Wavelet Based Color Video Steganography

Anush Kolakalur, Ioannis Kagalidis, and Branislav Vuksanovic, *Member IACSIT*

***Abstract*—This paper describes the algorithm developed with the aim to hide a "secret" color video sequence within another color video sequence. An approach to apply a wavelet transform in order to decompose the cover video sequence and then replace the less significant wavelet band with "secret" video frames has been implemented and tested. On the receiver side, process is reversed and the hidden color video recovered from stego color video. Proposed algorithm has been implemented using Mat lab and PSNR and MSE error metrics employed to evaluate the quality of both video sequences.**

***Index Terms*—Discrete wavelets transform (DWT), LSB, PSNR, and Steganography.**

I. Introduction

Steganography is a science of hiding data or messages within other data or a message. It is one of the ways of achieving safe, secure and covert communication. In a perfectly secure system, a normal message should be indistinguishable from a stego-object, and therefore undetectable by a human or by a computer looking for patterns [1], [2].

Practically, this is not always the case. In order to embed covert data into a carrier message, the carrier data must contain a certain amount of insignificant data or noise. This helps the embedding process by replacing this data or noise with the data which is secret and needs to be hidden from intruders. While enabling the use of steganography, this distortion of original, carrier data can limit the use of some data types and formats for steganography applications [3].

Small amount of redundant noise or data makes a text based steganography a difficult task to achieve. Thus, it is very easy for a third party to modify data in text based steganography by altering the text itself or by changing the format of the text containing the file (e.g. from .TXT to .PDF, etc.). Some popular text based steganography methods have been recently summarized and described in details [3].

Line-shift encoding is one of the popular techniques where each line of text is shifted up or down vertically by minimum of 3cm. The covert message is encrypted according to the position of the line whether it was up or down vertically from the original line [4]

Word-shifting encryption principle is similar to that of line-shift encryption; this method hides covert messages in-between horizontal spaces of words. Visibility of covert messages in this method is almost negligible. Both of the mentioned methods require either the original file or the knowledge of the original files alterations to be able to decrypt the covert information [4].

Manuscript received November 15, 2014; revised February 2, 2015.

The authors are with the School of Engineering, University of Portsmouth, and Hants. PO13DJ, UK (e-mail: anush.kolakalur@myport.ac.uk, ioannis.kagalidis@port.ac.uk, branislav.vuksanovic@port.ac.uk

Hiding covert information in digital images has become a widely researched subject in the recent years. It relies and takes advantage of the limited ability of the human visual system (HVS) [1], [2]. Digital images used in steganography are typically 8-bit and 24-bit per pixel images with each image type coming with its own advantages and disadvantages. As an advantage, 8-bit images are relatively small in size, but the potential drawback is that only 256 possible colors or grey levels can be utilized in encryption. 24-bit images are more flexible compared to 8-bit images [4], although the obvious drawback is that the large size can make them more prone to be suspected when shared over an open system environment. A possible solution to overcome the aforementioned drawback with 24-bit per pixel images is to apply digital image compression [2], although care has to be taken when selecting the particular image compression technique. Lossy compression might help in reducing the size of 24-bit digital images but the parts of the hidden information could be lost during the compression process. Lossless image compression avoids this pitfall but the achieved compression might not be significant. Popular digital image encoding techniques used recently are least significant bit encryption methods [5] and masking and filtering techniques [6]. Other, more robust techniques such as complex algorithms, image transformation techniques and image encryption techniques have been recently reported and described [7].

A. Video Steganography

Video steganography refers to techniques used to hide video data within another video data. The most popular and convenient technique used for video steganography is the least significant bit (LSB) substitution technique, very much similar to the same method used for image steganography.

Recently, a modification to the traditional LSB technique by replacing LSB bits by LSB+3 bits has been proposed [8]. Utilization of integer wavelet transforms in video steganography has also been presented [9] and the possibility of extending the scheme to color images proposed. Use of discrete cosine transform (DCT) in combination with LSB has been reported[10], although in this scheme only text data have been hidden as well as retrieved from the cover video file.

