A NANOMECHANICAL IDENTIFICATION TAG TECHNOLOGY FOR TRACEABILITY AND AUTHENTICATION APPLICATIONS

Mehrdad Ramezani, Angela R. Newsome, Mayur Ghatge,
Fengchao Zhang, Swarup Bhunia, and Roozbeh Tabrizian
University of Florida, USA

ABSTRACT

This paper reports on a novel ultra-miniaturized identification technology that enables non-clonable tags for a wide span of applications, ranging from consumer electronic systems to commercial goods and products. The new labeling technology is based on nanomechanical resonators with spectral signatures composed from multiple high quality-factor resonance peaks. The spectral signature of the resonant nanomechanical label is used to generate a unique digital tag. Benefitting from highly randomized variations in spectral signature induced by the nanofabrication processing, an array of resonant labels can realize a set of highly randomized tags to serve as watermarks with a large entropy. Proof-of-concept resonant nanomechanical labels, implemented in an ultra-thin stack of aluminum nitride on silicon, demonstrate 28 randomly distributed resonance peaks over 25-100MHz span. A unique digital translation procedure, based on the frequency of resonance peaks, is developed yielding rigid digital tags with 63-bit length. The nanomechanical resonant labels are measured over wide temperature variations and excitation powers to verify the consistency of their major performance metrics including digital tag randomness, uniqueness and repeatability.

INTRODUCTION

As the explosive increase in product counterfeiting becomes a major treat to the global economy in recent years [1, 2], the development of effective identification and authentication approaches stands as an imminent challenge that calls for immediate action. Counterfeiting attacks affect the supply chain through targeting a wide range of goods, including consumer electronic systems, currency, medicine and food products. Growing complexity of globally distributed supply chain for majority of products increases their vulnerability for counterfeiting. In addition to the large-scale economic effect of counterfeiting, global trades in specific counterfeit goods, such as food, medicine and pesticides, carry serious health and safety issues [2]. Hence, there is a critical need to protect today's supply chain from the destructive effects of counterfeiting attacks. To this end, various identification and authentication techniques have been used to enable traceability of genuine products and identify the fake counterparts. These techniques include Universal Product Code (UPC) barcodes [3], quick response (QR) codes [4], radio-frequency identification tags (RFID) [5], and surface acoustic wave (SAW) labels [6]. Such techniques rely on designation of a digital tag, through a specific operation physics, to a physical label that is attached or imprinted on the product; hence enabling traceability and authentication of the host.

Although relatively successful to control and combat the growth of counterfeiting, the available approaches suffer from fundamental limitations that make a label susceptible to cloning, tampering, damage/distortion, and abolishment. While UPC barcodes rely on optical readouts and are required to be in the line of sight of the reader, they can be easily identified, removed and replicated. Furthermore, UPC generators and decoders are widely available to counterfeiters for reproduction and cloning of tags. RFID tags use an integrated circuit (IC), that generally contain 96-512 bits of identification information, and an antenna to function. The bits contained within the IC are used to identify the host object. Unlike UPC barcodes, RFID tags and their corresponding code cannot be visually identified, hence a counterfeiter would require complex reverse engineering techniques. However, since RFIDs rely on electromagnetic read-out techniques at low to moderate frequencies, they require large label area and are prone to destructive / malicious interference. Furthermore, RFIDs are not applicable to metallic products such as vehicle parts, due to the reflection and destructive interference of the electromagnetic waves in conductive media, as well as the detuning of spectral characteristics of its constituent components. SAW labels rely on interaction of surface waves with patterned metal lines on the chip and use a similar read-out technology as RFID tags. Therefore, although SAW labels provide superior performance in extreme conditions, they suffer from similar limitations of RFID tags, including large form-factors and limited resolution in cluttered environment [6].

