Multimed Tools Appl (2017) 76:23805–23833
DOI 10.1007/s11042-016-4109-4

A watermarking technique to improve the security level in face recognition systems

Mohd Rizal Mohd Isa[1] · **Salem Aljareh**[1] · **Zaharin Yusoff**[2]

Received: 17 January 2016 / Revised: 26 October 2016 / Accepted: 31 October 2016 /
Published online: 23 November 2016

Abstract This paper presents a proposal for a suitable and viable combination of a face recognition system and a watermarking system, namely a PCA—DCT combination, as a new watermarked face recognition scheme that will ensure the authenticity of the data being transmitted in the face recognition system, which will then increase its level of security. The emphasis is on recognizing and rejecting stolen biometric data reintroduced into the system. The research begins with an analysis of biometric systems, with an emphasis on face recognition systems, and in particular with reference to the recorded threats on such systems, Biometric watermarking algorithms proposed by previous researchers within the face recognition environment are then studied, noting their proposed solutions to the said threats. This would then give a good idea towards a watermarked face recognition scheme to be proposed to enhance the security of face recognition systems, especially in terms of the authenticity of the data being transmitted. This watermarked face recognition scheme is the main objective, which will be then worked into the PCA—DCT combination, followed by a check on all the 8 possible locations where data may be intercepted and/or reintroduced. All the results produced are positive, apart from a few situations that will have to be left for future work. Non degradation of the individual PCA and DCT systems due to the combination is also checked and experimented on, again with positive results. Finally, the robustness of the watermarked face recognition scheme is experimented on to evaluate its resilience against attacks.

✉ Salem Aljareh
salem.aljareh@port.ac.uk

✉ Zaharin Yusoff
zarinby@gmail.com

Mohd Rizal Mohd Isa
up630277@myport.ac.uk

[1] School of Engineering, University of Portsmouth, Portsmouth, UK

[2] Computer Science Department, Faculty of Defence Science and Technology, National Defence University of Malaysia, Sungai Besi Camp, 57000 Kuala Lumpur, Malaysia

Keywords Biometric systems · Face recognition systems · Principal Component Analysis (PCA) · Discrete Cosine Transform (DCT)

1 Introduction

Biometrics is a relatively new domain in information security technology [18]. It determines the identity of a person based on his/her biophysical features (e.g. face, fingerprint, palm-print, and iris), or behavior features (e.g. signature, voice, and gaits). Various biometric systems have been developed during the past few decades, such as automated fingerprint recognition systems (AFRS), iris recognition systems, and face recognition systems, and they have been successfully deployed in a wide range of applications, including access control, attendance control, customs checking, etc. Compared with traditional token based security systems, biometric systems are much friendlier and more difficult to cheat because biometric traits are unique to every person and are permanent throughout his/her life.

Although biometric techniques offer reliable methods for personal identification, they do suffer from several security problems [1, 9, 10, 26]. A study reported in [28] analyzed threats in biometric systems and listed them out into eight classes. As an example, one kind of attack may take place when the scanner captures the biometric traits and sends them to the feature extraction module for further processing. At this location, the transmission channel is vulnerable to several threats, such as eavesdropping attack, replay attack, man in the middle attack, and brute force attack. For instance, during the raw data transmission between the said modules, the biometric traits can be intercepted and the attackers can 'replay' the biometric traits directly to the feature extractor and effectively bypass the scanner. Countermeasures to such attacks include transmitting data over encrypted channels, the use of symmetric or asymmetric keys, digital signatures, and Timestamp/Time to Live (TTL) tags.

Figure 1 depicts the components of a typical biometric system, where the biometrics data of the Subject captured by a Sensor is to be matched with one of the authorized Objects stored in a database. The core component is made up of a Feature extraction module and a Matcher that

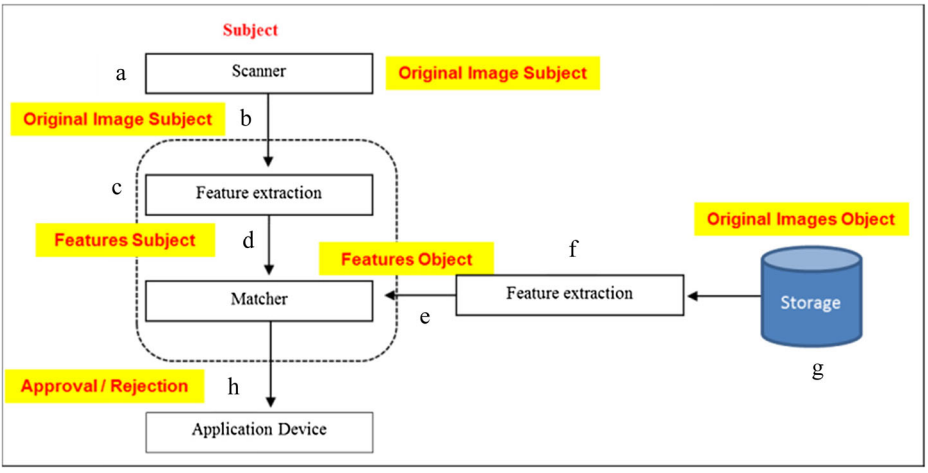


Fig. 1 Typical components of a biometric system and possible locations for interception and reintroduction of data

compares the features extracted from the Subject and those from an Object. A match will result in an Approval status sent to the Application device, else a Rejection.

Figure 1 can also be seen as the typical components of a face recognition system, where the Sensor device is a Scanner, and the Object database is a Facial database. As mentioned, there may be attacks on a biometric system, where data may be intercepted (stolen), manipulated, and then reinserted (replayed) into the system to achieve Approval. Here, Fig. 1 also shows the 8 points (a,b,c,d,e,f,g,h) where biometric data may be vulnerable to attacks. At each vulnerable point, the biometric data may be intercepted, and the intercepted (stolen) data may later be reinserted (replayed) at the same point or at the other 7 points. Hence, 8 vulnerable points (to intercept data from) * 8 vulnerable points (where the data may be reinserted) = 64 possible situations. The figure also shows the possible types of data that may be intercepted and/or reinserted. Measures to increase the level of security of biometric systems will have to secure these 8 points, both in terms of blocking entry, as well as to ensure the authenticity of the data being transmitted.

Indeed, in order to attain a more widespread utilization of biometric techniques, an increased level of security of biometric data is necessary [28], in particular against interception and replay attacks at the 8 vulnerable positions. Cryptography and watermarking are among the possible techniques to achieve this. However, while cryptography does make transmitted data quite unreadable against eavesdropping, it does not provide security once the data is decrypted. On the other hand, watermarking involves embedding information into the host data itself, so it can provide security even after decryption, as the watermark is attached to the host data.

Recently, researchers have proposed algorithms based on image watermarking techniques to protect biometric data [3, 8, 15, 17, 22, 27, 29, 32]. In biometric watermarking, a certain amount of information, referred to as a watermark, is embedded into the original cover image using a secret key, such that the contents of the cover image are not altered. Some of these methods perform watermarking in the spatial domain [8, 17, 22, 28], while other methods embed the biometric watermark in the frequency domain [15, 27, 29, 32].

It is in this area that this work focusses on, namely to find a suitable combination of a face recognition system and a watermarking system, ensuring that the combination will not degrade the performance of the individual systems, with the ultimate objective being to enhance the level of security of the face recognition system at the 8 possible locations where data may be intercepted and/or reintroduced, in particular in terms of the authenticity of the data being transmitted.

2 Work on watermarking within face recognition systems

Unlike for work on watermarking in general, it has been found that only a few watermarked biometrics schemes have been proposed specifically for protecting face images [4–6, 11, 13, 14, 20, 21, 24, 29, 31–33, 38, 39].