The developments to hide more complex data inside a video can be achieved by the implementation of two-dimensional discrete wavelets transforms (DWT2). The more detailed discussion of the DWT2working and implementation in this work is illustrated in the following sections.

B. Discrete Wavelets Transforms

Wavelet transform is one of the established techniques to accomplish time-frequency transformation of a signal or image. In many cases it is considered to be superior to Fourier

DOI: 10.7763/IJET.2016.V8.878

transform due to the fact that wavelets can capture frequency as well as location-in-time information about the analyzed waveform or image [11]. In fact transform domain techniques have been shown to hold better to decryption attempts and attacks[12], [13]. Some of the often used discrete wavelet transforms include Haar, Daubechies and Symlets wavelets.

One of the oldest and simplest wavelet transforms is the Haar wavelet. This transform cross multiplies a function or a given waveform with the Haar wavelet with various shifts and stretches. Main concept of Daubechies wavelets is similar to that of Haar wavelets but the two methods differ in the way scaling and wavelets are defined. Here, a scaling function called "father" wavelet generates multi resolution orthogonal observations [14]. Symlets are a part of the wavelet family and a modified version of Daubechies with enhanced symmetry [15], [16].

C. Wavelet Based Steganography

Wavelet transformation is usually accomplished through two stages - quantization and encoding. Methods for embedding data or information which needs to be hidden are usually applied after the wavelet transformation. The coefficients obtained after the application of discrete wavelet transforms are modified according to the stego data - data which requires hiding with the aim to be reconstructed once the data has been received at the end of the hiding process. The hidden data is retrieved by reversing the hiding process and applying the inverse discrete wavelet transform application on the stego image [17], [18]. This process is illustrated in Fig. 1.

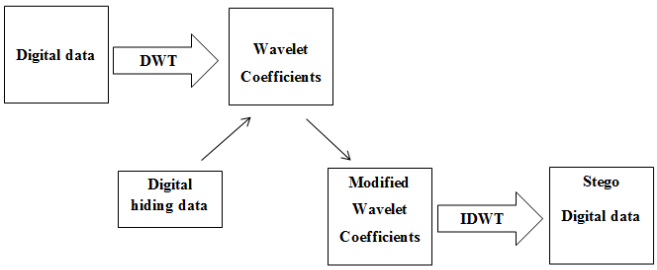


Fig. 1. Embedding process using DWT and IDWT.

II. Algorithm Development

Development of the video steganography method described in this work followed five different stages. First, a technique aimed at hiding a grey scale image in another grey scale image has been developed and tested, followed by the extension of this approach in order to hide a grey scale image in another color type image. This has then been modified into an algorithm able to hide a single grey scale image in a number of RGB or color images and further into a method to hide multiple grey scale images, i.e. a grey scale video in streaming color images or color video. Finally a two stage algorithm to hide a color sequence in another color sequence using wavelet bands was developed as well as the way of inversing the encryption algorithm in order to reconstruct the wavelets to the stego video.

Fig. 2 shows the first part of the encryption process which can be summarized in the following nine steps:

1) The cover color video is broken down in red, green and blue channels.
2) The secret color video is also broken down in red, green and blue channels.
3) The red channels are extracted from the cover color video and wavelet transformed into four wavelet bands.
4) The total numbers of cover color video frames are divided into 3 equal blocks (i.e. if the total number of cover color video frames are 300, then each block has 100 frames).
5) All of the blocks having 100 frames of the cover color video each are wavelet transformed and wavelet bands are obtained.
6) In the 300 HH bands, first 100 HH bands are replaced with 100 red channels of secret color video frames, second 100 HH bands are replaced with 100 green channels of secret color video frames and third 100 HH bands are replaced with 100 blue channels of secret color video frames.
7) In this step, the stego red channels are reconstructed with modified bands. This reconstruction process results in stego red channels of cover color video.
8) The stego red channels are concatenated with untouched green and blue channels to obtained stego video frames.
9) The frames are stitched sequentially to obtain a color video which is known as the stego video and is identical to the cover color video.