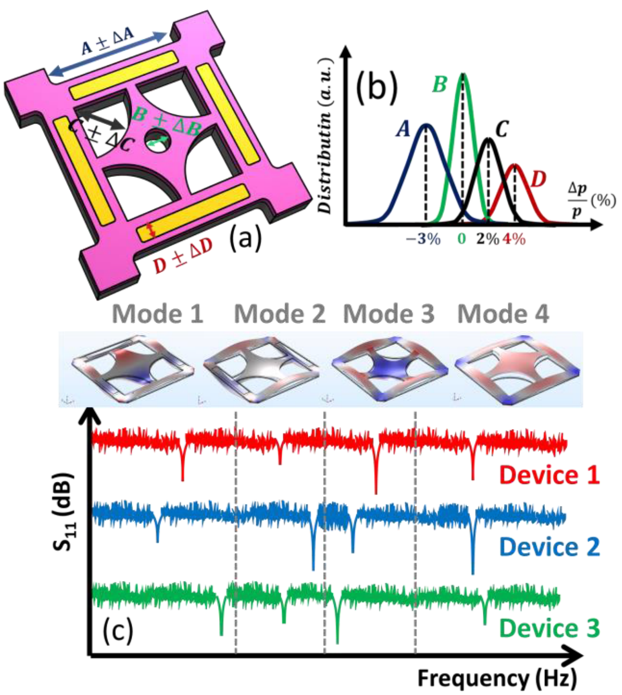


Fig. 1: (a) Resonant NEMS label implemented in AlN-on-Si, highlighting fabrication process uncertainties; (b) Gaussian distribution of various geometrical parameters resulted from fabrication uncertainties; (c) Distinct spectral signature of devices with identical designs, implemented in a single batch. The signature contains several high-Q acoustic resonance modes.

In this paper, we present a novel product labeling approach based on resonant nano-electro-mechanical systems (NEMS) for realization of ultra-miniaturized labels that substantially surpass fundamental limitations of the current labeling technologies for product identification and authentication. Resonant NEMS labels are implemented in ultra-thin piezoelectric-on-silicon stack and engineered to have multiple high quality-factor (Q) resonance

978-1-940470-03-0/HH2018/$25©2018TRF
DOI 10.31438/trf.hh2018.57

modes in their spectral signature (i.e. frequency response). The frequency and amplitude of the resonance modes in the spectral signature of the micromechanical resonant labels are randomly defined through the fabrication variations and are used to generate digital labels with extra-large entropy (Fig. 1). Benefiting from ultra-miniaturized form-factors and high-*Q* of constituent modes, non-clonable and tamper-resistant NEMS labels operating at high frequencies can be realized with extreme robustness and resolution over wide temperature ranges, to surpass fundamental limitations of the current state-of-art identification label technologies.

RESONANT NEMS LABEL CONCEPT

A resonant NEMS label is a perforated plate that is implemented in an ultra-thin aluminum nitride on silicon (AlN-on-Si) stack and geometrically engineered to have multiple resonance modes in a relatively small frequency span. Opting for proper thicknesses of AlN and Si as well as optimization of lateral dimensions of the label enable high-*Q* energy trapping of various flexural and extensional mechanical resonance modes in a single device (Fig. 1). Benefiting from the large electromechanical coupling of the piezoelectric AlN film and large mechanical *Q*s enabled by low loss Si layer the resonance modes of the device can be excited with relatively small input powers, which enable robust contact-less read-out of the resonant NEMS label with superior signal-to-noise ratios.

The performance of resonant NEMS labels, i.e. the frequency of high-*Q* peaks and their relative amplitudes in the spectral signature, is closely correlated with nanofabrication uncertainties, including lithographical alignment imperfections and exposure dose nonuniformities, and variation of piezoelectric film thickness and texture over the substrate. Such inherent uncertainties demonstrate a Gaussian randomness, which propagates to the performance of the implemented resonant NEMS label; hence naturally realizing digital tags with a large entropy and without a need for an external random generator. The intrinsic nature of random tag generation results in substantial immunity of NEMS labels to reproduction or cloning.

