A Salient Region Watermarking Scheme for Digital Mammogram Authentication

M. L. D. Wong, S. I. J. Lau, N. S. Chong, and K. Y. Sim

***Abstract*—A region of interest (ROI) based fragile watermarking scheme for digital mammogram authentication is presented in this paper. Here, we propose a new mammogram segmentation scheme for the automatic definition of the ROI for a given mammogram. Difference Expansion based embedding techniques have been used to provide authentication features for the given mammogram. Furthermore, we have implemented the proposed watermarking scheme in both MATLAB and C. Through exploiting the inherent parallelism in the low level image processing layer, we have ported the scheme onto the CUDA platform to further accelerate the real time performance of the proposed scheme. Experimental results and discussions are presented towards the end of this paper.**

***Index Terms*—CUDA, digital mammogram authentication, fragile watermarking, ROI segmentation.**

I. Introduction

Digital mammography screening is performed to detect early stages of breast cancers among women. The screening process produces large amount of digital data which privacy and security need to be ensured. However, the recent advances in digital media editing capabilities have provided various means to maliciously alter these mammograms without introducing visually perceptible artifacts. Hence, there is a need for means to ensure the authenticity and integrity of these mammograms over a communication channel, e.g. within a telemedicine framework.

As with other medical media, we need to ensure the medical information remained unchanged throughout the protection and authentication process in order to avoid any chances of mistakes made in the diagnosis and prognosis process [1]. Conventionally, a cryptographic hash is used for authentication of digital media. However, the cryptographic hash can only provide an overall sense of integrity and does not provide localized authentication. In other word, the authentication using a cryptographic hash could not tell which pixel or region has been tampered with if the authentication fails. In order to bridge this gap, various digital watermarking based approaches are proposed as an alternative means of authentication [2].

To this end, a fragile watermarking scheme is commonly used. As implied by its name, watermarks of this nature are destroyed (non-recoverable) once the corresponding pixels or regions are tampered with. Therefore, it does not allow a single bit to be modified for a watermarked media. In the ideal case for mammogram authentication, an authentic and yet exactly same image is expected to be received by the authenticator. To satisfy this requirement, a reversible scheme is also desired.

For real world deployments, the watermark embedding process requires a real time or near real time performance to facilitate satisfactory user experience. Once the mammograms are acquired, the watermarking process should take place in the background. After which, the watermarked mammograms is stored onto a DICOM portal while the non-watermarked original is discarded. To ensure that, the end user has a reasonable interaction time, we propose a General Purpose GPU based approach to accelerate the performance of an existing watermarking scheme. In this paper, we present the performance profile for three prototypes of the watermarking scheme, i.e. the MATLAB prototype, the CPU based prototype and the CPU/GPU based prototype. For this work, we chose to implement the CPU prototype using C and the CPU/GPU platform chosen was the NVIDIA "Computer Unified Device Architecture" (CUDA) framework.

The rest of this paper is organized as follows: Section II presents some backgrounds on the difference expansion based watermarking schemes while Section III presents the proposed watermarking scheme. Section IV presents the CUDA framework and some acceleration methods used in this paper. Section V presents the experimental results while we draw some concluding remarks in Section VI.

II. Related Works

A. Reversible Watermarking Techniques of Difference Expansion

Tian [3] first proposed to embed watermarks using Difference Expansion (DE) through an integer transform of selected pixel pairs. The selected pixel pairs can either be any two horizontal or vertical adjacent pixels, or any two pixels selected in a pre-defined pattern. The pre-defined pattern may be initialized through the use of a security key and hence providing greater security to the scheme. As the scheme embeds a single bit for every pairs of pixels, the theoretical embedding capacity is then 0.5 bit per pixel (bpp).

In an attempt to increase the embedding capacity, Alattar proposed a reversible watermarking scheme of colour image [4]. The proposed method used spatial and spectral triplets of pixels to hide two bits of information. Spatial triplet is any three pixel values chosen from the same spectral, or color component. On the other hand, the spectral triplet is any three pixels chosen from different spectral components.

Soon after the triplet difference expansion method was proposed, Alattar devised a new difference expansion of quads (a group of four pixels) for reversible watermarking of

Manuscript received December 18, 2012; revised February 20, 2013.

