Image Authentication and Restoration Using Digital Watermarking by Quantization of Integer Wavelet Transform Coefficients

Tanveer Ahsan*, Ui-pil Chong*

Abstract

An image authentication scheme for gray scale image through embedding a digital watermark by quantization of Integer Wavelet Transform (IWT) coefficients of the image is proposed in this paper. Proposed method is designed to detect modification of an image and to identify tampered location of the image. To embed the watermark mid-frequency band of a second level IWT was used. An approximation of the original image based on LL band was stored in LSB bits of the pixel data as a recovery mark for restoration of the image. Watermarked image has achieved a good PSNR of 40 dB compared to original cover image. Restored image quality was also very good with a PSNR of more than 35 dB compared to unmodified watermarked image even when 25% of the received image is cropped. Thus, the proposed method ensures a proper balance between the fidelity of the watermarked image and the quality of the restored image.

Keywords : Integer Wavelet Transform, Digital Watermarking, Image Authentication, Tamper Localization, Image Restoration

I. Introduction

Digital media has opened a great opportunity for dealing with multimedia data like image, sound, video with a great ease but at the same time has brought some challenges to solve. Digital images are very easy to modify and this opportunity, as a consequence, makes it harder for a person to be sure whether this image is an authentic one or altered in some way after capture. Hence, the issue of designing authentication scheme for an image comes. There are a handful of ways to authenticate an image. For example, one method for answering the question whether an image has been altered at all is to append a cryptographic signature to it [1]. However, using digital watermark to authenticate an image has some advantages. First advantage is that, with digital watermarking, the requirement for storing a separate metadata is removed. Secondly, any changes to the image directly affects watermark embedded in the image. Thus, by comparing against a known reference mark, it is possible to detect what and where the changes in the image happened.One of the earliest and most explored methods to authenticate JPEG image is due to Lin and Chang [2] who proposed to insert authentication data in the JPEG coefficients. Wong [3-4] proposed some secret and public key based watermarking schemes which allow a user with an appropriate key to verify the integrity of an image. Later, Wong and Memon [5] proposed a further developed scheme to resist vector quantization attack. Fridrich and Goljan [6-7], for the first time, proposed some watermarking schemes that can both localize the tampered location of an image and reconstruct the corrupted image by self-embedding a low resolution version of the image in it. In this method, a low resolution copy of the cover image of 50% jpeg quality is embedded in the LSB area of the cover image. Ke et al also proposed a scheme for restoration of tampered image [8]. Ho et al proposed a z-transformed based scheme to authenticate digital image in pixel level [9]. Lin and Yang proposed a multipurpose digital watermarking technique based on vector quantization [10]. Xiao et al [11] proposed an improvement of the semi-fragile method proposed in [2]. Zou et al [12] and Coelho et al [13] proposed integer wavelet transform based image authentication scheme. However, none of the method proposed in [9-13] addressed the problem of restoration of image.

In the literature, it is found that the major focus is given on identification of fake and tampered image. Reconstruction of image is given less attention as it demands some compromise both in the quality of the watermarked image and also in the quality of the restored image. Sometimes, when the quality of the restored image is good, the fidelity of watermarked image is compromised. Chang et al proposed an

* 울산대학교 전기공학과
투고 일자 : 2012. 7. 13 수정완료일자 : 2012. 10. 31
게재확정일자 : 2012. 11. 3
* This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (No. 2012-0004513)

SVD oriented watermark scheme capable of producing high quality restored image [14]. But, in that scheme the watermarked images have achieved PSNR in the range of 30-35 dB which is a little bit low. The proposed approach is designed to ensure a balance between this two, i.e. to ensure good fidelity of the watermarked image as well as the quality of the reconstructed image.

Usage of wavelet transform in the digital image processing has gained popularity in recent times. One of the most popular applications of discrete wavelet transform is in the JPEG2000 image compression scheme whereas its predecessor, JPEG standard, was DCT based. Discrete wavelet transform is also being used in the domain of digital watermarking. Kundur and Hatzinakos proposed a fragile watermarking scheme for tamper proofing, where the watermark is embedded by quantizing the DWT coefficients [15]. One of the main advantages of using DWT is its power in multi-resolution analysis. This capacity was exploited in the proposed scheme to encode a low resolution version of the image and embed it in the original image.

Spread spectrum watermarking method has been a popular choice for watermarking digital media with the purpose of protecting owner's copyright. However, it was found empirically that for authentication purpose quantization based watermarking performs better than spread spectrum watermarking [16].