Tzouveli et al., [31] proposed a robust watermarking scheme with a face detection method on real life images. The scheme detects the face region using a two dimensional Gaussian model of skin color distribution, and then the QSWT (Qualified Significant Wavelet Trees) as well as the DWT watermarking technique to embed the watermark in the selected area. The experimental results showed that the efficiency of the proposed face detection algorithm and the robustness of the watermarking scheme against various signal distortions were good.

Unfortunately, the proposed scheme was not designed for biometric authentication systems, but rather for protecting the face area of real life images for copyright protection. The proposed scheme could possibly be enhanced so that it would be compatible with biometric authentication systems.

A robust biometric watermarking scheme was proposed in Vatsa et al., [32]. It was to improve recognition accuracy and for protecting face and fingerprint images from tampering. The Multi-resolution Discrete Wavelet Transform (DWT) watermarking technique for embedding a face image into a fingerprint image was used. The quality of the extracted face image is enhanced using a Support Vector Machine (SVM) algorithm by selecting the best quality pixels from two extracted face images. Experimental results showed that the fingerprint verification accuracy is maintained at a high level even under attacks. As for the extracted face images, the SVM improved by at least 10 % for verification accuracy.

Chen and Chang [6] proposed a watermarking system for personal image copyright protection by embedding the owner's eigenvalue information as a bar code image into different positions based on a SHA-1 sequence. Experiments showed that the imperceptibility value and the watermark detection rate are over the acceptable benchmark. Even though the proposed scheme indeed protects the cover image, again the scheme was not designed for nor experimented on biometric image authentication.

Another interesting approach is found in Salahi et al., [29] where a CT (Contourlet Transform) watermarking technique is used for securing face recognition systems. First, the face image is transformed in the CT domain at three levels, and then the smallest variance is selected for watermark embedding. A logo which is generated using a Walsh code is used as the hidden message. Experiments were conducted to calculate the performance of the face recognition system with and without watermarking under several attacks. The results show that the proposed scheme is robust against various attacks with the performance of the face recognition being hardly affected due to the watermark embedding. However, other face recognition algorithms were not tried with the CT domain watermarking technique to investigate their performance. This is a robust watermarking technique to cater for ownership authentication, but the embedding does not cover the entire face image, nor is there a check for the most appropriate places for embedding. Furthermore, it is also possible that the recognition rate is not affected because the watermark is embedded in a place from where the face features are not extracted for authentication. The image processing attacks used to investigate the robustness of the proposed scheme were also apparently not very strong, as the attacks did not deeply ruin the face image.

Most image watermarking is performed using DWT. However, one of the major drawbacks of DWT is that the transformation does not provide for shift invariance because of the down-sampling of its bands. To address the problems of DWT based watermarking, Yan and Liu [38] presented a 3-level RDWT (Redundant Discrete Wavelet Transform) biometric watermarking scheme. The proposed scheme first computes the embedding capacity of a face image by using an edge and corner phase congruency method. RDWT decomposes a face image into four sub-bands such that the size of each sub-band is equal to the original image. The redundant space in RDWT provides for additional locations for embedding, and the watermarking scheme can be designed as such that the exact location for watermark embedding can be determined. Since the size of each RDWT sub-band is equal to the size of the input image, the three levels of the RDWT decomposition provide adequate capacity to embed the watermark data without affecting the edge and corner locations. Only the second and third levels of the RDWT are used for embedding because these two levels provide more resilience to geometric and

frequency attacks. Extraction is simply the reverse of the embedding process. Experimental results show that the scheme is resilient to many different signal processing attacks.

A fragile watermarking scheme was proposed in Zhang [39] that focuses on the facial image database in a face recognition system. The main objective is to protect the face images against tampering attacks by detecting the locations of any modifications. Experiments were conducted on the impact on recognition accuracy, detection rate, as well as the speed of face recognition with and without the watermark. The results from the experiments indicated that the scheme has a high recognition rate, sustains a good imperceptibility level of face images, as well as a high sensitivity level against tempering the watermarked facial images.

Li et al., [20] proposed a novel salient region based authentication watermarking scheme to protect biometric templates by embedding the watermark in the region of background (ROB) and the region of salient (ROI) to investigate the face recognition rate. Experimental results showed that the proposed scheme is able to detect any interfered area, and recover the original biometric features while maintaining the recognition rate. They also proposed a semi fragile biometric watermarking to protect a face image from tampering. It was shown that the recognition rate is very minimally affected due to the watermark embedding.

Behera and Govindan [5] proposed a multimodal biometric watermarking techniques using DCT and Phase Congruency model for personal identification system such as e-passport and e-identification cards. The authors protect the face image by embedded the demographic data and fingerprint information of the same person as watermark. The authors claimed their proposed technique have achieved significance improvement on quality, complexity and accuracy of recognition rate. However, from analyzing the author's results, the recognition rate of the watermarked image is not investigated.

In 2012, Isa and Aljareh [13] proposed a watermarked face recognition scheme based on a DCT watermarking technique using the COX algorithm. According to Isa and Aljareh, the embedded watermark did not degrade the face recognition rate of the PCA algorithm. The proposed scheme is applied to face images where the password of a given person is hidden in the corresponding image to authenticate him. In their latest work, Isa et al., [14] proposed a blind robust watermarked face recognition scheme based on the combination of PCA as the face recognition algorithm, with the DCT watermarking technique to enhance the security of the face recognition system without degrading the recognition rate. The authors analyzed, in particular, the 8 vulnerable positions where data could be intercepted and/or resubmitted Ratha et al., [28], and the experiment set up is generally discussed in the paper.

Inamdar and Rege [12] proposed a dual watermarking scheme for biometric data as copyright protection, where multiple biometric watermarks (speech and face biometric traits) of the owner are embedded as well as an offline signature being delicately overlaid on the cover image. Before embedding, speech is compressed using Linear Predictive Coding (LPC) and a Gabor face is created from the face biometric traits. All three watermarks, Gabor face, LPC coefficients, and offline signature are the biometric characteristics of the owner and hence they are highly related to the copyright holder. The proposed scheme is robust because as the multiple watermarks are embedded in different areas of the image, at least one watermark will survive under watermarking attacks.

Amongst the latest research paper was from Kekre et al., [19]. They have proposed a biometric watermarking using partial DCT-walsh wavelet and SVD (Singular Value Decomposition). A face image is selected as a cover image while iris image as the embedded watermark. They claimed the proposed technique is highly robust against compression, selective and random cropping, noise addition and resizing attack. However, the proposed

technique does not perform well under selective cropping attack, but can be protected if the embedded watermark were to be on the middle frequency coefficients (instead of low frequency) of the cover image. If this is the case, the authors should also re-evaluate the other attacks if the watermark were to be embedded in the middle frequency.

From a rather thorough literature survey, it is found that previous research tends to protect the face image against certain threats on biometric authentication systems only in general, rather than trying to recognize and reject attempts to attack at specific points in the system. There is indeed a need for a watermarked face recognition scheme that would able to cover the eight positions described earlier against intentional attack, as given by Ratha et al., [28]. This is precisely the focus of this research. From a rather extensive literature survey related to the 8 vulnerable points given in Fig. 1, it is found that most researchers focus on the protecting biometric data at certain positions only, mainly at position a (scanner) and position g (storage). We also found that many proposed schemes focus on maintaining the quality of the face image, whereas in a face recognition system, the quality of the face image is not important as long as the feature extraction module is able to extract the features from the face image for authentication (this has an impact on the robustness of the watermark against tampering). In our research, we focus on efforts towards ensuring the full security at all 8 vulnerable points, although some may not be relevant and some may have to be left for future work.