The authors are with the Faculty of Engineering, Computing and Science, Swinburne University of Technology Sarawak Campus, Malaysia (e-mail: {dwong, jlau, nschong, ksim}@swinburne.edu.my).

color images [5]. This improved scheme hides three bits in the difference expansion of quads (4 pixels). The quad is formed from 4 pixel values chosen from four difference locations within the same color component. The simplest way of choosing the quads is to consider every 2x2 adjacent pixel values as quad. The maximum embedding capacity of the new quad DE scheme is computed to be 0.75 bpp. However, in practice we can expect a lower capacity as some quads may not be embeddable.

B. Region of Interest (ROI) Segmentation in Mammograms

In the development of bio-medical watermarking, one would normally segment a medical media into its ROI and RONI. The ROI refers to the critical and information bearing region and RONI referred to the otherwise. Conventionally, ROI definition is usually a fixed geometry (e.g. square, rectangle, circle or ellipsoid) defined manually.

Al-Qershi et al. proposed a scheme capable of hiding patient's data, verifying authenticity of ROI, localize tampered areas, and recover the tampered areas within the ROI [6]. The scheme adopted Tian's DE technique to watermark the RONI and a modified DE technique developed by Guo et al. [7] in the ROI.

Al-Qershi *et. al.*'s scheme proposed two watermarks to be generated. First, a watermark consists of compressed patient's data which was concatenated with a compressed hash computed from the ROI. Then, a second watermark consists of a compressed version of the ROI, the average values of individual blocks (16 x 16) of the ROI, the embedding map of ROI (*EM1*), the embedding map of RONI (*EM2*), the original LSB of changeable pairs in RONI (B), and the LSB of pixels of a predefined secret area in RONI used to embed additional information require to initiate the watermark extraction process (*Orgbits*).

After the formation of the respective watermarks, the ROI was divided into quads and the first watermark was embedded into the ROI using modified DE technique proposed by Guo *et al*. While the second watermark to be embedded into RONI using Tian's DE technique. The information defining the ROI is to be embedded into the secret area of RONI using Tian's technique too.

1) Mammograms segmentation

There have been several previous works done in mammogram segmentation. Some of these methods proposed to use thresholding [8] and [9], gradients [10], modelling background region by using a polynomial [11], fuzzy analysis algorithm [12], or active contours [13].

Generally, methods to approach to image segmentation can be grouped into three classes: pixel-based methods, regional (continuity-based) methods, and edge-based methods. Pixel-based methods are the least powerful and particularly susceptible to noise, but at the lowest level of difficulty in implementation. The other two groups of classes approach the segmentation task with opposing behaviors: continuity-based methods search for similarities while the edge-based methods search for differences.

2) Saliency based segmentation

S. Feng *et al.* [14] proposed a selective visual attention-driven model (SVAM). The proposed SVAM to be applied in localized content-based image retrieval (CBIR) where the user is only interested in a portion of the image.

In the improved saliency map construction algorithm, the multi-scale contrast features (saliency map) is defined as a linear combination of contrasts in the Gaussian image pyramid. L. Itti et al. proposed that 9 pyramid levels are to be constructed to compute the contrast between different levels [15]. On the other hand, S. Feng *et al*. proposed to compute the contrast between 3 different levels only and achieved satisfying results validated empirically.

III. Our Proposed Watermarking Scheme

Here, we proposed an alternative approach for reversible ROI-based watermarking to authenticate digital mammograms. The objective of the scheme is to protect the ROI of the watermarked mammograms from unauthorized alteration. In this scheme we propose an automated ROI definition as a pre-processing step to the watermarking procedures. The automated ROI definition algorithm of the scheme is capable to provide a larger embedding capacity in RONI than Al-Qershi *et al*.'s scheme. The algorithm eliminate of the need of selecting the ROI explicitly by hand. Furthermore, unlike the conventional ROI definition, the ROI selected by the algorithm conforms to natural shape of the breast and therefore minimizes the redundant area in the defined ROI. The detailed ROI extraction, embedding and authentication procedures are as follows:

A. Automatic ROI Definition

First, the mammogram was decomposed into a three level Gaussian Pyramid. Following which, the intensity (contrast) saliency map is constructed through a linear combination of the pyramid levels decomposed earlier. A threshold value is then computed using the improved moment-preserving threshold method proposed by Chen [16]. The ROI is then defined through binarization of the saliency map using the computed threshold.

Fig. 1 (d) shows a particular example of the ROI (denoted by the white filling region) extracted using this approach.

