

## I<sup>2</sup>S<sup>3</sup> the Integrated Intelligent Secure Sensor Systems project

A.B.T. Hopkins and  
K.D. McDonald-Maier,  
*University of Essex, Colchester,  
United Kingdom.*

W.G.J. Howells,  
*University of Kent,  
Canterbury,  
United Kingdom.*

A.T. Erdogan and T. Arslan,  
*University of Edinburgh,  
Edinburgh,  
United Kingdom.*

### Abstract

*Secure systems are of growing importance for protecting the assets and rights of business and individuals, who are increasingly reliant on surveillance equipment for deterrence of criminals and enforcement of justice. The Integrated Intelligent Secure Sensor Systems Project (I<sup>2</sup>S<sup>3</sup>) integrates the novel technology necessary to extend the capabilities of surveillance equipment to provide preemptive warnings by detection of suspicious activity. Advanced reconfigurable hardware provides an ultra low power platform to underlie the image analysis and novel remote biometric identification algorithms. Each of the distributed sensor nodes is secured through a novel technique named ICmetrics which exploits synergies between biological and artificial systems.*

### 1. Introduction

Society is increasingly in fear of the malicious and violent exploits of organized crime, and is burdened by demands for vigilance of potential terrorist activity. In contrast, people are concerned about the impacts of stop and search policing and are worried that civil liberties will be progressively eroded to the point where their way of life is threatened. This gives rise to an unprecedented demand for improved security policy and solutions that prevent crime and terrorism without compromising the freedom and civil liberties that society holds dearly. Furthermore, the electronic systems that our society heavily depends on for every day activities are also vulnerable. This is especially the case for systems such as surveillance equipment which can be hacked or tampered with so that criminals can exploit its features for their ill-gotten gains. Significant social and technological advancement is required to overcome these challenges, and Integrated Intelligent Secure Sensor Systems (I<sup>2</sup>S<sup>3</sup>) represent a platform that contributes by integrating the technology

necessary to enable practical realization of a secure camera based surveillance system that autonomously identifies threats and raises alert. The platform will be realized using a variety of algorithms and techniques that rely on biological features and receive biological inspiration.

### 2. Benefits of I<sup>2</sup>S<sup>3</sup>

To help counter society's growing fear of terrorist attacks and criminal activity, and to protect the interests of individuals and business, the I<sup>2</sup>S<sup>3</sup> system aims to develop a novel secure remote sensing system that is based around an integrated network of intelligent cameras. It will be capable of identifying authorised personnel and potentially suspicious people by tracking them between camera views and proactively identifying potentially threatening behaviour patterns. The system will have the capability to report activity and provide supporting evidence so that human security operators can take preventative action or attempt to curtail escape with guidance from the security network, which itself will be ensured as secure and tamper free.

The project possesses three major innovative features, each of which is elaborated later:

1. Efficient remote biometric based person identification.
2. Biologically inspired ICmetric based encryption for secure communication.
3. Evolvable hardware technology incorporating new custom reconfigurable System-on-Chip hardware.

### 3. Image analysis and remote biometrics

Remote biometrics, defined as personal identification without the need to formally supply a biometric sample, such as writing a signature or posing for a photograph [1], is a highly desirable concept with significant advantages in terms of improved security

and personal convenience. Remote biometrics is recognised as a promising tool to help fight crime, but despite their advantages, it is acknowledged that they are a significantly challenging problem. In practical terms, the remote biometrics will provide unique identification of a person based on CCTV images without the person providing any form of sample image, thus users are identified without inconvenience or specific reference to their given name or a human recognised identifying value such as passport ID or government employment / ID number.

Through autonomous identification of observed personnel, potential threats are targeted more quickly than conventional exhaustive database search driven methodologies. Realization of the remote biometrics is based on novel techniques for facial recognition and generic remote biometrics techniques built on adaptive systems associated with weightless artificial neural networks. Such networks possess the significant advantages of fast learning, with a relatively small training set, and computational simplicity, allowing them to be easily implemented directly in hardware. The technology has been developed over a number of years and has now achieved a level of maturity suitable for focused adaptation to a practical application. Despite these advantages, the overall computational load is still too high for conventional embedded computing platforms such as microcontrollers, thus motivating research of more efficient algorithms and higher performance computer architectures that do not degrade power consumption.

The domains addressed by I<sup>2</sup>S<sup>3</sup> are:

D1. Identifying one of a limited number of known individuals for access control to, for example, a secure installation.

