R_p \) to keep the oscillation amplitude level constant. This method can operate at a wide range of the frequencies, from 500 kHz to 10 MHz. However, it is only available for inductors with a high Q-factor of at least \( Q > 10 \) [21]. The auto-balancing bridge method is mainly used for modern impedance measurement equipment, such as impedance analyzers and LCR meters [24]. Through the feedback loop in Fig. 4(b), the current \( I_x \) in DUT and the current \( I_r \) in the reference resistor \( R_r \) are equally balanced. The value of \( Z_{\text{DUT}} = R_pV_x/V_r \) can be obtained from the measured \( V_r \) and \( V_x \). The auto-balancing bridge method is used for the impedance measurement over a wide frequency range up to 120 MHz, and it has high signal-to-noise ratio [25]. In this case, the auto-balancing bridge method is adopted since the Q-factor value is roughly 5 due to the size limitation of the inductor with a small diameter, \( \phi = 1.5 \) mm.

III. CIRCUIT DESIGN

Fig. 5 shows the block diagram of the proposed liveness detection scheme. It includes an OTA-C (Operational Transconductance Amplifier-Capacitor) sinusoidal pulse generator, an auto-balancing bridge with a de-sensitive resistor and a passive peak holder. The inductor, \( Z(s) \) is connected between the \( \text{DUT\text{\_IN}} \) and \( \text{DUT\text{\_OUT}} \). The OTA-C sinusoidal pulse generator is implemented as variable frequency AC voltage source for the auto-balancing bridge. The auto-balancing bridge outputs the impedance value corresponding to the impedance measurement range. A de-sensitive resistor is added to compensate for the loop stability of the auto-balancing bridge. The passive peak holder circuit holds a maximum impedance value within the measurement range.

Fig. 6 shows the timing diagram of the detection scheme. The liveness detection process starts by the \( \text{FST} \) signal. For every clock period \( T \), the frequency sweeps from \( f_{\text{HIGH}} \) to \( f_{\text{LOW}} \).

The frequency sweep range is divided into 23 steps (= 23 × Clock period). During the frequency sweep, the corresponding impedance value, \( |Z(f)| \), appears at the \( V_{\text{OUT}} \) node. The peak holder circuit holds the maximum impedance value \( |Z(f)|_{\text{max}} \) at the resonance frequency as \( V_{\text{PEAK}} \).

A. OTA-C SINUSOIDAL PULSE GENERATOR

The RF sensor requires a frequency generator within the 10-30 MHz band. An OTA-C with a 100 MHz bandwidth is used to control the output frequency by tuning \( g_m \) and \( C_L \) values [26, 27]. In Fig. 7, the oscillation condition is

\[
\frac{g_m}{C_L} = \frac{g_{m1}}{C_L} + \frac{g_{m2}}{C_L} \tag{2}
\]

and an assumption can be made that \( g_m = g_{m1} = g_{m2} = g_m/2 \). The oscillation frequency \( \omega_n \) and the sinusoidal pulse output voltage \( V_{\text{OSC}} \) can be written as

\[
\omega_n = \frac{g_m}{g_m} \left( g_m = g_{m1} = g_{m2} \right) \tag{3}
\]

\[
V_{\text{OSC}}(t) = \frac{I_{SS}}{g_m} \sin(\omega_n t) = \frac{I_{SS}}{g_m} \sin\left( \frac{g_m}{2\pi C_L} t \right) \tag{4}
\]

The values of \( I_{SS} \) and \( g_m \) depend on the required amplitude of the sinusoidal signal \( V_A \). The load capacitor value \( C_L \) is set by the frequency range. Generally, a linear frequency control is performed by changing the \( g_m \) of the OTA [26, 27]. In this design, only the load capacitors \( C_L \) vary to generate a constant output amplitude \( V_A = I_{SS}/g_m \) from (4).