B. Embedding Procedures

Following the ROI extraction, a hash message for the ROI, denoted as H_{roi}, is computed using SHA-256 algorithm. Subsequently, the LSBs of the difference values of the changeable pairs in ROI are grouped together and denoted as B_{org1}. The patient's data is then compressed and concatenated with H_{roi} to form the first watermark bit stream to be embedded, B_1. If the length of B_1 is greater than the maximum embedding capacity of the ROI, then the compressed version of patient's data is partitioned into two parts, PD_1 and PD_2 where $|PD_1| = |B_1| - |H_{roi}|$.

B_1 is then embedded in ROI using Alattar's DE of quads method. The first location map is constructed during the embedding process in ROI, denoted by LM_1. B_1 is to be embedded in both expandable and changeable quads in ROI.

A second location map, LM_2, is then constructed using Tian's DE method for the RONI. The LSBs of the difference value of the changeable pairs in RONI are grouped together

as B_{org2}. B_{org1} and B_{org2} can now be concatenated in series to form B_{org}.

LM_1, LM_2, and B_{org} are then compressed, giving rise to $LM1_{comp}$, $LM2_{comp}$, $Borg_{comp}$ respectively. The compressed location maps and difference values are then concatenated with PD_2 (if exist) to form second bit stream, B_2. Finally, B_2 is embedded into RONI using Tian's DE to complete the embedding procedures.

Once the embedding procedures are completed as detailed above, the embedding parameters are then packaged and encrypted for delivery to the receiver along with the watermarked mammogram using a secure channel. The embedding parameters include the two embedding thresholds for the RONI and ROI respectively, as well as the ROI border information. For our scheme, we have set the embedding threshold T is set to 5 and gradually increased by a step size of one, should the embedding process fails owing to insufficient embedding capacity. However, the scheme will terminate the embedding procedures eventually if the embedding capacity calculated, at $T = 30$, is insufficient for the given ROI. From the experimental results, it showed that embedding capacity remain almost constant for $T > 30$.

C. Authentication Procedure

At the receiver's end, the ROI and RONI are re-constructed with the given information of ROI's border. Pixels in RONI are first divided into pairs and scanned using Tian's DE. The difference value of the pairs to be partitioned into changeable set and not changeable set.

The LSBs of the difference values from the changeable set are collected and decomposed into its original parts: LM_{1comp}, LM_{2comp}, $B_{orgcomp}$, and PD_2. LM_1, LM_2, and B_{org} are then recovered through decompression. For LM_2 and B_{org}, the difference values which hold the watermark bit are then restored to reconstruct the original RONI. Using LM_1, B_1 can be extracted from ROI using Alattar's quads DE. B_1 is then decomposed into PD_1 and H_{roi}. The quad groups holding the watermark bit are restored during extraction to reconstruct the original ROI. PD_1 and $PD2$ are then concatenated together and decompressed to obtain the patient's data.

A hash message is then calculated from the recovered ROI and if it is equal to H_{roi} then the mammogram is considered authentic. Otherwise, the mammogram is regarded as tampered.

IV. Acceleration Through CUDA

A. CPU/GPU Co-Development

A MATLAB prototype was first implemented to assist in the division between CPU and GPU. We then run a performance profiling exercise on the prototype. From the profile we determine the sub-processes that are computational intensive and these sub-processes then analysed for their suitability for GPU acceleration. Among these, the sub-processes that are parallel in nature are chosen to be implemented first. However, owing to the limited space of this paper, the performance profiling result is not disclosed. Overall, in embedding operation, the Gaussian Pyramid decomposition, set classification and embedding sub-process were chosen to be ported onto CUDA. Whereas for the authentication, adoption was applied to the set classification and region recovery sub-processes.

In the embedding process, the Gaussian Pyramid decomposition is the major focus of CUDA adoption. The construction of the Gaussian pyramid decomposition for the saliency map was done via naïve implementation by completing several runs of convolution of a 2D Gaussian filter on the input image with each run completing a level of the Gaussian Pyramid. Each CUDA thread in a CUDA block is responsible to load an equally size segment of image data from the global memory onto the shared memory of their respective block and then completes a convolution to a single pixel. The memory-loading phase was aided by the GPU's hardware texture to avoid uncoalesced global memory read. As the saliency map is generated, ROI and RONI will be able to be sorted into respective vectors for speedier further processes.

The set classification sub-process refers to the classification of the RONI and ROI data into difference sets as proposed in Tien's and Alattar's DE scheme. This process followed after the regions had been sorted out from input image. The implementation of this sub-process is straight forward as the vectors were in one dimension. Each CUDA thread operates on one member in the vector thus labeling them into different sets as required for the embedding sub-process to take place. Then, the CPU side will need to prepare and package the necessary bit stream needed for embedding. After this, the actual embedding sub-process will be able to take place in GPU by adopting similar strategy where each thread handling one member in the vectors.