III. Testing

This section illustrates the testing of three of the five stages, i.e. intermediate algorithms and provides results obtained during the algorithm development.

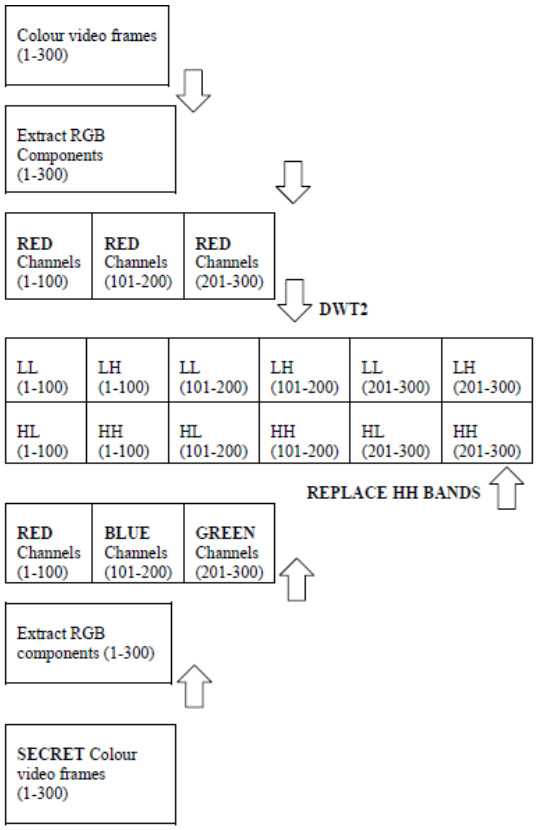


Fig. 2. Hiding the channels of secret video are in the HH bands of red channels of cover video.

A. Grey Scale Image Hidden in a Color Video

The formats considered for testing at this stage are avi, mp4, 3gp and mov as the PSNR values of these formats do not differ drastically. The testing is carried out by hiding the covert grey scale image in a color video of 10 seconds duration with a frame rate of 30 frames per second (30×10=300 video frames). Each of the 300 frames has the same grey scale image hidden in them.

Fig. 4 illustrates four randomly selected stego video frames which are compared with corresponding original cover video frames. Although differences can be detected by the HVS when those selected images are magnified, the PSNR values are still high (in the range of 35-36 dB).

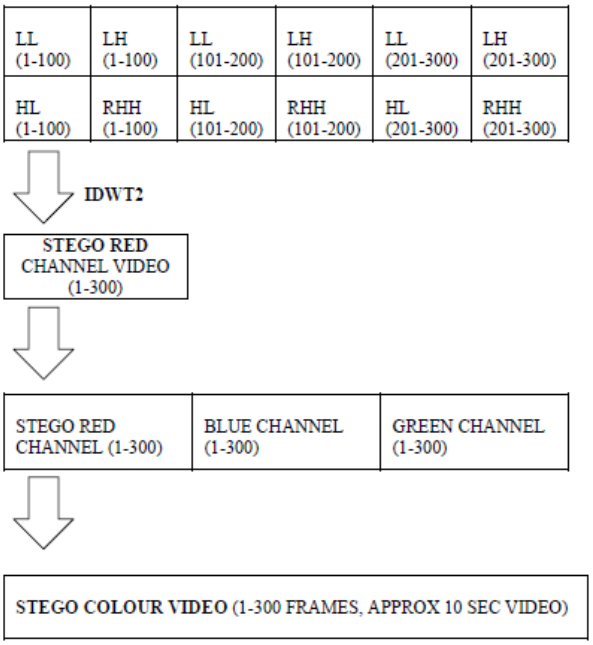


Fig. 3. Generation of stego colour video (REPLACED HH BANDS= RHH).