To sweep the frequency, the load capacitor \( C_L \) consists of a capacitor bank which is comprised of one reference capacitor, \( C_{\text{REF}} \), and 23 unit capacitors, \( C_{\text{UNIT}} \). The capacitor bank is connected to the output of each OTA stage and is used to determine the value of \( C_L \). During the frequency sweep, the value of \( C_L \) increases by \( C_{\text{UNIT}} \) per every clock period \( T \) with the
switch control signal SW[22:0]. The value of \( C_L \) varies from \( C_{ref} \) to \( C_{ref} + 23C_{unit} \) over 23 clock periods. The \( C_{ref} \) and \( C_{unit} \) values are determined according to the measurement frequency range \( f_{LOW} = g/m \{ 2\pi (C_{ref}+23C_{unit}) \} \) to \( f_{HIGH} = g/m/(2\pi C_{ref}) \). In this design, the target output frequency range is 10-30 MHz and the output amplitude \( V_A \) is 0.5 V.

B. AUTO-BALANCING BRIDGE CIRCUIT

The conventional structure of the auto-balancing bridge is the type-I structure in Fig. 8 [22]-[25]. The gain of the type-I structure is \( |A_{type-I}(s)| = R_{REF}/|Z(s)| \). In this case, the output voltage is inversely proportional to the DUT impedance. The type-I structure outputs a minimum voltage \( v_{OUT,MIN} \) for maximum impedance, \( |Z(s)|_{max} \). In the type-II structure shown in Fig. 9, the location of the DUT \( |Z(s)| \) and reference resistor \( R_{REF} \) are switched. The output voltage is linearly proportional to the impedance of DUT, which is \( |A_{type-II}(s)| = |Z(s)|/R_{REF} \). In this design, the maximum impedance \( |Z(s)|_{max} \) of each fingerprint is compared. The output of the type-II structure can be compared directly.

C. LOOP STABILITY COMPENSATION

Fig. 10(a) shows the parasitic capacitance at the conjunction point. In the conventional auto-balancing bridge circuit, the negative input of the op-amp \( v_i \) is placed near the ground reference to avoid the parasitic capacitance effect [23]. Then \( C_{PI} \) can be ignored as both are connected to the ground reference, and \( C_{P2} \) appears as the output load capacitor. To keep \( v_i \) to the ground, a bi-voltage (+V to -V) sources are needed, but it makes the IC design complicated. In this paper, the \( v_i \) voltage is placed at \( VDD/2 \) rather than the ground. This parasitic capacitance in the auto-balancing bridge circuit causes performance degradation.

Fig. 10(b) shows the loop gain \( A(s)f(s) \) bode plot including the parasitic capacitances. In a small signal analysis, the parasitic capacitance, \( C_{PI} \), is parallel to \( R_{REF} \) so that \( Z_{in}(s) = R_{REF}/(1+sC_{PI}R_{REF}) \). The open loop gain \( A(s) \) is the transfer function of the op-amp, and the feedback factor of the auto-balancing bridge feedback loop is

\[
f(s) = \frac{V_i'}{V_o} = \frac{Z_{in}(s)}{Z_{in}(s)+Z(s)}
\]

The feedback factor \( f(s) \) in (5) has a -30 dB magnitude decrease and a -156 deg phase shift near the resonance frequency of \( Z(s) \). When the \( f_{3dB} \) of the op-amp is lower than the resonance frequency \( \omega \) \( \omega > \omega_o \), a negative phase margin (PM) would cause the feedback loop to be unstable.

To maintain loop stability, using a higher \( f_{3dB} \) op-amp can be an option. A desired specification (e.g., DC gain and \( f_{3dB} \)) can be calculated from the loop gain transfer function. This approach can be limited by a fixed GBW (Gain Bandwidth Product) of the op-amp, which depends on the CMOS process technology. In this paper, the loop stability compensation technique is proposed by adding a de-sensitive resistor \( R_d \) to the feedback loop with under 10 mW in additional power consumption. When \( |A(s)f(s)| \gg 1 \), the closed loop gain is

\[
|A_{CL}(s)| = \frac{Z(s)}{R_{REF}} \cdot \frac{A(s)f(s)}{1+A(s)f(s)} \approx \frac{Z(s)}{R_{REF}}
\]