In the authentication process, the set classification sub-process is identical to the set classification sub-process in embedding process with minor difference in the classification condition. On the other hand, the region recovery sub-process in authentication operation, as its name suggest, removes the embedded bit stream from ROI and RONI vector, thus recovers the original image. It is in fact the reverse of the embedding sub-process in embedding operation. Therefore, similar strategy is adopted for them.

V. Experimental Result

To evaluate the effectiveness and practicality of the scheme provided, a series of experiments were conducted and their respective results are presented in the following sections. In these experiments, samples of public domain mammograms from the mini-MIAS database of mammograms were utilized [17].

A. Automatic ROI Selection

We have repeatedly evaluated the effectiveness of the proposed automatic ROI selection algorithm. Here we give one specific case for illustration purpose. Fig. 1 (a) the original mammogram image used for this case study while Fig. 1 (b), (c) (d) shows the ROI map generated using three methods. Here, white pixels represent the ROI and black pixels represent the RONI). Figure 1 (b) shows the ROI map constructed by direct binarizing the original input mammogram and 0(c) shows the ROI map constructed through binarizing the saliency map of the input

mammogram. 0(d) shows the ROI map constructed from thresholding the saliency map of the input mammograms using IMPT which the algorithm proposed herein. It is found that using the proposed algorithm; we can generate a smoother and compact ROI.

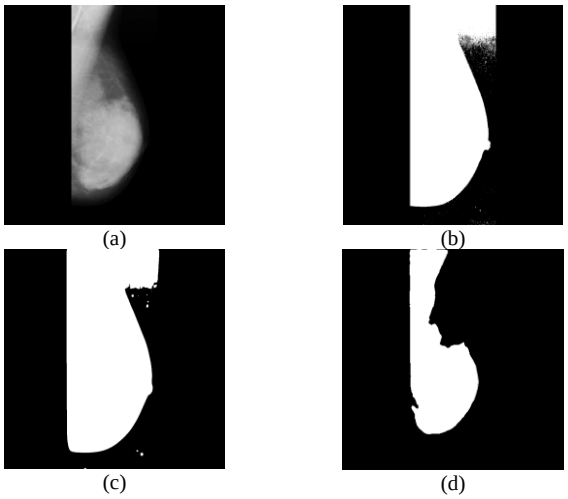

Fig. 1. This figure shows (a) the original mammogram, (b) the ROI obtained with direct thresholding (c) the ROI obtained via saliency map + direct thresholding and (d) the ROI obtained via saliency map + improved moment invariant thresholding.

B. Visual Quality

Seven mammograms of different class of abnormality present with same image dimensions were used to test our scheme. All the mammograms used are of the same size (1024x1024). 0shows one of the mammograms used to test the scheme in its original version and watermarked version. In TABLE I. we present the results of the embedding process obtained by the scheme. Here, G denotes "fatty-glandular" and D denotes "dense-glandular" in background tissue column in the table. There are seven classes of abnormality present of the mammograms (in the third column): calcification denoted as CALC, circumscribed masses denoted as CIRC, spiculated masses denoted as SPIC, ill-defined masses denoted as MISC, architectural distortion denoted as ARCH, asymmetry denoted as ASYM, and normal denoted as NORM.

The watermarked mammograms show good visual quality in term of Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity (SSIM). The mammograms authentication scheme also shows high embedding capacity (with average of >0.53). The watermarked mammograms by the scheme were proven reversible by comparing the extracted mammograms with the original mammograms pixel by pixel. The authenticity of ROI can also be verified by comparing the embedded hash extracted with the recalculated hash of the reconstructed (reversed) ROI. From the results, the original mammograms can be reconstructed exactly in case of no tamper detected.

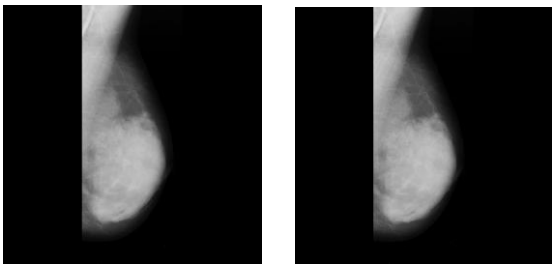

Fig. 2. (a) Original "mdb038.pgm". (b) Watermarked "mdb038.pgm".