D2. Identifying behaviour that could be threatening, a very simple example being a stranger who remains in a public location for an extended period of time.

Novel adaptive systems which take inspiration from nature are the key to addressing the challenges of remote biometrics as they learn efficiently from reduced sample sets. In case D1, an individual's facial and or gait characteristics will be learnt under variable conditions, such as differing head positions and lighting, while for D2, they will support person tracking in potentially crowded locations over extended time.

To allow feasibility within the project and mitigate risks, two modes of remote biometric will be created. Firstly, facial recognition based on semi-idealised images taken of individuals in fixed locations, such as entering a security portal or passport control, where one to one matching is required will be developed for

securing confined areas such as commercial facilities. Secondly, the general surveillance scenario will be investigated where the goal is to identify unusual or suspicious behaviour rather than identify the individuals concerned. This will primarily require tracking the individuals deemed to be of concern and is the main objective.

#### 4. ICmetrics

Security of system data and communication will be achieved via a concept termed "ICmetrics", which is a novel biologically inspired technique based on analysis of a sensor node's unique properties, synergetic to the way Biometrics exploit the naturally unique properties and features of biological systems [2, 3]. Significantly, the properties may not be stable, and may take values based on a particular (usually, although not necessarily, Gaussian) distribution. Within integrated networks of sensors as proposed by this paper, each hardware node will be similar in construction and will be based around an identical System-on-Chip device. Therefore their properties are potentially similar, and there appears to be no clear way of distinguishing between devices. However in practice this is not the case, because each sensor node is its own sub-system, constructed from hardware and software, whose properties and features are made unique by their individual exposure to the environment. Furthermore, utilisation of adaptive biologically inspired algorithms in both hardware and software further enhances the range of feature types, and increases overall variation between samples.

ICmetrics in principle provides the following three significant advantageous operations:

1. The identity of a particular circuit contained within a device may be determined with a high degree of confidence, hence ensuring its authenticity and freedom from malicious tampering or changes in behaviour like those caused by faults.
2. A unique identifying number may be used as a basis for an asymmetric encryption system, allowing data to be encrypted in the knowledge that it may be decrypted only on the desired device.
3. Similarly, ICsignatures may be associated with data emanating from a given system ensuring its source.

In this project, ICmetrics will be employed to identify the sensor nodes and generate encryption keys, offering significant improvements over conventional techniques. Existing encryption technology, typified by asymmetric encryption [4], suffers from a specific drawback. Regardless of the

length of the encryption key, the associated private key must be stored, and whatever the mechanism, compromise of the storage or encryption will allow access to all data protected by the key [5, 6], much like a safe with a stolen key.

The significant advantages of ICmetrics are:

- Removal of any form of stored template for validating a node at any central database, preventing database compromise and cloning or tampering of sensor nodes.
- The security of the system will be as strong as the ICmetric and encryption algorithm employed, there is no back door. Access is gained by providing another ICmetric sample or breaking the cipher employed by the encryption technology.

Private decryption key storage is a major weakness in traditional encryption systems; I2S3 overcomes this by uniquely associating keys with each sensor node's ICmetric which will be used to generate the private keys on demand [6]. Specially secured circuits will leave no exposed key print in the system's main memory hierarchy for the application software to access, so there will be no stored key, intentionally or otherwise, available for use by maliciously tampered software.

## 5. Custom reconfigurable hardware

Even with this project's improvements in remote biometric algorithms, they are still reliant on computationally intensive imaging. Conventional microprocessors are entirely insufficient for this task, while reconfigurable architectures, such as FPGAs or fabrics like PACT 0, are also unsuitable as they still consume too much power and area. Furthermore, they do not properly support dynamic reconfiguration, so will not support this project's adaptive algorithms well. The University of Edinburgh has demonstrated that a new class of reconfigurable architectures that could be generated to offer huge power and area advantages with the ability to dynamically optimise circuit functionality in real time [9-10]. This is achieved by tailoring the architecture's computational fabric. The basic and core elements of the architecture are the programmable cells which can be programmed to execute one type of operation similar to a CPU instruction. The cells are interconnected through an island-style mesh architecture which allows operation chaining in the datapaths. The number and type of these cells are parameterisable upon application. The salient feature of the architecture is that both the programmable cells and their programmable interconnections can be dynamically reconfigured at

specific points in time. This instruction cell based architecture has similar flexibility of a coarse-grain FPGA and programmability of a DSP. Furthermore, since it employs a coarse-grained reconfigurable architecture, it has lower power consumption and less silicon area than a generic fine-grained FPGA.