3 Methodology

The research begins with an analysis of biometric systems, with an emphasis on face recognition systems, and in particular with reference to the eight threats that have been listed out by [28]. Next, biometric watermarking algorithms proposed by previous researchers within the face recognition environment are studied and classified according to their proposed solutions to the said threats.

The above would then give a very good idea towards proposing a watermarked face recognition scheme to enhance the security of face recognition systems, especially in terms of the authenticity of the data being transmitted. This watermarked face recognition scheme is the main objective.

For an implementation to validate the proposed watermarked face recognition scheme, the Principal Component Analysis (PCA) method, the most popular holistic approach for face recognition, is singled out with the reasons backing the choice. For the watermarking approach, the Least Significant Bits (LSB), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) techniques, being representative of their respective approaches, are looked at to complement the PCA to increase its level of security. An analysis shows that the DCT would probably perform the best, and a further analysis is carried out to ensure that the PCA—DCT combination will not degrade the performance of the individual systems.

The proposed watermarked face recognition scheme is then worked into the PCA—DCT combination, followed by a check on the 8 possible locations (of Fig. 1) where data may be intercepted and/or reintroduced to ensure the authenticity of the data being transmitted. Within the 64 (8×8) possible situations, some may not be relevant, many will be shown to be resolved (fully-protected), while the (few) remaining ones will have to be left for future work.

This methodology covers and achieved the main objectives of this research as mentioned in the Introduction, with the ultimate goal being to enhance the level of security of the face

recognition system at the 8 possible locations where data may be intercepted and/or reintroduced, in particular in terms of the authenticity of the data being transmitted:

- To find a suitable combination of a face recognition system and a watermarking system,
- To propose the appropriate watermarked face recognition scheme,
- Ensuring that the combination does not degrade the performance of the individual systems.

The rest of the paper will cover the findings in the following manner:

- Proposing the watermarked face recognition scheme to protect the face image from 8 vulnerable positions for system rejection of stolen data (in section 4)
- Using a PCA—DCT combination, ensuring that the combination will not degrade the performance of the individual systems (in section 5)
- Experimentation for (in section 6):

– Validation of system rejection of stolen data
– Validation of non-degradation of PCA and DCT due to the combination
– Determining the frequency band for watermarking (a necessity)
– Robustness of the watermark scheme (a necessity)
– Validation for the choice of PCA—DCT combination: comparative study of watermarking techniques

The underlying idea here is to show that the PCA-DCT combination does not degrade the performance of the individual systems, and that the proposed watermarked face recognition scheme will ensure the authenticity of the data being transmitted in the face recognition system at the 8 vulnerable positions where data may be intercepted and/or reinserted. The watermarking scheme also needs to be shown to be robust against signal processing attacks, and in particular the watermark cannot be easily removed by an attacker.

4 The proposed watermarked face recognition scheme

In a generic face recognition system, there are three main processes – face detection, face extraction and face recognition (respectively points a, c and e in Fig. 1). The input of a face recognition is always an image and the output is an identification or verification of the person appearing in the image. A face is detected and extracted from the scene, then followed by the feature extraction step by obtaining the relevant facial features from the data. A similar feature extraction approach (point f) works on the targeted object (from point g) - the target object is determined by some means, perhaps by tagging a smart card carrying the identity of the subject. Finally, the system recognizes (at point e) the face using template matching strategies whereby the algorithms compare input images with stored patterns of faces or features, resulting with an approval if there is a match, and a rejection otherwise. The pattern database is learnt from a set of training images.

Watermarking techniques are usually proposed to add ownership information and/or camouflage copyright marks of multimedia objects and information in digital images, audio and video. When face recognition is combined with watermarking techniques, watermarks are usually inserted and embedded into the image of the subject as soon as it is captured (at point

a), and additional watermarks may be embedded in the object image once retrieved from the database (at point g) to make it the same as for the subject. This is then followed by the feature extraction process on both sides (at points c and f), resulting in their respective feature files, on which the matching algorithm will work. In essence, this matching is exactly like the matching on the features of the original images, except that these features have been (in a sense) transformed to include the watermarks (albeit not done directly).

The main thing to note here is that the matching should give exactly the same results (approval or rejection) as with the original face recognition process, because:

- Exactly the same watermarks are inserted into both the subject and object images
- Exactly the same face recognition algorithm is used

– The same original face recognition feature extraction algorithm is used on both ends
– The same original face recognition feature matching algorithm is used.

Now, it remains to see how the proposed watermarked face recognition scheme will enhance security. The proposed watermarked face recognition scheme makes use of 2 different watermarks:

- Logo
- Timestamp

The logo serves as in any other watermarking technique that inserts particular images within object images. The main purpose is usually to identify genuine images within the database of objects. However, in this proposed work, it will be seen further on that it is also used to identify stolen images.

The timestamp is the main security enhancer, as it will be used as a form of session ID. Any image stolen from within the process and reinserted later will be immediately recognized as coming from a different session and will be rejected. In addition, like the logo, it can also be used to identify stolen images by its mere existence within the image.

In order to check on the coverage of proposed watermarked face recognition scheme, Fig. 2 depicts the proposed scheme indicating the places where the watermarks are present within the system, and most importantly the positions where attackers can steal biometric data from within the system and then reinsert it at the same or at other positions.

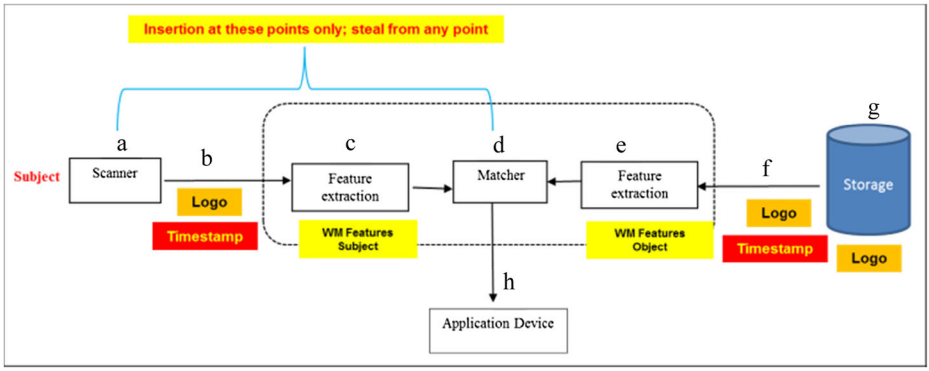


Fig. 2 The proposed watermarked face recognition scheme

The diagram indicates that data may be stolen from any of the 8 points a, b, c. d, e, f, g, h, and then reinserted at the same place or at any other point, which gives rise to $8 \times 8 = 64$ situations. We will look at all these further below. First, two key points about this watermarked face recognition scheme proposed work are to be noted:

- It covers only situations where data is stolen from the system, and NOT when fresh data is introduced.
- It also covers only situations where the watermark has been introduced (hence not at point a).

The above means that the following two situations are excluded, and may be left for future work – presenting a printed image to the scanner (at point a), and when the approval code is stolen at point h and reused by reinsertion later on at the same point.

It is also to be noted that in as much as data may be stolen from any of the 7 remaining points (other than a), there is nothing to gain by reinserting the stolen data at points e, f and g, as these points transmit or store authenticating data and not the one to be authenticated. This then reduces the total number of situations to be checked from $8 \times 8 = 64$ down to $7 \times 4 = 28$. Within these 28 situations, observe that data stolen from the following points will have the given contents (recall that points a and h are outside the scope) as shown in Tables 1 and 2:

This above means that only the following combinations of stolen→reinsertions are possible:

Thus two fundamental points underlie this technique:

- Any image stolen from anywhere other than from point a will already have a watermark inserted (at least a logo), and its presence can be readily detected. The image can then be immediately rejected if it is reinserted at point a.
- Data stolen from one point may have to be processed externally before reinserting at another point. For example, for an image stolen from point a, to be reinserted at points c or d will have to have its features extracted before being reinserted. However, apart from points a and g, all data would have the timestamp watermark, and so a later reinsertion (as a subject) will not tally with the timestamp of the object watermark.