LABEL FABRICATION AND CHARACTRIZATION

An array of resonant NEMS labels is implemented in a stack composed from 50nm/120nm/50nm Mo/AlN/Mo transduction stack on top of a 70nm single crystal silicon layer. Fig. 2 demonstrates the fabrication process flow for the implementation of the resonant NEMS labels. Mo/AlN/Mo transduction stack is sputtered on the SOI substrate. The top Mo layer is patterned to form input / output electrodes. This is followed by the RIE of the entire stack to pattern the lateral geometry of the label. Finally, the device is released through etching the buried silicon dioxide (BOX) layer in HF. Fig. 3 (a) demonstrate the SEM image of an array of resonant NEMS labels along with corresponding pads to enable their electrical characterization. Fig. 3 (b) shows an individual resonant NEMS label, highlighting the excitation / read-out electrodes on the AlN film as well as the lateral dimensions of the label. Fig. 4 shows the transmission response (i.e. $|S_{21}|$) of a resonant NEMS label over the frequency span of 25-100 MHz. As evident in Fig. 4, the spectral signature of the label contains 28 distinctive high-*Q* resonant peaks with different insertion losses. *Q*s over 300-1000 are measured for the resonance modes, which are 1-2 orders of magnitude higher compared to electronic resonator counterparts. Such high *Q* directly

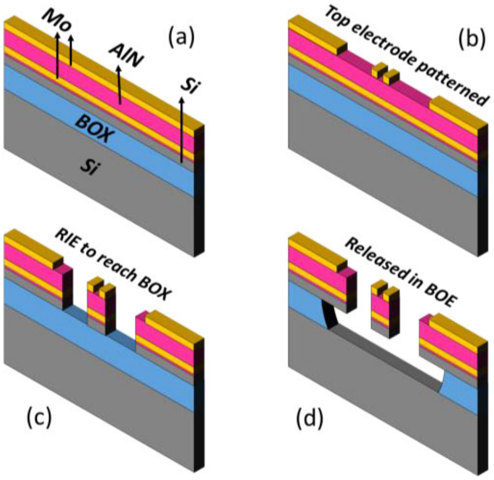


Fig. 2: Fabrication process for implementation of resonant MEMS label. (a) Starting with a stack of Mo/AlN/Mo/AlN(seed)/Si/BOX with thicknesses of 50nm, 120nm, 50nm, 20nm. 70nm, and 2μm, respectively. (b) Patterning top Mo to make the top electrodes. (c) Etching up to BOX layer to define the device geometry. (d) Releasing the device in HF.

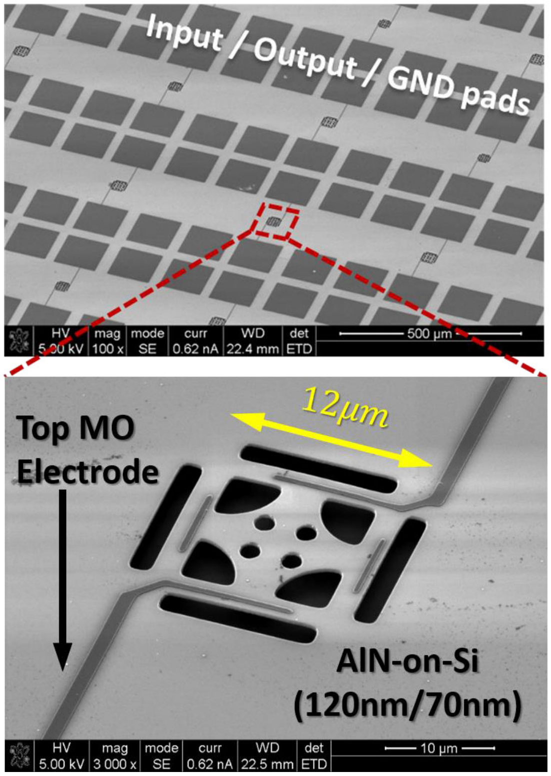


Fig. 3: (top) An array of resonant NEMS labels implemented in a single batch. (bottom) An individual NEMS label with an overall thickness of ~300nm and lateral dimensions of 12μm.