Fig. 4. Selected stego video and the corresponding cover video frames.

The PSNR figure for the retrieved covert grey scale image scaled up by integer 3in this example, shown in Fig. 5 is 19 dB.

B. Grey Scale Video Hidden in Color Video

The testing of this step is carried out by hiding the covert grey scale video of 5 seconds duration in a color video of 10 seconds duration with both videos having the same frame rate of 30 frames per second. The first 150 frames of the color cover video are used by the algorithm and each of them had first 150 of the same grey scale video frames as covert image hidden in them. The frames are retrieved sequentially from the first 150 frames of color cover video and stitched into a grey scale video.

Fig. 6 shows stego frames 30and 150, the corresponding hidden grey scale video frames, and resultant corresponding retrieved grey scale video frames after up-scaling by an integer of 3.

C. Color Video Hidden in Another Color Video

The final version of the algorithm is tested on "avi" format videos. Fig. 7 shows three corresponding frames, one from each block of the stego color video where each of the frames has any one component of the hidden video frame (i.e. red, green and blue in a sequentially order of video frames).

The retrieved color video is shown in Fig. 8 which shows the original retrieved video frame and integer multiplied by 2 and 3 with improved PSNR values.

Fig. 5. Retrieved covert grey scale image.

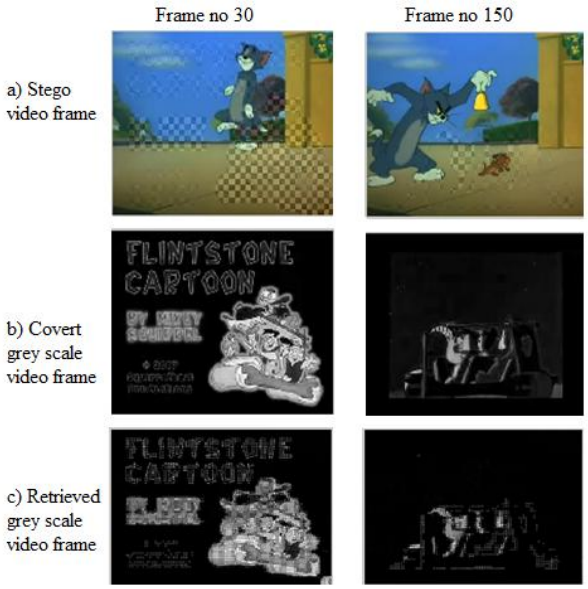
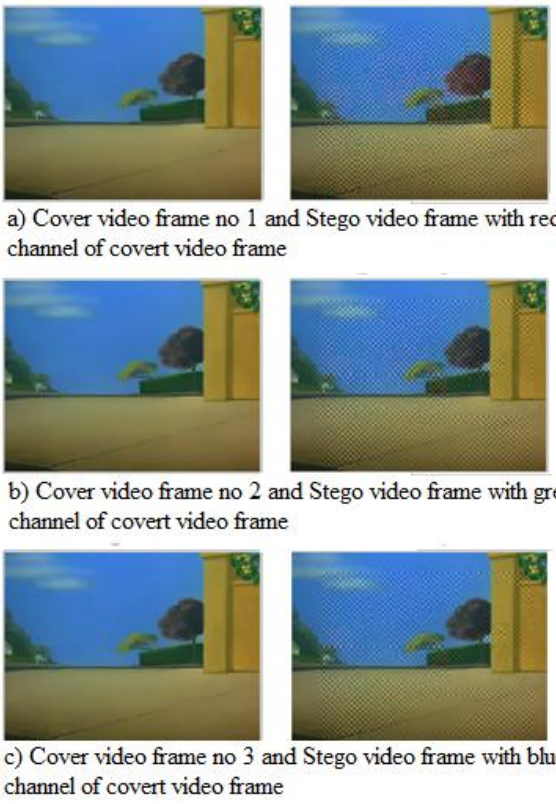


Fig. 6. Stego frames 30 and 150, the corresponding hidden grey scale video frames, and resultant corresponding retrieved grey scale video frames after up scaling by integer 3.