From the above, one should then be able to deduce that the system should be able to reject data stolen from and reinserted at according the following Table 3:

5 PCA—DCT combination system

In this study, only one face recognition algorithm is selected to combine with one of three watermarking techniques. Although this may seem quite limited, the algorithm and techniques

Table 1 The contents of stolen data from point b to point g

b	c	d	e	f	g
Subject	Subject	Subject & Object	Object	Object	Object
Image	Features	Features	Features	Image	Image
Logo	Logo	Logo	Logo	Logo	Logo
Timestamp	Timestamp	Timestamp	Timestamp	Timestamp	Not Applicable

Table 2 The positions from which data may be stolen from and the possible reinsertion positions with the required contents

Stolen at	Reinsertion at	Contents
b, f, g	a	*Requires image*
b, f, g	b	*Requires image*
c, d, e	c	*Requires features*
c, d, e	d	*Requires features*

chosen are considered representative of their respective approaches (being the most cited and considered the best), and it would at least set a new benchmark and reference for other implementations to follow.

PCA is one of the most used algorithms and has proven to be very effective for information compression in face recognition systems. Furthermore, researchers have shown that PCA performs well in recognition when the training data set is small (which is the case in this research), and is very stable with different training sets [16]. Furthermore, according to [25], the DCT approach is very robust to JPEG compression since JPEG itself makes use of DCT.

Having assured that data stolen from and reinserted at the relevant points would be rejected ($7 \times 4 = 28$ situations), next is to check that the PCA and DCT will not disturb each other's performance, especially in terms of accuracy. The choice of PCA—DCT combination is validated via experimentation reported in 6.6.

On this point, analytical results validated by experiments as presented by [36] have shown that when DCT is first applied on a pixel file to obtain a frequency domain file (with changes in coefficients), and then followed by the application of PCA for compression as well as reconverting to an image (compressed file), the result is the same as that of a direct application of PCA on the original pixel file. This is as illustrated in Fig. 3 – path 1.

This result would mean that it is safe to say that DCT does not degrade the accuracy performance of PCA algorithm, at least in terms of the accuracy of face recognition, should there be a need to introduce watermarking at certain points of the face recognition system. Ideally, we would want to have the same analytical results both ways, namely also for the application of DCT following an application of PCA – path 2 in Fig. 3 – which would then show that PCA also does not degrade the accuracy of DCT. Proving this result is beyond the scope of this work, and so experiments are conducted to show some form of validation of this result, which is reported in 6.3.

6 Experimentation

There are two important factors in building the watermarked face image. Firstly and most importantly, the face recognition rate is maintained with the embedded watermark as a security

Table 3 System rejection of stolen data

Rejection by	Stolen at	Reinsertion at	Rejection at
Illegitimate presence of logo	b, f, g	a	a
Timestamp does not tally	b, f, g	b	b
Value of features do not match (by the face recognition system)	c, d, e	c, d	d

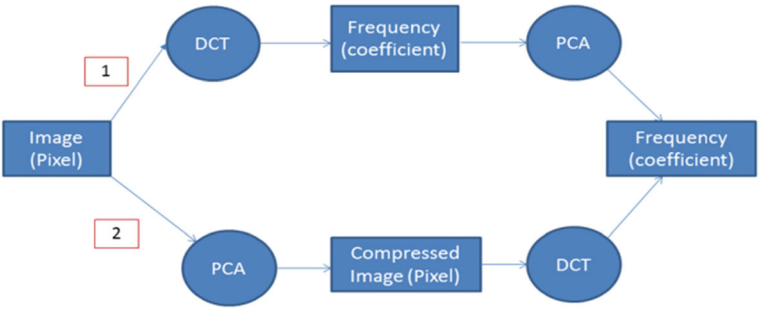


Fig. 3 DCT and PCA do not degrade each other accuracy

mechanism. Secondly, the watermark detection rate should be high without affecting the recognition rate. Both these factors go hand in hand. Previous researchers tend to put an emphasis on the perceptibility of the face image, whereas in reality, biometric authentication systems do not really need a clear face image as long as face features can be extracted successfully for authentication. The printed image is never shown to anyone.

Five experiments are conducted to validate the claims made in this paper, which all proved successful:

1) Security – system rejection of stolen data

   – Illegitimate presence of watermarks (logo)
   – Timestamp does not tally
   – Value of features do not match (based on the face recognition system)

2) Non degradation accuracy performance of PCA and DCT due to the combination
3) Determining the frequency band for watermarking
4) Robustness of the proposed watermarked face recognition scheme.
5) Comparative study of watermarking techniques

All the experiments are conducted using the Our Database of Faces [23] at AT&T Laboratories, Cambridge University. The database contains a set of face images of 40 persons with ten different images for each person. The images were taken at different times, with various lighting conditions, different facial expressions (open /closed eyes, open/closed mouth, smiling/unsmiling etc.) and dissimilar facial details (glasses/ no glasses). All the images were taken against a dark homogeneous background with the subjects in an upright and frontal position. The size of each image is 92×112 pixels with 256 grey levels per pixel in PGM format.

Recall that one of the main purposes of our proposed scheme is for countering replay attacks with a robust blind watermarked face recognition scheme to protect the biometric traits from being re-used (replayed) by attackers. The face image can be protected against such an attack by placing the watermark in the area where the face feature extraction happens. As such, the proposed scheme should meet the following goals:

- Reject face images that have been stolen and re-inserted later at any point within the face recognition system.

- Retain the recognition rate for watermarked face images to maintain the effectiveness of the face recognition system.

In the proposed watermarked face recognition scheme, the Viola & Jones algorithm [34] is adopted for the face detection algorithm, and the PCA for the feature extraction technique. The Viola & Jones algorithm is very effective for the localization of the spatial extent of the face and to determine its boundaries. The algorithm was observed to perform reasonably well on the face images used in this work. PCA has been chosen as the feature extraction algorithm because PCA has proven to be very effective for information compression, and several researchers have also shown that PCA performs better in face recognition when the training data set is small, which is our case.

6.1 General modules

The five experiments will be presented in turn further below, but first we present the two most critical modules utilized in the system – the watermark embedding module and the watermark extraction module.

6.1.1 Watermark embedding module

The overall watermark embedding process is illustrated in Fig. 4, and the details of the steps are as follows.

Step 1. Read the face image and the watermark image.
Step 2. Transform the watermark image into binary and convert the binary watermark sequence into an Arnold Transform (AT). The AT [37] is used in order to protect the watermark against intentional reconstruction by intruders.
Step 3. Detect the face area using the Viola Jones technique.