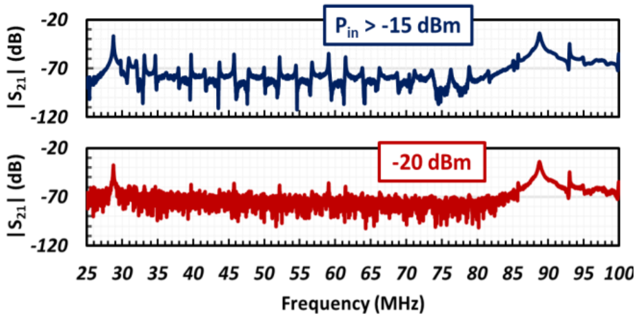
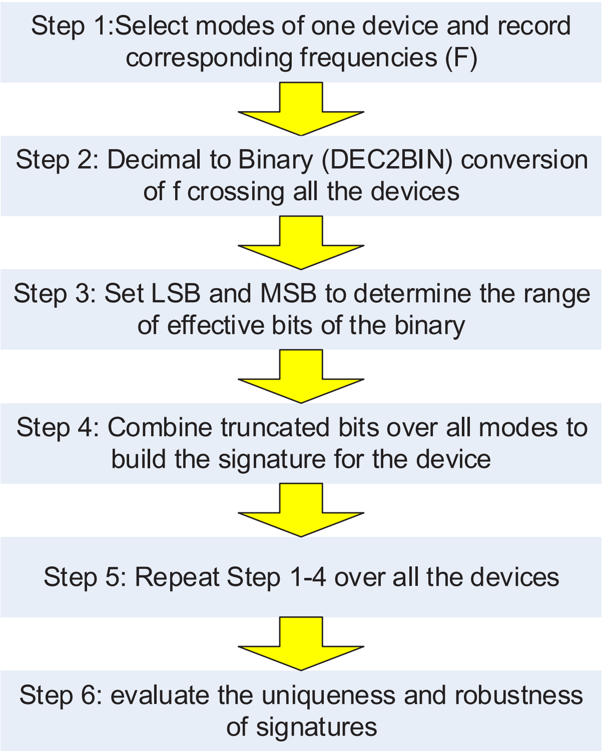


Fig. 4: Measured spectral signature of the resonant NEMS label for different excitation power levels.



Step 1:Select modes of one device and record corresponding frequencies (F)

Step 2: Decimal to Binary (DEC2BIN) conversion of f crossing all the devices

Step 3: Set LSB and MSB to determine the range of effective bits of the binary

Step 4: Combine truncated bits over all modes to build the signature for the device

Step 5: Repeat Step 1-4 over all the devices

Step 6: evaluate the uniqueness and robustness of signatures

Fig. 5: The systematic procedure used for extraction and translation of the digital tags and examination of their robustness for each resonant NEMS label.

translates to the signal-to-noise ratio of the read-out system; enabling robust codes that are immune to environmental variations or destructive noise / interference. The 28 peaks of the spectral signature are used to generate a digital tag for the corresponding NEMS label, as described in the next section.

DIGITAL TAG TRANSLATION

A systematic procedure is used for generation of digital tags for each resonant NEMS label (Fig. 5). The digital tags are generated based on utilization of the frequency of resonance peaks in the corresponding spectral signature. For each device, strong peaks are identified and corresponding frequencies (*f*) are recorded. Then decimal to binary (dec2bin) conversion is conducted to covert the decimal value to binary. After that, the resulting binary is truncated to ideal length for high entropy and stability against noise, following by combination of the result of all modes together to generate the final signature corresponding to each device. Such a procedure is repeated for several labels implemented in the same batch and the extracted signatures are evaluated in terms of randomness, uniqueness and robustness. Table 1 shows the corresponding digital tag of the device with spectral signature in Fig. 4, along with six other devices with identical design, measured on the same die. A 63-bit tag is extracted for each device, highlighting the large entropy of the resonant NEMS label technology.