This paper proposes a novel method for authentication of grayscale image by using digital watermarking. The proposed method embeds a digital watermark in a grayscale image by the process of quantization of the grayscale values of the pixels of an image. To embed the watermark, mid-frequency bands of a second level wavelet transform was used to ensure both the fidelity of watermarked image and the accuracy of tamper detection. A low resolution version of the original image was stored in the LSBs of the watermarked image to recover a tampered image. The method designed with a goal to ensure a better balance between the fidelity of watermarked image and the quality of reconstructed image.

II. Integer Wavelet Transform

Discrete Wavelet Transform (DWT) is suitable for identifying the areas of the cover image where a watermark can be imperceptibly embedded because of its excellent spatio-frequency localization properties. The integer wavelet transform is a specialized version of general DWT which maps integers to integers. In fact, Integer Wavelet Transform is essentially a Discrete Wavelet Transform. However, the advantage of using integer wavelet transform is that it can be implemented with only fundamental arithmetic operations.

In integer wavelet transform, the image is first decomposed in 4 subbands, LL_1, HL_1, LH_1 and HH_1 respectively. The LL_1 band is further decomposed into four subbands obtaining LL_2, HL_2, LH_2 and HH_2. This decomposition can be performed as many times as required. The LL band, or more specifically LL_k band of IWT contains the low frequency components of the image and it can be treated as an approximation of the image. Here **k** indicates the maximum level of decomposition done on the image. Most of the energy of the image is concentrated in this band. Any modification done to this band is visually most perceptible. The HL and LH band of IWT contain horizontal and vertical components of the image and the HH band is called the diagonal band. These latter three bands are high frequency bands. These bands contain the detail information of an image like the edge information. The following figure depicts a two level decomposition of an image using integer wavelet transform.

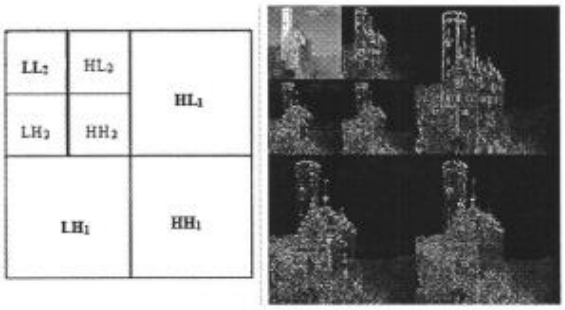


Fig. 1. Different bands in wavelet transform (photo courtesy: Wikipedia)

III. Proposed Method

This paper proposes a method to authenticate an image by means of digital watermarking. In addition to that the scheme proposed here is capable to restore the original image from a corrupted image. We will ensure that if any part of the image is modified or cropped then the scheme will be able to restore the image to its original form. It is known that quantization based watermarking is more suitable for authentication purpose [16]. If we apply quantization to all the pixels directly and change the grayscale values then the image will be significantly modified. So, we have decomposed the image by using integer wavelet transform. Hence, we get different subbands of the image. The next step is to select one or more suitable subbands to apply the quantization. In the proposed method, the values of the HL_2 and LH_2 bands were quantized to embed a digital watermark to the image. Any or both of the bands could be used for embedding the digital watermark.

However, both of the bands were used to reduce the false positive signal in the proposed method. LL band was not used for embedding the watermark to ensure high fidelity of the image. HH band is generally avoided as it contains important edge information of the image. The LL_1 component was also used in the proposed scheme as an approximation of the original image and it is encoded into the LSBs of watermarked image as a recovery mark. This recovery mark is extracted from the transmitted image. If any tampering is detected in the transmitted image, then this extracted recovery mark is used to restore the image to its original state. To obtain wavelet transform band we used Haar wavelet with lifting scheme. Furthermore, the operation is done in only integer domain to ensure lossless decomposition. It also ensured high computational speed of the proposed scheme.