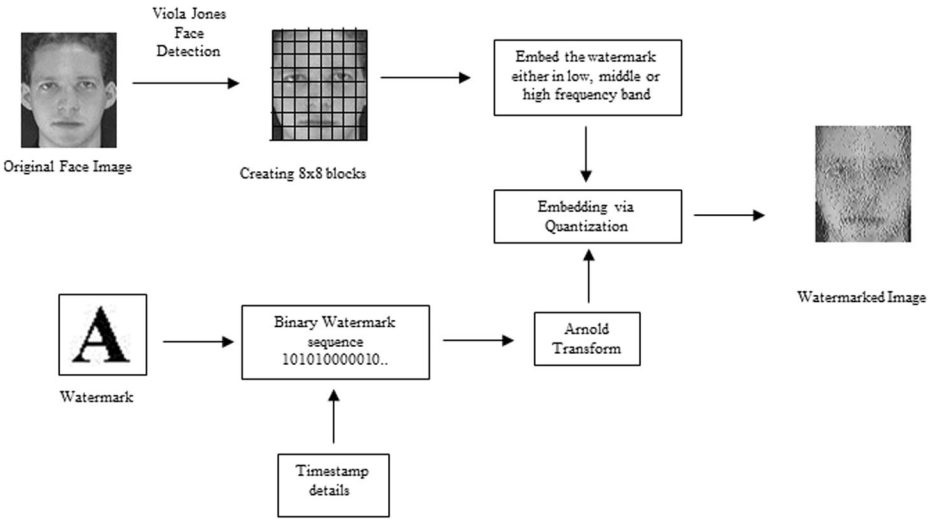


Fig. 4 Watermark embedding process

Step 4. Divide the face area image into 8×8 blocks, and convert each block into a DCT transform.

Step 5. Protect against compression. In order to protect the watermark against JPEG compression, each DCT coefficient from every block is quantized using the quantization table of the JPEG compression standards. (Refer to Fig. 5 below).

Step 6. Choose the frequency band for watermark embedding to be done in Step 7. [This frequency band is decided based on Experiment 3 – see below].

Step 7. Choose the robustness level for watermark embedding [This watermark strength value is decided based on Experiment 4.] Then execute watermark embedding. For this, let C(k,l) be the DCT coefficients in the chosen frequency range, R the modulus, P the mathematical remainder of |C(k,l)| with $P \in \{0, 1, 2, \ldots., R-1\}$, and the other variables be declared via the formulae as given below. The value of R is a predefined constant and is used as a reference threshold. The higher the value of R, the higher the level of robustness of the method, but the quality of the watermarked image decreases. The value of R is chosen in such a way so as to obtain a balance between robustness and the face recognition rate, which apparently also depends on image quality.

$$
\begin{array}{ll}
P = |C(k,l)| \ mod \ R\ ; & \\
\text{if watermark bit} = 0: & \text{if watermark bit} = 1: \\
if \ \ P \geq 3 \times \frac{R}{4} & if \ll P \ \frac{R}{4} \\
C(k,l)^{*} = C(k,l) - P + 5*\frac{R}{4} & C(k,l)^{*} = C(k,l) - P - \frac{R}{4} \\
else\, if \ P < 3*\frac{R}{4} \&\& \ P \geq 2*\frac{P}{4} & else \ if \ P > \frac{R}{4} \&\& \ P \ll 2*\frac{R}{4} \\
C(k,l)^{*} = C(k,l) - P + \frac{R}{4} & C(k,l)^{*} = C(k,l) - P + 3*\frac{R}{4} \\
else & else \\
C(k,l)^{*} = C(k,l) & C(k,l)^{*} = C(k,l)
\end{array}
\tag{1}
$$

Step 8. Repeat steps 6 and 7 until the entire watermark is successfully embedded into the remaining blocks. Apply inverse DCT to each block to construct the watermarked face image.

6.1.2 Watermark extraction module

The overall watermark extraction process is illustrated in Fig. 6, and the details of the steps are given after that.

Fig. 5 Quantization table recommended in the JPEG specification

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

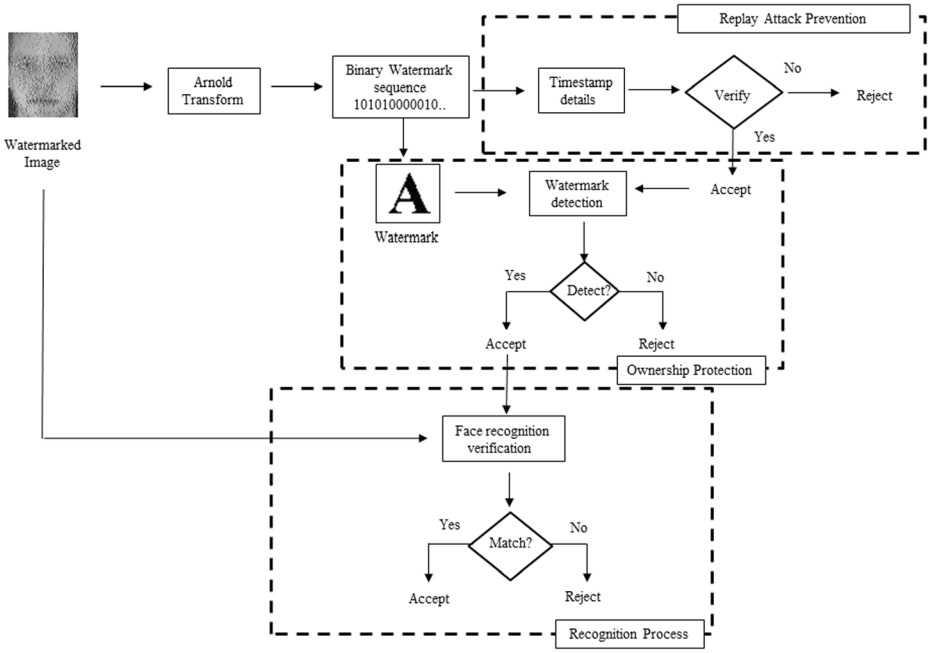


Fig. 6 Watermark extraction process

The watermark extraction steps are very closely related to the watermark embedding steps. In essence, the watermark can be extracted by reversing the embedding steps provided the location of the embedded watermark is known. As the scheme is based on blind watermarking concepts, the original image is not needed as a reference. There are two variables needed for extraction: the locations of the watermark bits and the value of the modulus R. The extracted bits are assembled to obtain the watermark pattern and then the inverse Arnold transformation is applied.

Step 1. Detect the face area of the watermarked face image.

Step 2. Divide the watermarked image into 8×8 blocks and convert each block into the DCT frequency domain.

Step 3. Extract the watermark bits using the equation below and the embedded watermark location. Let C(k,l)* be the DCT chosen frequency coefficients of the embedded watermark, eb the extracted watermark bit, and R the modulus.

$$eb = \begin{cases} 0, \ if \ (C(k,l) \ mod \ R) < \dfrac{R}{2} \\ 1, \ if \ (C(k,l) \ mod \ R) \geq \dfrac{R}{2} \end{cases} \tag{2}$$

Step 4. Repeat steps 2 and 3 on each block until all watermark bits have been extracted and concatenated into a watermark pattern.

Step 5. Inverse the watermark pattern with the Arnold transformation.

Step 6. Reconstruct the watermark pattern to obtain the extracted watermark.

The watermark embedding and extraction processes are used at runtime as well as in all the five experiments, which we are now in a position to present.

6.2 Experiment 1 - system rejection

The experiment was to test for rejection in the following situations, using the images of 10 individuals:

a) Rejection 1 - Illegitimate presence of logo (at point a)
   Rejection at point a is based on the presence of a logo within the submitted image.
b) Rejection 2 - Timestamp does not tally (at point b)
   Rejection at point b is based on the value of the timestamp not within the acceptable range of the current time.
c) Rejection 3 - Feature values do not match (at point d)
   Rejection at point d is done by the face recognition Matcher, also based on the features converted from the timestamp in the submitted image which do not match with the features converted from the timestamp converted from the image coming from the object database. All were successfully rejected by the system (30 situations).
d) Additional - Logo does not exist (at points a, g)
   Although mentioned in section 4 as not being within the scope of this research ($7 \times 4 = 28$ situations), experiments were also conducted for a particular situation at point a and one for point g. Rejection at point a is based on the existence of a logo, while rejection at point g is when the logo does not exist.