The uniqueness of signatures is evaluated by the inter device Hamming Distance (inter HD) and the histogram of inter HD ($interHDavg$) is shown in Fig. 6. The averaged inter HD is calculated as:

$$interHD_{avg} = \frac{2}{n(n-1)} \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} HD_{i,j} \qquad (1),$$

where $HD_{i,j}$ stands for the inter HD between devices i and j.

Table 1: The extracted digital tags for seven resonant NEMS label implemented on the same die, having identical designs, measured in 30℃ using an excitation / read-out power of -5dBm.

	Digital Tag (Frequency) - 63bits
Device1	001100001001100011001100110001110011010111001011010101100000000
Device2	100010010100100110001101100010001100010110001010111010011001100
Device3	011011101011110000100000011100010110010000011010100111010110000
Device4	011000001011010010011100011011110111100001001100011101001111111
Device5	010100010010110010011000010011001101011011110011001110000010011
Device6	1000101110011000000001111010010011101010100110010110110011010111
Device7	011101010100100011100101111001110101001111101010010110010100110

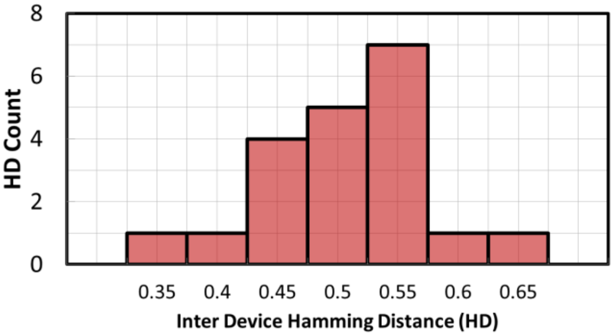


Fig. 6: The histogram of inter HD of the seven devices with digital tags detailed in Table 1; all devices are fabricated on the same die.

TAG ROBUSTNESS EVALUATIONS

To evaluate the robustness and consistency of the resonant NEMS labels two experiments are performed. In the first experiment, the consistency of extracted digital label is examined under various read-out / excitation power levels ranging over -80dBm to 15dBm. A minimum excitation power of -15dBm is required for reliable and repeatable read-out of the spectral signature. Lower excitation powers, below -15dBm, results in low signal to noise ration of read-out, which prevents from reliable identification of resonance peaks and extraction of digital tags. Fig. 4 compares the spectral signature for two excitation powers below (i.e. -20dBm) and above (i.e. > -15dBm) the required threshold. Table 2 summarizes the frequency of the first 9 resonance peaks of the signature, measured with three different excitation powers of -5dBm, 5dBm and 15dBm. Besides the excitation power evaluation, the resonant NEMS label is characterized over temperature range of 30°C - 70°C. Table 3 summarizes the frequency of the first 9 resonance peaks of the resonant NEMS label of Fig. 4, at three different temperature points of 30°C, 50°C, and 70°C. Fig. 7 demonstrates the extracted robustness of the resonant NEMS labels under different excitation power levels and operation temperatures, through the bit error rate (BER).

Table 2: The extracted decimal tags of the resonance peaks for different excitation powers.