In the proposed method, wavelet transform coefficients of HL_2 and LH_2 bands were quantized. The technique used for quantization of the wavelet transform coefficients is as follows:

Let **d** be the amount of modulation in IWT coefficients after quantization and **b** be the value of the watermark bit in the reference pattern that will be embedded. Also, let **p** be the IWT coefficient to be modulated and **m** be the modulated IWT coefficient. Now, **m** will be modulated by using following algorithm:

```
f = floor(p/(2*d))
c = ceil(p/(2*d))
if |p-f| <= |p-c|
        if b == 0
                m = f*2*d
        else
                m = f*2*d + d
        endif
else
        if b == 0
                m = (f+1)*2*d
        else
                m = (f+1)*2*d + d
        endif
endif
```

As we can see **p** is modified in such a way so that the amount of change is minimum. The value of **m** is nearer to **f** if |**p-f**| is less than |**p-c**|, otherwise the value of **m** is nearer to **c**. In this way we ensure that the quality of the image is not much degraded after quantization. Moreover, the modulated value **m** is a multiple of **2d** if a **0 (zero)** is embedded and **m** is a not a multiple of **2d** if a **1 (one)** is embedded.

A binary image was taken as the watermark. The resolution of this image should be one fourth of the cover image in each dimension. This watermark image is embedded into the cover image by using the following algorithm:

1. Divide the image into 8×8 subblocks
2. Compute 2-level IWT for each of the block
3. LL_1 band of a block X is embedded into the LSB of a different block Y as a recovery mark. The location of block Y is determined by using a secret watermark key which should be available to the watermark detector.
4. Modify the IWT coefficients of the HL_2 and LH_2 band according to the algorithm described above. Each bit of the watermark image is embedded in one coefficient of HL_2 band and in one coefficient of LH_2 band
5. Compute Inverse IWT for each block to get the watermarked image

The image is divided into blocks and watermark is embedded in each block separately. So, by checking the watermark of a particular block we can identify whether that block is modified or not. The recovery data for a particular block is preserved in another block. So, it is possible to restore the image to its original form by using that data.

Let **x** be a IWT coefficient of received image. Then, watermark bit **b** from this coefficient was extracted by using the following algorithm:

```
if |x mod 2*d| <= t then set b = 0
else set b = 1
```

Here, **t** is a predefined threshold value.

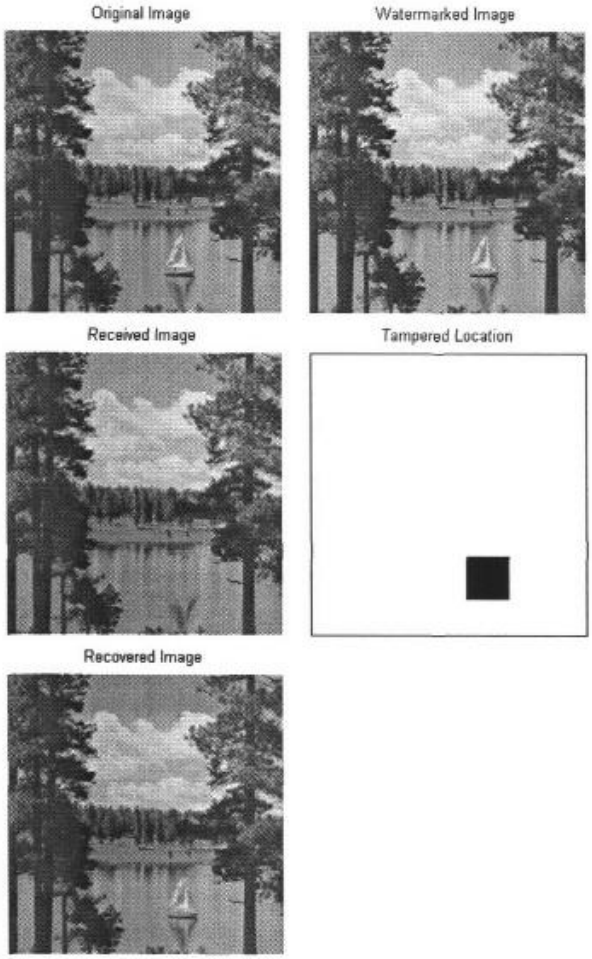
1. Divide the image into 8×8 blocks
2. Extract Recovery mark from each block of the image
3. Compute 2-level IWT for each of the block
4. Extract Watermark from HL_2 and LH_2 band of each of the block of the image
5. Compute correlation coefficient of extracted watermark and original watermark for each block
6. If the correlation between extracted watermark and original watermark is larger than the threshold then mark the block as authentic, otherwise mark the block as inauthentic or tampered.
7. Replace the tampered blocks using recovery mark

The watermark extraction and recovery process is as follows:

Ⅳ. Simulation and Experimental Result

Simulation was done using several standard gray scale images including peppers, lake, mandrill, pirate etc. The images were first watermarked using embedding scheme. A binary image was used as the watermark pattern which is embedded in the cover image. After watermarking is done, some portion of the image was cropped and replaced with a similar looking image. This tampered watermarked image is then passed to the detector. The detector extracts the two watermarks embedded in the HL_2 and LH_2 band. If any of the extracted mark is corrupted then the image is identified as inauthentic. The detector outputs two images. The first image shows the location of the tampered block by marking the region with black color. The unmodified locations are indicated with white color. The other image is the recovered image.