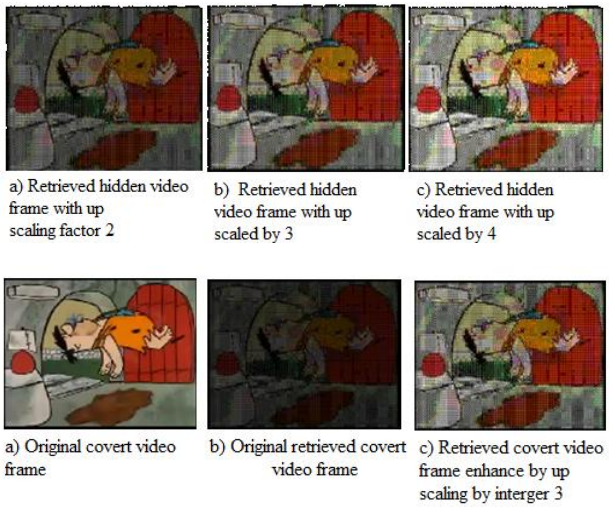


a) Cover video frame no 1 and Stego video frame with red channel of covert video frame

b) Cover video frame no 2 and Stego video frame with green channel of covert video frame

c) Cover video frame no 3 and Stego video frame with blue channel of covert video frame

Fig. 7. Three corresponding frames, one from each block from the stego color video; each of the frames has any one component.



a) Retrieved hidden video frame with up scaling factor 2

b) Retrieved hidden video frame with up scaled by 3

c) Retrieved hidden video frame with up scaled by 4

a) Original covert video frame

b) Original retrieved covert video frame

c) Retrieved covert video frame enhance by up scaling by interger 3

Fig. 8. Two retrieved video frames with different scaling.

IV. Results

Table I shows the PSNR values achieved with different wavelet types used in testing.

TABLE I: PSNR (dB) Values of Different Wavelets

Wavelet type	HAAR	Db1	Db2	Db10	Db20
Stego image	47.813	47.813	47.8535	47.97	47.9872
Retrieved image	61.4620	61.4620	61.5020	62.11	62.13

Table II shows the PSNR values for the same videos with different formats which were used in the testing. The PSNR values for all the formats are in the range between 31 and 32 dB thus the developed algorithm is suitable to be applied to any of those formats.

TABLE II: PSNR Values for Same Videos with Different Formats PSNR Values dB

.wmv	*.avi*	*.mp4*	*.3gp*	*.mov*
32.3716	31.4944	31.4164	31.5622	31.4850

TABLE III: Shows the PSNR Values for Retrieved Color Video with Different Integer Multiplications PSNR Values for Different Scaled Retrieved Frame

Without any scaling	x2 scaling	x3 scaling	x4scaling
11.9057	15.6069	20.0816	18.9357

Table III shows the PSNR values for retrieved color video with different scaling. The computation error is the cause of the poor quality in the retrieved video reflected in the PSNR values in the range of 9 to 10 dB after retrieving the color video from the cover color video. In order to enhance the quality of the retrieved video the image elements are scaled up in each. Results are shown on Table III indicating significant improvement when integer 3 up scaling is applied. However, if the integer multiplier is greater than a threshold integer, then the quality degrades. It could be concluded that the decryption process is feasible and quality of the retrieved video is indicated by the acceptable PSNR figures.

Table IV shows the PSNR values and MSE of stego color video along with retrieved color video, also shows PSNR and MSE for different types of wavelets with execution time measured for encryption and decryption.