The closed loop gain is hardly changed by any \( f(s) \) variation in (6). The stability of the feedback loop can be compensated by changing \( f(s) \) while maintaining closed loop gain. In Fig. 11(a), \( R_d \) is added at the op-amp negative input. The input impedance is changed to \( Z_{in}(s) = (R_{REF} \| R_d)/(1+sC_{PI}(R_{REF} \| R_d)) \), and the feedback factor \( f'(s) \) is

\[
f'(s) = \frac{V_i'}{V_o} = \frac{Z_{in}(s)}{Z_{in}(s)+Z(s)}
\]

The stability and phase margin improve when the de-sensitive R value decreases, as shown in Fig. 11(b).
IV. MEASUREMENT RESULTS

Fig. 12 shows a die photograph of the proposed liveness detection circuit on the capacitive fingerprint sensor IC. This work is fabricated in 0.18-μm mixed-signal CMOS process technology. The entire chip area is 43.8 mm², the fingerprint sensing area is 26.9 mm², and the area of the proposed liveness detection circuit is 0.3 mm².

The assembled capacitive fingerprint sensor module is shown in Fig. 13. A small inductor sensor is combined with the capacitive sensor package, and the terminals on both sides of the coil are used as DUT_IN and DUT_OUT. The remaining pins are connected to the FPGA controller. Fig. 14 shows the Si-graphite and polyvinyl fake fingerprints used in the measurements, and two samples (#1,2) were measured for each.

Fig. 15 shows the measurement results of the OTA-C sinusoidal pulse generator frequency sweep from \( f_{\text{HIGH}} \) to \( f_{\text{LOW}} \).

In Fig. 15(a), the oscillation frequency of OTA-C sinusoidal pulse generator is 22.6 MHz at the start of the frequency sweep. The frequency is 6.3 MHz at the end of frequency sweep, which is shown in Fig. 15(b). Fig. 16 shows the transient output measurement of the proposed design according to the fingerprint type: no fingerprint (air), fake fingerprint (Si-graphite, polyvinyl) and live fingerprint. At the beginning of the frequency sweep, the output is reset during one clock period. Then, at the end of the frequency sweep, the maximum impedance within 6.3 – 22.6 MHz band is held at the output. The fake fingerprints output values are located between air and live fingerprints. It is same result as the impedance analyzer in section II.

Fig. 17 shows the results for each fingerprint measurements using a 10-bit ADC (Analog to Digital Converter). In order to set the boundary level, the measurements for the air and live fingerprint were taken 10 times, while those for the fake fingerprints were taken 100 times for each case. The minimum gap between live and fake fingerprints was about 115 LSB. Liveness detection can be done by simply setting an arbitrary threshold level between the gaps with a sufficient margin. Based on a simple comparison of output values without complex software algorithms, the results favour a hardware-based liveness detection methodology. The key specifications are summarized in Table I. In order to minimize power dissipation, the RF sensor-based liveness detection circuits should only be activated when fingerprint recognition is in progress.

V. CONCLUSION

This paper introduced a RF sensor-based liveness detection scheme and its circuit implementation without using any software algorithms. This provides a solution to the anti-spoofing measures of existing capacitive fingerprint systems. The scheme can distinguish certain fake fingerprints from live ones through their differentiation on inherent impedance characteristics. This design can be applied to various kinds of impedance measurement sensors.
Furthermore, the proposed loop stability compensation technique can secure phase margins at a high frequency. This work can be easily combined with an existing capacitive fingerprint sensor with a small size of 0.3 mm² (accounting for only 0.7 % of the total area). The circuit is fabricated at 0.18-μm mixed-signal technology.

ACKNOWLEDGMENT

The authors would like to thank the following members of Canvasbio for their contribution: Junyun Kim for sensor module assembly, Juncheol Ok, Dongho Kim and Dongmin Kim for IC design consultation, and Yeonjoong Yoon for layout guidance.

REFERENCES