Fig. 2. Lake: a) Original Image, b) Watermarked image,



c) Received Image, d) Identification of tampered location, e) Recovered image

Figure 2 illustrates how any modification in the received image is detected and tampered location is identified. Recovered image is also shown.

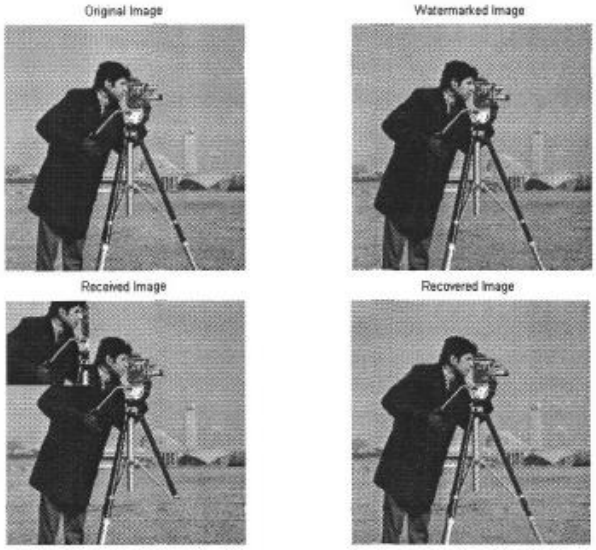


Fig 3. Cameraman: a) Original Image, b) Watermarked image, c) Received Image, d) Recovered image

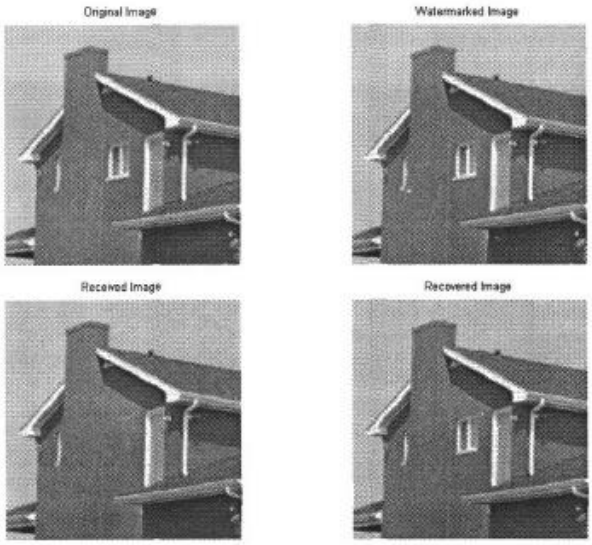


Fig..4. House: a) Original Image, b) Watermarked image, c) Received Image, d) Recovered image

Fig. 5. Binary watermark image

Figure 5 shows the binary watermark image which is

embedded into HL_2 and LH_2 subbands. If the cover image is unaltered then there will be no change in this watermark image. Otherwise, there will be some changes in the extracted watermark image.

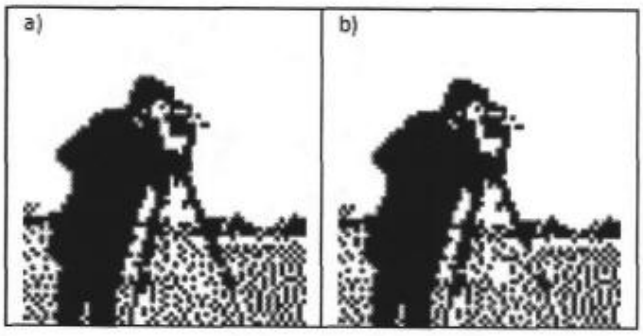


Fig. 6. a) Extracted watermark from an unmodified image, b) Extracted watermark from a modified image

Figure 6 shows how the binary watermark image is changed if the image modified.