TABLE IV: Shows the PSNR and MSE Values for Various Wavelets Tested and Their Execution Time

Wavelet types	PSNR value (dB)		MSE value		Code execution time or code run time or computation time	
	Output Video	Retrieved hidden video	Output Video	Retrieved hidden video	Encryption code	Decryption code
Haar	35.2015	20.7176	19.6304	551.2147	165.557s	82.212s
Symlets2	35.2066	20.5646	19.6076	570.9807	171.607s	87.819s
Symlets5	35.1287	20.5378	19.9623	574.5073	212.570s	93.507s
Symlets10	35.0337	20.6136	20.4040	564.5747	249.969s	139.163s
Symlets15	34.9524	20.6531	20.7891	559.4612	376.623s	199.829s
Symlets20	34.8594	20.6839	21.2394	555.5051	1353.698s	695.973s
Daubechies2	35.2066	20.5646	19.6076	570.9807	175.800 s	92.872 s
Daubechies5	35.1702	20.5906	19.7724	567.5664	186.353 s	100.993s
Daubechies10	35.1179	20.6489	20.0119	559.9998	197.968s	97.632s
Daubechies15	35.0771	20.7044	20.2009	552.8981	279.704s	118.550s
Daubechies20	36.3183	20.4778	15.1791	582.5005	309.864s	132.678s

Although, it is evident from the table that Haar and Db20 wavelets performance is very close, computation time for Haar wavelet is significantly shorter compared to Db20. Daubechies20 have a slight edge over the Haar in terms of stego video PSNR and Haar have a slight edge in terms of retrieved video PSNR. Considering both points, it can be concluded that the use of Db20 is superior and Daubechies20 is the wavelet chosen in the algorithm.

Since the PSNR value is in the range above 30, the encryption process is feasible and this process resultant video i.e. the stego video is imperceptible whilst data transmission.

V. Conclusion

A color video within video hiding algorithm has been proposed in this paper and stages of the algorithm development illustrated. The algorithm has been implemented in Mat lab and various tests regarding the quality of encoded video and carrier video as well as computational time needed to complete the encryption of a short video sequence measured. The results indicate the feasibility of the proposed approach although the computational requirements are significant. The results correspond with parts of [19], [20] and are also somewhat inferior to those achieved using hybrid wavelet transforms on images but illustrate the feasibility of the application of wavelets for video steganography.

The PSNR value of nearly 37 dB indicates the quality of the covert video in stego video. The PSNR value of nearly 21 dB, shown in Table III and illustrated in Figure 8 indicate the feasibility of retrieving process of the covert video and the potential of the proposed algorithm.

Various video format sand types of wavelet transform have been tested. Some indication of the optimal selection has also been given in the results section, Table I and II.

References

[1] I. J Cox, *Digital Watermarking and Steganography*, 2nd ed. Amsterdam, Netherlands: Morgan Kaufmann Publishers, 2008.

[2] K. S. Petitcolas and A. P. Fabien, *Information Hiding Techniques for Steganography and Digital Watermarking*, Boston: Artech House, 2000.

[3] Wikipedia, the Free Encyclopedia. (July, 2014). [Online]. Available: http://www.en.wikipedia.org/wiki/Steganography"http://en.wikipedia.org/wiki/Steganography

[4] Xdata Security. (2014). [Online]. Available: HYPERLINK http://www.xdatasecurity.com/about-steganography/introduction-to-steganography-and-watermarking.htm.

[5] A. McAndrew, *Introduction to Digital Image Processing with Matlab, Mac Mendelsohn*, Ed. Massachusetts, USA: Course Technology, 2004.

[6] H. Maitre, *Image Processing*, 1st ed. London, UK: ISTE Ltd, 2008.

[7] R. E. Woods, S. L Eddins, and R. C. Gonzalez, *Digital Image Processing Using Matlab*, Second ed. USA: Gatesmark, LLC, 2009.

[8] P. Bhautmage, A .Jeykumar, and A. Dahatonde, "Advanced Video Steganography Algorithm," *International Journal of Engineering Research and Applications(IJERA)*, vol. 3, no. 1, pp. 1641-1644, February 2013.