This instruction cell based architecture will support an "evolvable" node architecture, which will be realised in conjunction with specialty design tools donated by Spiral Gateway to drive custom sensors. Additionally, a strategy will be employed for distributing embedded software units within the various fabrics based on a cellular biologically inspired evolutionary algorithm that will allow the monitoring of subjects between sensors in real-time.

## 6. Conclusion

The security problems addressed by this paper and the related social problems that it helps fight are of growing public, government and global concern. Society needs this research to help maintain security and tranquillity, while business needs it to protect commercial activity / knowledge and prevent attack on their communications from hackers and malicious employees. Moreover, its benefits will aid the fight against terror without compromising civil liberties as its tracking approach uses autonomously learnt abstract identities rather than relying on pre-stored personal data, employee biometric databases or a national identity system. The integrity of stored data and communications will also be rigorously secured by the novel ICmetrics based template-free encryption. Furthermore, the inherently complicated and computationally intense remote biometric algorithms will be feasible for online use by way of high-level domain specific optimisations and a novel evolvable computing platform that offers high performance with low power and a small form factor suitable for remote networked sensors as envisaged by the I2S3 project.

## 7. Acknowledgement

This research is supported in part by the UK Engineering and Physical Sciences Research Council (EPSRC) under Grants EP/C54630X/1 (ESPACENET) and EP/C005686/1 (ReSIP).

## 8. References

- [1] W.M. Hu, T.N.Tan, L Wang, and S. Maybank, "A survey on visual surveillance of object motion and

- behaviors”, *IEEE Trans. on System Man and Cybernetics Part C*, vol. 34 no. 3, Aug. 2004, pp 334-352.
- [2] F. Hao and C. W. Chan, “Private Key Generation from On-line Handwritten Signatures”, *Information Management & Computer Security*, Vol. 10, No. 4, 2002, pp. 159-164.
- [3] Y.W. Kuan, A. Goh, C.L.D. Ngo and B.J.A. Teoh, “Extraction of Cryptographic Keys from On-line Handwritten Signatures” *Int’l Symp. on Information and Communications Technology*, 2005, pp. 5-8.
- [4] H. Dobbertin, V. Rijmen and A. Sowa, *Advanced Encryption Standard – AES: 4th Int’l Conf.*, AES2004, Bonn, Germany, May 10-12, 2004.
- [5] G. Howells, M.C. Fairhurst and F. Deravi, “Improved Data Security Using Template-Free Biometric Based Encryption”, *ECSIS Symp. on Intelligent Systems for Defense and Security (ISDS), part of 4th European Conf. on Intelligent Systems and Technologies*, Iasi, Romania, Sep. 20-21, 2006.
- [6] G. Howells, A.B.T. Hopkins and K.D. McDonald-Maier, “Ensuring data integrity and hardware identity using ICmetrics”, *ECSIS Symp. on Intelligent Systems for Defense and Security (ISDS), part of 4th European Conf. on Intelligent Systems and Technologies*, Iasi, Romania, Sep. 20-21, 2006.
- [7] S. Douglass, “Introducing the Virtex-5 FPGA Family”, *Xcell Journal*, Xilinx, No. 59, 2006, pp. 8-11.
- [8] PACT XPP Technologies, “XPP-III Processor Overview”, Version 2.0.1, <http://www.pactxpp.com>, Jul. 13, 2006.
- [9] Z. Khan and T. Arslan, “Pipelined implementation of a real time programmable encoder for low density parity check code on a reconfigurable Instruction cell architecture”, accepted for *2007 Design, Automation and Test in Europe (DATE 07)*, to be held in Nice, France, Apr. 16-20, 2007.
- [10] A. Major, Y. Yi, I. Nousias, M. Milward, S. Khawam, T. Arslan, “H.264 Decoder Implementation on a Dynamically Reconfigurable Instruction Cell Based Architecture”, *2006 IEEE Int’l SOC Conf. (SOCC 2006)*, Sept. 2006, pp. 107-108.
- [11] Y. Yi, I. Nousias, M. Milward, S. Khawam, T. Arslan, I. Lindsay, “System-level Scheduling on Instruction Cell Based Reconfigurable Systems”, *2006 Design Automation and Test in Europe (DATE 06)*, Munich, Germany, vol. 1, Mar. 6-10, 2006, pp. 1-6.