C. Speed Enhancement between CPU and GPU

In order to compare the performance between the CPU implementation and the GPU implementation, we conducted a series of experiments with various image size as tabulated in Table II. The processing time for the embedding process of the images of different size of the scheme in MATLAB, the CPU implementation of the scheme (using OpenCV), and the GPU implementation scheme were presented here. In these experiments, the hardware platform used was a PC workstation equipped with Intel Core2 Quad Q9400 2.66GHz as CPU and a NVIDIA GeForce 9500 GS Graphics card.

TABLE I: EMBEDDING RESULTS FOR 7 MAMMOGRAMS OF DIFFERENT CLASS OF ABNORMALITY PRESENT

Image	Chracter of background tissue	Class of abnormality present	Image size	Size of ROI (%)	Embedding capacity (bpp)	PSNR	SSIM
mdb001.pgm	G	CIRC	1024×1024	26.5	0.53	45.73	0.9798
mdb038.pgm	D	NORM	1024×1024	21.7	0.52	46.41	0.9809
mdb072.pgm	G	ASYM	1024×1024	21.5	0.51	46.91	0.9813
mdb124.pgm	G	ARCH	1024×1024	24.5	0.54	46.38	0.9822
mdb175.pgm	G	SPIC	1024×1024	30.4	0.54	45.28	0.9770
mdb211.pgm	G	CALC	1024×1024	34.2	0.53	45.36	0.9776
mdb264.pgm	G	MISC	1024×1024	37.5	0.58	44.79	0.9777

TABLE II: PROCESSING TIME FOR THE EMBEDDING PROCESS

Image Size	Processing Time		
	MATLAB (s)	CPU (ms)	GPU (ms)
456 ×600	53.306	32.454	50.048
912 ×1200	206.288	125.974	138.807
1368 ×1800	496.096	259.871	263.809
1824 ×2400	873.349	453.139	430.941
2280 ×3000	1361.443	737.728	646.130
2736 ×3600	1966.086	993.222	910.394

As observed from the results, the speed improvement of CUDA is more visibly observed when the image size is large. At small image size, the overall embedding operation was overwhelmed by the time required for data transferring between CPU and CPU memory. However, as data size grows, this dominating factor become less significant where the processing of data took over most of the overall processing time.

VI. Conclusion

In this paper, we proposed a ROI-based reversible fragile watermarking scheme for mammograms using the two difference expansion watermarking methods. The scheme defined the ROI automatically by using the selective visual attention-driven model proposed by Feng et al. and then binarized the saliency map constructed by improved moment-preserving threshold.

Our scheme automatically fine tunes the embedding threshold to increase the embedding capacity of the given mammogram. Besides, the scheme reconstructs the original mammograms from the watermarked mammograms as it is proven to be authentic. The scheme exhibit high visual quality as reflected from the PSNR values and SSIM values reported.

In terms of the speed improvement, CUDA platform was utilized. While a marginal speed improvement was observed, it was less than our expectation. For future works, we will investigate other means of optimization methods in CUDA implementation to further boost the speed performance.

Acknowledgment

This work was supported in part by Malaysian Government's MOSTI ScienceFund 01-02-14-SF0005.

References

[1] M. Awrangjeb, "An overview of reversible data hiding," in *Proc. the 6th International Conference on Computer and Information Technology (ICCT-03)*, pp. 74-79, 2003.

[2] D. Anand and U. C. Niranjam, "Watermarking medical images with patient information," in *Proc. 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS)*, pp.703-706, 1998.

[3] J. Tian, "Reversible watermarking by difference expansion," in *Proc. of Workshop on Multimedia and Security: Authentication, Secrecy, and Steganalysis*, J. Dittmann, J. Fridrich, and P. Wohlmacher, Eds., pp. 19-22, 2002.

[4] A. M. Alattar, "Reversible watermark using difference expansion of triplets," in *Proc. the 2003 IEEE International Conference on Image Processing*, vol. 1, pp. 501-504, 2003.

[5] A. M. Alattar, "Reversible watermark using difference expansion of quads," in *Proc. the IEEE International Conference on Acoustics, Speech, and Signal Processing*, vol. 3, pp. 377-380, 2004.

[6] O. M. Al-Qershi and B. E. Khoo, "Authentication and data hiding using a reversible ROI-Based watermarking scheme for DICOM images," in *Proc. World Academy of Science, Engineering and Technology*, vol. 38, pp. 829-834, Feb. 2009.