[9] K. L. Narayanan, G. Prabakaran, and R Bhavani, "A high capacity video steganography based on interger wavelet transform," *Journal of Computer Appilications,* vol. 5, no. EICA2012-4, February 2012.

[10] P. V. Bodhak and B. L Gunjal, "Improved protection in video steganography using DCT and LSB," *International Journal of Engineering and Innovative Technology (IJEIT)*, vol. 1, no. 4, April 2012.

[11] N. Moldovyan and A. Moldovyan, *Innovative Cryptography*, Boston: Charles River Media, 2007.

[12] S. Thepade and S. Chavan, "Appraise of multifarious image steganography techniques," *International Journal of Engineering Research and Applications*, vol. 3, no. 2, pp.1067-1174.

[13] H. B. Kekre, A. B. Patankar, and D. Koshti, "Performance comparison of simple orthogonal transforms and wavelet transforms for image steganography," *International Journal of Computer Applications*, vol. 44, no. 6, April 2012

[14] H. Jahankhani, *Handbook of Electronic Security and Digital Forensics*, Singapore: World Scientific, 2010.

[15] B. J. Blake, *Secret Language*, Oxford, UK: Oxford University Press, 2010.

[16] F. Keinert, *Wavelets and multiwavelets*, London, UK: Chapman & Hall/CRC, 2004.

[17] M. Holschneider, *Wavelets: An Analysis Tool*, Oxford, UK: Clarendon Press, 1995.

[18] M. D. Valle, R. M. Guerrero, and J. M. G. Salgado, *Wavelets Electronic Resource: Classification, Theory and Applications*, Hauppauge, N.Y: Nova Science Publishers, 2012.

[19] S. D. Thepade and S. S. Chavan, "Robust image steganography with wavelet transform and Hybrid wavelet transform generated using Kekre, Walsh and sine transforms," in *Proc. the 'ICACCI',* IEEE, 2013, pp. 1964-1969 .

[20] H. B Kekre, A Athawale, P. N Halarnkar, and V. K. Banura, "Performance comparison of DCT and walsh transform for steganography," in *Proc. the International Conference and Workshop on Emerging Trends in Technology (ICWET 2010)*, 2010, pp. 81-88.

Anush Kolakalur completed his MSc in communication system engineering from University of Portsmouth, United Kingdom. He is a student member of IET. His rearch interests inculde cryptography, steganography, communication security and cyber security.

Ioannis Kagalid was graduated from the University of Leeds with a degree in electronic and electrical engineering. He attended the University of Portsmouth Postgraduate Course and graduated with an MSc degree in control technology. He joined the University of Portsmouth Robotics Research Group and He received his PhD in cooperation by observation for heterogeneous robots. During his academic career he worked briefly as a lecturer in the Department of Computer Science and Mathematics in the University of Portsmouth before joining the School of Engineering in the University of Portsmouth where he is currently working as a senior lecturer. His current research interests are in robotics, sensor fusion and artificial intelligence.

Branislav Vuksanovic was graduated from the University of Belgrade, Serbia with degree in electrical and power engineering. He holds MSc degree in measurement and instrumentation from South Bank University, London and a PhD in active noise control from the University of Huddersfield, UK. Previously, he worked as a project engineer for Croatian Electricity Board in Osijek, Croatia. During his academic career he worked as a research fellow at Sheffield and Birmingham Universities on Optical Brain Imaging and Medical Video Compression projects. He also worked as a lecturer at the University of Derby where he was a member of Sensors and Controls Research Group. Currently he works as a senior lecturer at the University of Portsmouth, School of Engineering. He has published papers in the field of active noise control, biomedical signal processing and pattern recognition for intrusion detection and knowledge based authentication. He published one book in digital electronics and microcontrollers field. Dr Branislav Vuksanovic is a member of IET, ILT and IACSIT. His current research interests are in the application of pattern recognition techniques for power systems and analysis of ground penetrating radar and ECG data.