Table 1. Correlation Coefficient between embedded and extracted watermark

Tampered %	Correlation Coefficient
6.25	0.9658
12.5	0.9175
25	0.7580
50	0.4337

Table 1 shows the correlation coefficient between embedded and extracted watermark when a percentage of the image is modified. Here, correlation coefficient over the whole image is measured. However, in the proposed method, the image is divided into 8×8 blocks. Watermark is extracted

$$CC = \frac{\sum (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum (x_i - \bar{x})^2 \sum (y_i - \bar{y})^2}} \quad (1)$$

from each block. Finally, the correlation coefficient for each block is measured separately to identify whether that block is modified or not. Correlation Coefficient of two vectors is calculated using equation 1.

Experimental results are evaluated in two ways: subjective evaluation and quantitative evaluation. Subjective evaluation was carried out and shown in the figures 2, 3 and 4. It is obvious from the figure that the images are successfully restored. For quantitative evaluation, the accuracy of the restored image was determined by evaluating Peak Signal to Noise Ratio (PSNR) value of the recovered image with the watermarked image. The efficiency of the algorithm from the viewpoint of imperceptibility is also evaluated in terms of PSNR. PSNR was calculated by using equation 2.

$$PSNR = 10 \log \frac{255^2}{\frac{1}{H \times W} \sum_{y=1}^{H} \sum_{x=1}^{W} (i(x,y) - w(x,y))^2} \quad (2)$$

Here, **H** and **W** denote image height and width respectively. **i(x,y)** and **w(x,y)** are the pixel values of **(x,y)** locations of the original and watermarked image respectively.

Table 2. Watermarked Image Fidelity

Image	PSNR (dB) Watermarked Image against Original Image	PSNR (dB) Recovered Image against Watermarked Image
Lake	40.15	32.85
Lena	40.30	36.33
Peppers	40.46	36.72
Walk bridge	40.41	32.34
House	40.62	38.26
Boat	40.54	36.34
Mandrill	40.51	32.65
Cameraman	40.37	32.49
Jet plane	40.05	33.65
Pirate	40.42	33.91

Table 2 summarizes the fidelity of watermarked image and the quality of recovered image by using PSNR value. Around 30% of the image was cropped while checking the quality of the recovery for different images. On an average the PSNR of the watermarked image was around 40 dB. Generally speaking, image with PSNR greater than 35 dB is acceptable as human visual system cannot distinguish the difference [1]. Therefore, the fidelity of the watermarked image is very much acceptable. Chang et al's scheme [14] achieves PSNR of 30-35 dB for different standard images with an average of 33 dB. It is observed that the proposed method shows better quality in terms of fidelity of the watermarked image.

To get a measure of the recovered image quality, PSNR of watermarked image and recovered image was used. Here, equation (1) is used again to measure the PSNR. However, in this case, **i(x,y)** denotes the pixel value of **(x,y)** location of the recovered image. Different percentage of the image was cropped and restored. The result is shown in Table 3. From the table, it is evident that even after cropping 25% of the image the recovered image has achieved a very good PSNR of 35 dB at the minimum. Furthermore, even after cropping 50% of the image, the PSNR of recovered image has not fallen much. The PSNR of restored image ranges from 32 to 40 dB with an average of 36 dB using Chang et al's scheme [14]. Quality of the restored image in the proposed method

found to be nearly similar to the method proposed in [14].

Table 3. Quality of Recovered Image

Tampered %	PSNR (dB) – Lena Recovered Image against Watermarked Image	PSNR (dB) – House Recovered Image against Watermarked Image
0.87	56.82	59.89
1.56	52.43	57.39
2.44	49.96	55.46
3.51	48.19	53.99
6.25	45.56	51.62
7.91	43.44	46.88
9.37	43.25	45.44
9.76	42.44	45.55
12.5	41.17	41.37
14.06	40.22	43.08
18.75	38.30	39.33
25.00	35.35	37.64
28.12	34.48	36.86
31.25	34.04	36.09
34.18	33.70	35.43
37.50	32.85	34.87
40.62	32.29	34.41
43.75	31.82	34.14
50.00	31.51	33.72

VI. Conclusions

The proposed method is computationally fast as it uses only integer based operation. Watermarked image in the proposed method showed good PSNR for the standard image which indicates a very acceptable fidelity. Tampered location of an inauthentic image was successfully identified by the proposed algorithm and the quality of the recovered image was also quite satisfactory. Proposed method ensured a better balance between the fidelity of watermarked image and the quality of the recovered image as compared to the method proposed in [14].