In the above, all were successfully rejected by the system – 30 situations each for (a), (b), (c), and 20 for (d). These results thus fully validate the claims.

6.3 Experiment 2 - non-degradation

This experiment is to validate the claim that the use of DCT will not degrade PCA-based face recognition, and vice versa.

Figure 7 below illustrates the analytical result validated by experiments as presented by Weilong Chen, Meng Joo Er, and Shiqian Wu [36] is shown as path 1. That experiment is repeated here. The other part of the experiment is the application of DCT following an application of PCA, i.e. path 2, in an effort to show that PCA also does not degrade the accuracy of DCT.

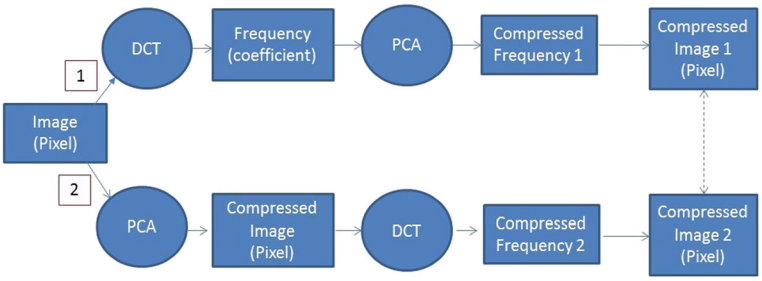


Fig. 7 Experiment 2 – DCT and PCA do not degrade accuracy of each other

The experiment is carried out for both paths with the same input images, with a hope to show that the results are identical with the input images. Should this be the case, given that PCA has been shown not to degrade DCT (Path 1), identical results from Path 2 would indicate that DCT also does not degrade PCA.

Recall that both paths result in essentially compressed coefficient files. For path 1, the DCT produces frequencies, which are then compressed by the DCT (Compressed Frequency 1). For path 2, the PCA compresses the image file, and the DCT produces the frequencies of the compressed file (Compressed Frequency 2). These two files at face value are quite different, but equality may be shown by reconverting the files resulting from both paths into pixel files and then both are compared to the respective original input images. For the comparison, the structural similarity (SSIM) index is used, and recall that the closer the value is to 1, the closer are the compared images.

The SSIM index is based on the concept of full reference image quality assessment in Wang et al., [35]. The SSIM index is calculated for various types of images, such as to check on the preservation of the quality of digital television and cinematic pictures, as well as for digital images and videos in general. The SSIM index is calculated on the various windows of an image. The measure is between two windows of common size $N \times N$ from two given images x and y where the SSIM index compares local patterns of pixel intensities that have been normalized for luminance, contrast and structure, and it is defined as follows:

$$\mathrm{SSIM}(\mathrm{x}, y) = \frac{\left(2\mu_x\mu_y + C_1\right)\left(2\sigma_{xy} + C_2\right)}{\left(\mu_x^2 + \mu_y^2 + C_1\right)\left(\sigma_x^2 + \sigma_y^2 + C_2\right)} \tag{3}$$

where μ_x and μ_y are respectively the means of the signals for x and y, σ_x and σ_y are the standard deviations of the signals for x and y, while C_1 and C_2 are constants with values much smaller than 1. σ_{xy} is the estimated correlation coefficient of the signals for x and y. A SSIM(x, y) value of 1 would mean the images x and y are completely identical, but for this experiment, a threshold value of 0.85 would already suffice.

The experiment is conducted with a set of face images of 40 different persons. The experiment first validates path 1, by showing that the output pixel files are identical to the input images, i.e. with an SSIM index of 1. This is then followed by comparing the results of path 2 with the input images, with the hope of similar results.

For PCA in the experiment, 20 principal components are used. In path 1, the face image is first converted into the frequency domain using DCT, after which the DCT coefficients are compressed using PCA. The compressed DCT coefficients are then reconstructed back into a pixel file using the Inverse DCT (IDCT) technique [7]. As for path 2, the face image is first compressed using PCA, after which the compressed face image is then converted into the DCT frequency domain and then reconstructed back into a pixel file using IDCT.

The SSIM index measurements for the similarity values between the original face images and the output pixel files for path 1 and path 2 are as given in the Table 4 below.

The results above show that for path 1 the compressed face images are exactly similar (identical) to the respective original face images, as stipulated by Weilong Chen, Meng Joo Er, Shiqian Wu [36]. As for path 2, the compressed face images have different SSIM values, but are all very close to 1. This shows that there is some disturbance in the quality compared with the original face images. The SSIM threshold value of 0.85 is considered acceptable, which is the case here. *[Note: Admittedly, this threshold value of 0.85 is essentially a conjecture.*

Table 4 The SSIM index measurements for Path 1 and Path 2

	SSIM	
Face images	Path 1	Path 2
Person 1	1	0.9216
Person 2	1	0.8692
Person 3	1	0.9543
Person 4	1	0.8950
Person 5	1	0.9387
Person 6	1	0.8938
Person 7	1	0.8936
Person 8	1	0.9518
Person 9	1	0.9290
Person 10	1	0.9216
Person 11	1	0.8798
Person 12	1	0.9402
Person 13	1	0.9089
Person 14	1	0.8717
Person 15	1	0.8670
Person 16	1	0.8730
Person 17	1	0.9053
Person 18	1	0.9111
Person 19	1	0.9320
Person 20	1	0.9006
Person 21	1	0.9287
Person 22	1	0.8929
Person 23	1	0.9383
Person 24	1	0.9016
Person 25	1	0.9295
Person 26	1	0.9311
Person 27	1	0.8818
Person 28	1	0.9044
Person 29	1	0.9307
Person 30	1	0.9221
Person 31	1	0.9113
Person 32	1	0.8732
Person 33	1	0.9223
Person 34	1	0.8687
Person 35	1	0.9397
Person 36	1	0.8658
Person 37	1	0.8655
Person 38	1	0.9131
Person 39	1	0.9420
Person 40	1	0.9107

Further experiments will have to be conducted to ascertain the correct threshold value (comparable to the universally accepted watermark detection rate of 0.75 – see Experiment 3 below). This will be left for future work.]

6.4 Experiment 3 - determining the frequency band for watermarking

This experiment is to determine the best frequency band to place the watermarks in an image, with the highest level of accuracy for face recognition, as well as the highest level of accuracy for watermark detection and recognition.

The experiment is conducted with a set of face images of 40 persons, with ten different facial expressions for each person. As such, 400 face images are used in this experiment for each frequency band. The detailed steps are as follows:

i. Every face image is embedded with the watermark in the low frequency band area.
ii. The watermarked face images are tested in the system to measure the face recognition accuracy rate as well as the watermark detection rate.
iii. The strength value of the watermark is increased slowly to find out at which level the accuracy and detection rate begins to deteriorate.
iv. Repeat step i with the middle and high frequency band areas.

6.4.1 Accuracy - maintaining the accuracy of face recognition with high watermark strengths

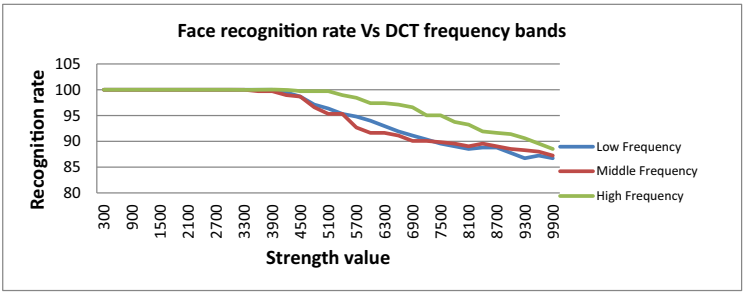
It is essential to investigate which frequency band has the least effect on the face recognition rate due to the embedded watermark. The results show that, as the strength value of the watermark increases, the face recognition rate for the middle frequency bands starts to decrease first, followed by the low bands and finally the high bands.