[7] X. Guo and T.-g. Zhuang, "A region-based lossless watermarking scheme for enhancing security of medical data," *Journal of Digital Imaging*, vol. 0, pp. 1-12, 2007.

[8] U. Bick, M. L. Giger, R. A. Schmidt, R. M. Nishikawa, D. E. Wolverton, and K. Doir, "Automated segmentation of digitized mammograms," *Academic Radiology*, vol. 2, no. 2, pp. 1-9, 1995.

[9] F. F. Yin, M. L. Giger, K. Doi, C. E. Metz, C. J. Vyborny, and R. A. Schmidt, "Computerized detection of masses in digital mammograms: Analysis of bilateral subtraction images," *Medical Physics*, vol. 18, no. 5, pp. 955-963, 1991.

[10] A. J. Mendez, P. J. Tahoces, M. J. Lado, M. Souto, J. L. Correa, and J. J. Vidal, "Automatic detection of breast border and nipple in digital mammograms," *Computer Methods and Programs in Biomedicine*, vol. 49, pp. 253-262, 1996.

[11] R. Chandrasekhar and Y. Attikiouzel, "Automatic breast border segmentation by background modeling and subtraction," in *Proc. the 5th International Workshop on Digital Mammography*, pp. 560-565, 2000.

[12] M. Wirth, D. Nikitenko, and J. Lyon, "Segmentation of the breast region in mammograms using a rule-based fuzzy reasoning algorithm," *International Congress for Global Science and Technology (ICGST) on Graphics, Vision and Image Processing (GVIP)*, vol. 5, no. 2, pp. 45-54, 2005.

[13] M. A. Wirth and A. Stapinski, "Segmentation of the breast region in mammograms using active contours," in *Proc. Visual Communications and Image Processing*, vol. 5150, pp. 1995-2006, 2003.

[14] S. Feng, D. Xu, and X. Yang, "Attention-driven salient edge(s) and region(s) extraction with application to CBIR," *Signal Processing*, vol. 90, no. 1, pp. 1-15, 2010.

[15] L. Itti, C. Koch, and E. Niebur, "A model of saliency-based visual attention for rapid scene analysis," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 11, pp. 1254–1259, 1998.

[16] I. P. Chen, M. Y. Lai, and L. L. Wang, "An improvement in the moment-preserving thresholding method," *International Journal of Imaging Systems and Technology*, vol. 18, no. 5-6, pp. 365-370, 2008.

[17] The mini-MIAS database of mammograms. *Mammographic Image Analysis*. (31 Jul. 2003). [Online]. Available: http://peipa.essex.ac.uk/info/mias.html

M. L. Dennis Wong received his BEng (Hons) in Electronics and Communication Engineering and his PhD from the Department of Electrical Engineering and Electronics, University of Liverpool, Merseyside, U.K. in 1999 and 2004 respectively. Currently, he is the Acting Dean for Faculty of Engineering, Computing and Science, Swinburne University of Technology Sarawak Campus, Malaysia. Prior to his current appointment, he was a Lecturer, a Senior Lecturer, later the Associate Head of School (Engineering) at the School of Engineering, Computing and Science, Swinburne Sarawak from 2004 to 2011. From mid-2011, he was an Associate Professor at the Department of Electrical and Electronic Engineering, Xi'an Jiaotong Liverpool University (XJTLU), Suzhou, Jiangsu Province, China. His research interests include statistical signal processing and pattern classification, machine condition monitoring, and VLSI Design for digital signal processing. Dr. Wong is a Senior Member of the IEEE and a Member of the IET.

Jack S. I. Lau received his BEng (Hons) from Multimedia University in 2008. He is currently pursuing a Master of Engineering by Research at Swinburne University of Technology, Sarawak Campus. His research interests are biomedical media authentication and fragile watermarking schemes.

N. S. Chong received his BEng Robotics and Mechatronics Engineering with First Class Honours from Swinburne University of Technology Sarawak Campus, Malaysia. He is currently a PhD candidate at Swinburne Sarawak. His research interests include omnidirectional vision, hardware accelerated platform, and robotic navigation.

K. Y. Sim received his BEng (Hons) from the National University of Malaysia in 1999 and Masters of Computer Science from University of Malaya, Malaysia in 2001. He is currently a Senior Lecturer and the Associate Head for Program Development and Accreditation at the School of Engineering, Computing and Science, Swinburne University of Technology, Sarawak Campus, Malaysia. His research interests include software testing and for embedded system testing. Mr. Sim is a member of IEEE and IEEE Computer Society.