Reference

[1] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, T. Kalker, Digital Watermarking and Steganography, Second Edition, p. 375, 2008

[2] C.-Y. Lin and S.-F. Chang, "A robust image authentication method distinguishing JPEG compression from malicious manipulation," IEEE Trans. Circuits Syst. Video Technol., vol. 11, no. 2, pp. 153 - 168, Feb. 2001

[3] P. W. Wong, "A watermark for image integrity and ownership verification," in Proceedings of IS&T PIC Conference, (Portland, OR), May 1998

[4] P. W. Wong, "A public key watermark for image verification and authentication", in Proceedings of ICIP, (Chicago, IL), October 1998

[5] P. W. Wong and N. Memon, "Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership Verification", IEEE Transactions on Image Processing, vol. 10, no. 10, pp. 1593 - 601, 2001

[6] J. Fridrich and M. Goljan, "Protection of Digital images Using Self-Embedding", Symposium on Content Security and Data Hiding in Digital Media, New Jersey Institute of Technology, May 14, 1999

[7] J. Fridrich and M. Goljan. "Images with Self-correcting Capabilities," in Proceedings of the IEEE International Conference on Image Processing, volume 3, pp. 792 - 796, 1999

[8] K. Ke, T. Zhao & O. Li, "A Restorative Image Authentication Scheme with Discrimination of Tampers on Image or Watermark", 4th International Conference on Multimedia and Ubiquitous Engi-neering (MUE), pp. 1-5, 2010

[9] A. T. S. Ho, X. Zhu, J. Shen, and P. Marziliano, "Fragile Watermarking Based on Encoding of the Zeroes of the z-Transform", IEEE Transactions on Information Forensics and Secu-rity, Vol: 3, Issue:3, pp: 567-569, 2008

[10] C. H. Lin, C. Y. Yang, "Multipurpose Watermarking Based on Blind Vector Quantization (BVQ)", Journal of Information Hiding and Multimedia Signal Processing, Volume 2, Number 3, July 2011

[11] J. Xiao, Z. Ma, B. Lin, J. Su, Y. Wang, "A semi-fragile watermarking distinguishing JPEG compression and gray-scale-transformation from malicious manipulation", IEEE Youth Conference on Information Computing and Telecommunications, 2010

[12] D. Zou, Y.Q. Shi, Z. Ni, W. Su, "A Semi-Fragile Lossless Digital Watermarking Scheme Based on Integer Wavelet Transform", IEEE Transactions on Circuits and Systems for Video Technology, 2006

[13] F. B. Coelho, J. S. Barbar, G. S. B. do Carmo, "The Use of Watermark and Hash Function for the Authentication of Digital Images Mapped through the use of the Wavelet Transform", Second International Conference on Internet and Web Applications and Services, 2007

[14] C-C Chang, C-C Lin, Y-S Hu, "An SVD Oriented Watermark Embedding Scheme with High Qualities for the Restored Image", International Journal of Innovative Computing, Information and Control, Volume 3, Number 3, June 2007

[15] D. Kundur and D Hatzinakos, "Digital Watermarking for Telltale Tamper-Proofing and Authentication", Proceedings of the IEEE, Volume: 87, Issue:7, July 1999

[16] C. Fei, D. Kundur and R. Kwong, "A Hypothesis Testing Approach for Achieving Semi-fragility in Multimedia Authentication", IEEE Transactions on Information Forensics and Security, Volume 4, Issue 2, June 2009

Tanveer Ahsan

Sep. 2011~Present: Univ. of Ulsan, School of Electrical Eng., Graduate Student
May 2003: East West Univ., Dept. of Computer Science and Eng., B.Sc.
Aug. 2003~Aug. 2007: International Islamic Univ. Chittagong, Dept. of Computer Science and Eng., Asst. Professor.

Aug. 2007~Present: International Islamic Univ. Chittagong, Dept. of Computer Science and Eng., Asst. Professor.

Interests : Face and Facial Expression Analysis, Image Processing, Pattern Recognition and Digital Signal Processing.

Ui-Pil Chong

Member

Dec. 1996: New York Univ.(Polytechnic), Dept. of Electrical and Computer Eng., Ph.D.
Jun. 1985: Oregon State Univ., Dept. of Electrical and Computer Eng., MSEE.
Feb. 1980: Korea Univ., Dept. of Electrical Eng., M.E.

Feb. 1978: Univ. of Ulsan, Dept. of Electrical Eng., B.E.

Mar. 1997~Present: Univ. of Ulsan, School of Electrical Eng., Professor.

Interests: Digital Signal Processing, Multimedia, Fault Detection and Diagnosis.