Figure 8 below shows the performance for the face recognition rate for each DCT frequency band. The underlying idea is to select the maximum strength value for the watermark where the face recognition still has 100 % accuracy for feature extraction. Referring to Fig. 8, the recognition rate begins to decrease around the strength value of 4200. Therefore, it can be summarized that the high frequency band is the best location to maximise the watermark strength while maintaining the face recognition rate.

Figure 9 shows the quality of the face image after embedding the watermark with different watermark strengths. It can be seen that at a very high watermark strength of 4200, where the recognition rate is still maintained at 100 %, perceptibility is still quite high even with the naked eye.

6.4.2 Detection - existence of watermark for acceptance or rejection

At the same time, it is also crucial to look at the watermark detection rate on each frequency band to balance with the face recognition rate. The proposed scheme not only needs to have a high face recognition rate but also a high watermark detection rate, with or without intruder attacks. The detection rate is measured using the Normalized Correlation (NC) score.



Strength Value (Modulus)	300	900	1500	2100	2700	3000	3300	3600	3900	4200	4500
Low Frequency	100	100	100	100	100	100	100	100	100	***99.48***	*98.70*
Middle Frequency	100	100	100	100	100	100	100	***99.74***	*99.74*	*98.96*	*98.70*
High Frequency	100	100	100	100	100	100	100	100	100	100	***99.74***

Fig. 8 Face recognition accuracy rate comparison with each DCT frequency band under different strength value

The previous experiment (a) showed that a 100 % face recognition rate can still be maintained up to a certain watermark strength value for each frequency band. This experiment looks at the watermark detection rates up to those specific values. From the results (see Table 5), it can be concluded that the watermark detection rate can be maintained at a high level on the low frequency band as the watermark strength value increases. In general, it is universally recognized that a watermark detection rate of over the threshold value of 0.75 is considered acceptable, as at such rates the watermark can still be fully recovered [2].

From the first experiment (a), it is found that the face recognition rate performs better in the high frequency band, whereas the second experiment shows that the low frequency band outperform the higher band on the watermark detection rate. The comparisons for face recognition and watermark detection rates for each frequency band are then compiled in Figs. 10, 11, and 12 in order to help determine which frequency band should be finally selected for watermark embedding.

From the figures above, it can be seen that all watermark detection rates are above the threshold value of 0.75 in all frequency bands. However, both face recognition and watermark detection rates are mostly maintained at high levels in the low frequency bands. This then leads to the conclusion that the low frequency bands are the most suitable for watermark embedding.

The watermark strength value for the last point of the highest recognition rate (100 %) in the low frequency bands is then selected for the evaluation of the robustness value of the proposed scheme – which turns out to be 3900.

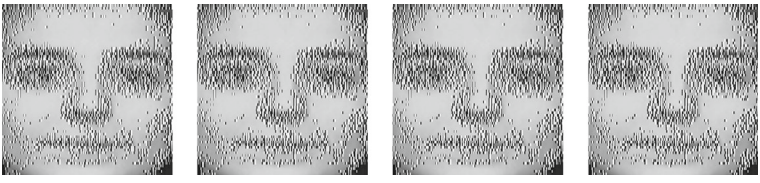


Fig. 9 The quality of the face image for different watermark strength values

Table 5 Detection rate for different frequency band

	Detection rate (NC)		
Watermark strength (R)	Low Freq.	Middle Freq.	High Freq.
300	1	1	1
600	1	1	1
900	1	1	1
1200	1	1	0.99
1500	1	0.99	0.98
1800	0.99	0.98	0.97
2100	0.99	0.97	0.96
2400	0.98	0.96	0.95
2700	0.97	0.94	0.94
3000	0.97	0.93	0.94
3300	0.97	0.92	0.94
3600	0.97	0.91	0.94
3900	0.97	0.91	0.94

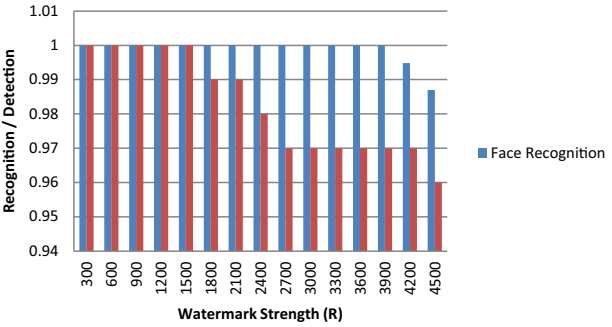


Fig. 10 Comparison of face recognition and watermark detection rates for watermarks embedded in the low frequency bands

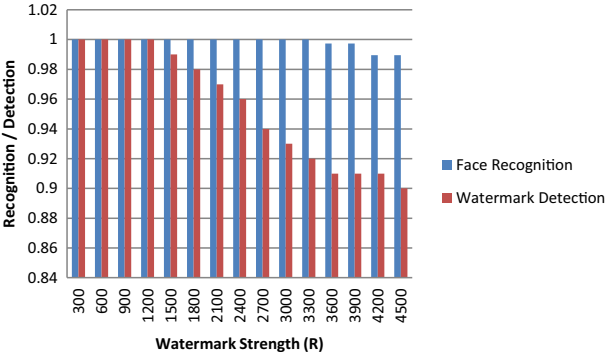


Fig. 11 Comparison of face recognition and watermark detection rates for watermarks embedded in the middle frequency bands

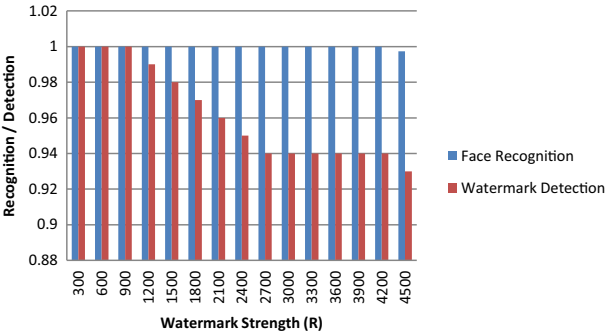


Fig. 12 Comparison of face recognition and watermark detection rates for watermarks embedded in the high frequency bands

6.5 Experiment 4 - robustness

This experiment is to determine the level of robustness of the watermark scheme. The robustness of the watermark scheme needs to be investigated to ensure that the watermark cannot be easily removed by an attacker.

From the results of Experiment 3, the lower frequency bands are chosen for watermark embedding, and the selected strength value for the watermark is 3900. For these chosen frequency bands and the watermark strength, this experiment is conducted with the same 400

Table 6 Detection rate after attacks

Attack type	Detection rate (NC)
Median Filter (3 × 3)	0.935682
Median Filter (5 × 5)	0.927467
Median Filter (7 × 7)	0.857539
Median Filter (9 × 9)	0.694807
Median Filter (15 × 15)	0.629405
Gaussian Noise (0,0.01)	0.907509
Gaussian Noise (0,0.05)	0.891861
Gaussian Noise (0,0.1)	0.886505
Gaussian Noise (0.01,0)	0.967328
Gaussian Noise (0.02,0)	0.968085
Gaussian Noise (0.1,0)	0.973004
Gaussian Noise (0.05,0)	0.970751
Salt&Pepper (0.001)	0.963221
Salt&Pepper (0.002)	0.960227
Salt&Pepper (0.01)	0.940843
Salt&Pepper (0.05)	0.904951
Salt&Pepper (0.1)	0.893861
JPEG compression (10 %)	0.807241
JPEG compression (30 %)	0.883940
JPEG compression (50 %)	0.914256
JPEG compression (70 %)	0.938168
JPEG compression (90 %)	0.959181

watermarked face images used for Experiment 3. Each watermarked face image is disturbed with various signal processing attacks (median filter, Gaussian noise, salt & pepper, JPEG compression), after which the watermark is extracted to evaluate the quality preservation performance. The extracted watermark is compared with the original watermark, also using the Normalized Correlation (NC) score.