Device1 Freq. at 30°C -5dbm (Hz)	Device1 Freq. at 30°C 5dbm (Hz)	Device1 Freq. at 30°C 15dbm (Hz)
28,750,000.0	28,750,000.0	28,750,000.0
30,929,687.5	30,648,437.5	30,929,687.5
31,984,375.0	32,335,937.5	31,984,375.0
33,109,375.0	32,734,375.0	33,109,375.0
34,656,250.0	34,820,312.5	34,656,250.0
39,695,312.5	39,343,750.0	39,695,312.5
43,703,125.0	43,539,062.5	43,679,687.5
45,765,625.0	46,164,062.5	45,742,187.5
52,164,062.5	52,164,062.5	52,164,062.5

Table 3: The decimal tags extracted for a NEMS label at three different operation temperatures, with an excitation power of 5dBm.

Device1 Freq. at 30°C 5dbm (Hz)	Device1 Freq. at 50°C 5dbm (Hz)	Device1 Freq. at 70°C 5dbm (Hz)
28,750,000.0	28,726,562.5	28,703,125.0
30,648,437.5	30,906,250.0	30,953,125.0
32,335,937.5	31,960,937.5	31,937,500.0
32,734,375.0	33,085,937.5	33,062,500.0
34,820,312.5	34,632,812.5	34,609,375.0
39,343,750.0	39,671,875.0	39,648,437.5
43,539,062.5	43,656,250.0	43,632,812.5
46,164,062.5	45,718,750.0	45,695,312.5
52,164,062.5	52,140,625.0	52,093,750.0

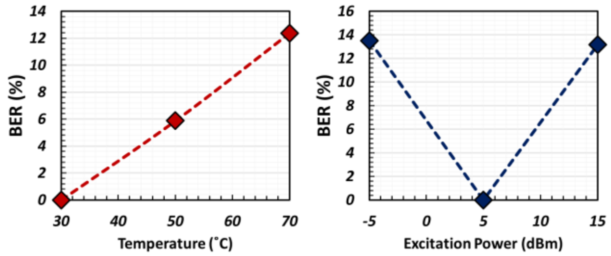


Fig. 7: Measured bit error rate (BER) versus (a) temperature variations and (b) excitation power variations.

Table 4: The qualitative comparison amongst common barcode technologies, with the presented resonant NEMS label.

	QR Code	RFID	Resonant M/NEMS Label
Size	***Minimum size:*** • 21 modules by 21 modules (dots) ***Maximum size:*** • 177 modules x 177 modules (dots)	***IC Minimum size:*** • 0.15mm x 0.15mm (smallest recorded size by Hitachi)	***Minimum Size:*** • Nano-meter scaling (sub 100-nm)
Invisibility	• Cannot be invisible due to sizing requirements for QR code dots for functionality.	• Visible due to the RF antenna and actual "tag" the microchip sits on.	• Not visible to the human eye without mechanical assistance.
Entropy	• 40 possible QR Code versions ranging from a minimum of 7 binary bits and a maximum of 2,953 binary bits	• Typically stores 96-512 bits of memory	***MEMS prototypes:*** • Entropy can be set based on frequency range set for device.
Cost	• Price based on the QR Code generator used. • Estimated $5/QR Code • QR code scanner prices range from $40-$300	• Ranges from $0.05 to $50, depending on the application. • RFID Tag scanner prices range from $500- $2,000	***Envisioned*** • $0.01-$0.05 benefiting from wafer-level batch fabrication / miniaturized size.
Robustness	• Can be used for different applications. • Error code correction allows functionality with some damage and distortion to QR Code. • Readable from all directions.	• Cannot be used on all materials such as: liquid and metal products. • Environmental variations (such as sensor signal clutters, temperature, etc.) can cause dysfunctionality.	• Physical and variations (i.e., electrode positioning and number of nanodots, temperature, power) will not distort digital signature • Ability to use on most material platforms
Vulnerability to Tampering	• Can be decoded using QR decoder techniques found via internet. • No true security • Easy malicious manipulation by hackers.	• Can be duplicated using reverse engineering techniques • Easily damaged or destroyed • Easily removed	• Clandestine (visually untraceable) • If detected, intrusive tampering will damage device / not allow for reverse engineering. • Vulnerability VERY limited due to size.
Application Space	• Consumer goods • Retail • Entertainment (i.e., concert and sports tickets) • Electronics • Social Applications	• Retail • Access management (i.e., hotel rooms, ID badges) • Military • Transportation • Toll collection • Government documents (i.e., passports) • Human Implantation	***Envisioned:*** • Consumer goods • Retail • Entertainment • Electronics • Currency • Government documents • Access management • Military Applications

The relatively small BER measured for excitation power and temperature variations demonstrates the robustness of the tags and highlights the potential of the resonant NEMS technology for realization of non-clonable ultra-miniaturized labels for anti-counterfeit authentication and identification. Table 4 presents a qualitative comparison for the tree most common barcode technologies from [4] [7-10], with the presented NEMS label technology.

CONCLUSION

This paper presents a novel resonant NEMS labeling technology, which can be applied to diverse class of products to reliably identify and authenticate them. Such technology enables realization of ultra-miniaturized labels for traceability and authentication applications, towards securing the supply chain against counterfeiting and piracy. Resonant NEMS labels are implemented in an ultra-thin AlN-on-Si stack piezoelectric and are engineered to have multiple high-*Q* resonance peaks in a small frequency span. The spectral characteristics of the resonant NEMS labels are used, along with a systematic translation procedure, to extract corresponding digital tags. Benefiting from 28 high-*Q* resonance modes that are randomly distributed in correlation with fabrication process uncertainties, 63-bit digital tags with large entropy are extracted for the NEMS labels. Robustness characterization, under various excitation powers and operation temperatures confirms the consistency of the digital tag of the corresponding resonant NEMS label.

REFERENCE

[1] Corben, R. *Economic Report Predicts Rise in Global Counterfeiting, Piracy*, https://www.voanews.com/a/global-trend-in-counterfeiting-and-piracy/3783360.html

[2] Hargreaves, S. *Counterfeit goods becoming more dangerous* http://money.cnn.com/2012/09/27/news/economy/counterfeit-goods/index.html

[3] Nachtrieb, J. and Profile, J. (n.d.). *The Seven Most Common Reasons That Barcodes Fail*. [Online] Barcode Test. Available at: http://barcode-test.com/the-seven-most-common-reasons-that-barcodes-fail-2/ [Accessed 9 Dec. 2017].

[4] Wikipedia. (n.d.). *QR code*. [online] Available at: https://en.wikipedia.org/wiki/QR_code [Accessed 10 Dec. 2017].

[5] Burke, P. and Rutherglen, C. (2009). *Towards a single-chip, implantable RFID system: is a single-cell radio possible?*. [online] National Center for Biotechnology Information. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2896640/ [Accessed 9 Dec. 2017].

[6] Barton, R. (n.d.). [online] NTRS NASA. Available at: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20140000415.pdf [Accessed 9 Dec. 2017].

[7] Dion Label Printing. (n.d.). *UPC A Barcode Size Standard*. [online] Available at: http://www.dionlabel.com/tl_files/dion/Downloads/Dion%20Label%20Printing%20Barcode%20Information.pdf [Accessed 10 Dec. 2017].

[8] ADC Barcode. (2017). *RFID and Inventory Control - ADC Barcode*. [online] Available at: http://adcbarcode.com/news/rfid-and-inventory-control/ [Accessed 10 Dec. 2017].

[9] QR Code.com. (2017). *Information capacity and versions of QR Code*. [online] Available at: http://www.qrcode.com/en/about/version.html [Accessed 10 Dec. 2017].

[10] Journal, R. (n.d.). *RFID Frequently Asked Question - RFID Journal*. [online] RFID Jourdan. Available at: https://www.rfidjournal.com/faq/show?86 [Accessed 10 Dec. 2017].

CONTACT

*Mehrdad Ramezani; tel: +1-352-328-7462; mehram@ufl.