Table 6 gives the experiment results for robustness. It can be seen that the proposed scheme is resilient especially against JPEG compression, Gaussian noise, as well as salt and pepper attacks, where the embedded watermark is hardly disturbed from such attacks. As for the median filter attack, the proposed scheme is able to survive up to 7×7 filters, which indicates that it is fairly robust.

As illustrated in Fig. 13 below, it can also be seen by the naked eye that the embedded watermark can still be clearly seen after a large number image processing attacks.

6.6 Experiment 5 - comparative study of watermarking techniques

This experiment is to validate the choice of DCT as the watermarking technique to be coupled with DCT, by comparing it with two other most used watermarking techniques – namely LSB (spatial) and DWT (transform/frequency).

As with most of the earlier experiments, this experiment is also conducted with face images of 40 persons, each with ten different facial expressions, giving a total of 400 different images. The images are embedded using the three said watermark techniques. The same earlier

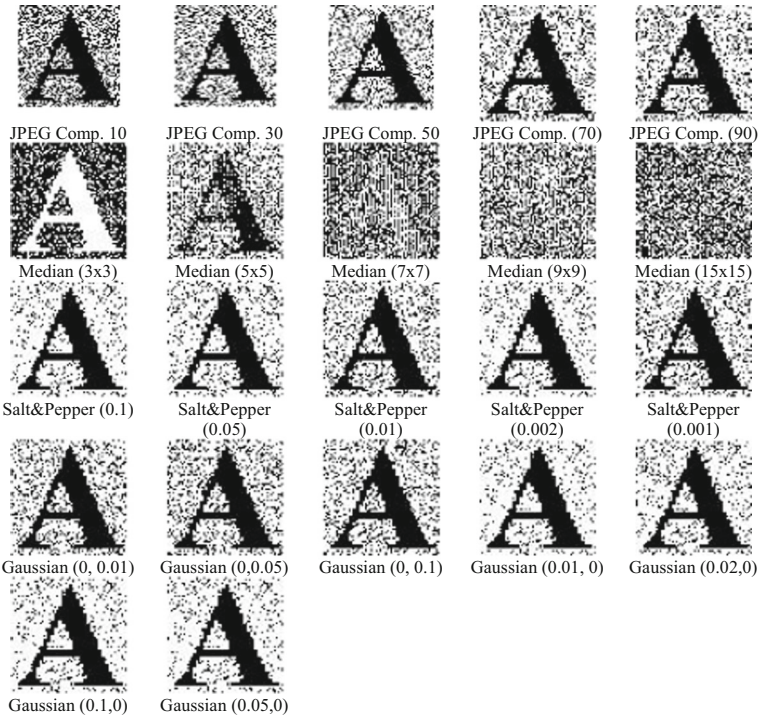


Fig. 13 Quality of watermark image after several attacks

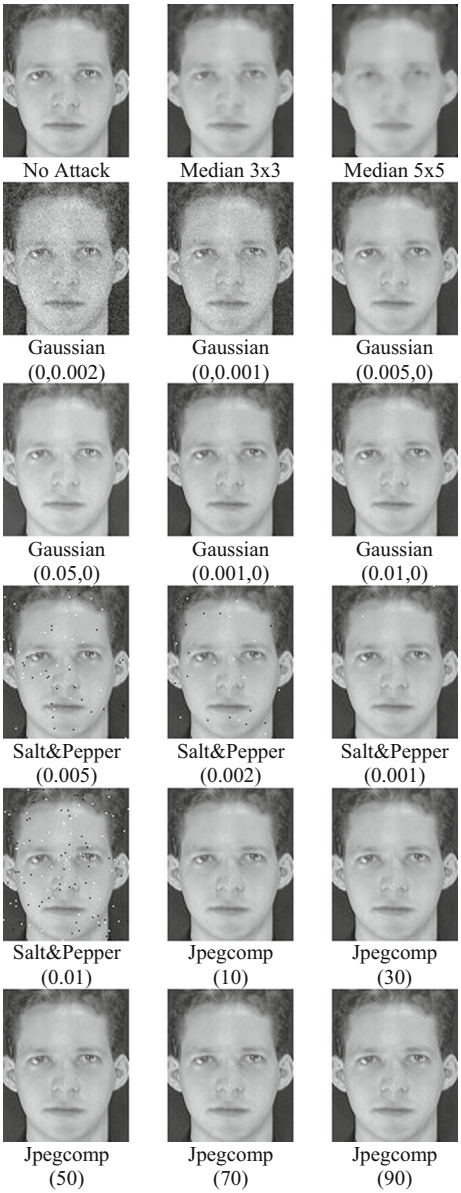


Fig. 14 Samples of various attacked images

accuracy measurements for face recognition, watermark detection, and watermark robustness are used for this experiment. The measures are to see how much degradation would the watermark technique affect the PCA recognition rate in the three mod combinations/models:

- Model 1: PCA-LSB
- Model 2: PCA-DCT (our choice)
- Model 1: PCA-DWT

Table 7 Face recognition rate comparison for Model 1, Model 2 and Model 3 under various attacks

Attack	Model 1 (PCA+LSB)	Model 2 (PCA+DCT)	Model 3 (PCA+DWT)
No attack	98.74	98.91	98.79
Median Filter (3 × 3)	95.96	96.24	95.94
Median Filter (5 × 5)	84.87	85.27	84.75
Gaussian Noise (0,0.001)	98.32	98.48	98.66
Gaussian Noise (0,0.002)	97.95	98.62	98.47
Gaussian Noise (0.001,0)	98.74	98.91	98.79
Gaussian Noise (0.005,0)	88.41	90.76	88.72
Gaussian Noise (0.01,0)	19.84	26.49	20.68
Salt&Pepper (0.001)	98.58	98.78	98.68
Salt&Pepper (0.002)	98.37	98.62	98.45
Salt&Pepper (0.005)	97.72	98.03	98.08
Salt&Pepper (0.01)	96.16	96.57	95.78
JPEG compression (10 %)	98.74	98.91	98.79
JPEG compression (30 %)	98.74	98.91	98.79
JPEG compression (50 %)	98.74	98.91	98.79
JPEG compression (70 %)	98.74	98.91	98.79
JPEG compression (90 %)	98.74	98.91	98.79

Table 8 Watermark detection rate comparison for Model 1, Model 2 and Model 3 under various attacks

Attack	Model 1 (PCA+LSB)	Model 2 (PCA+DCT)	Model 3 (PCA+DWT)
No attack	0.72	0.97	0.64
Median Filter (3 × 3)	0.71	0.74	0.56
Median Filter (5 × 5)	0.71	0.59	0.56
Gaussian Noise (0,0.001)	0.56	0.69	0.54
Gaussian Noise (0,0.002)	0.56	0.63	0.55
Gaussian Noise (0.001,0)	0.72	0.97	0.51
Gaussian Noise (0.005,0)	0.41	0.95	0.51
Gaussian Noise (0.01,0)	0.42	0.97	0.51
Salt&Pepper (0.001)	0.72	0.94	0.57
Salt&Pepper (0.002)	0.72	0.89	0.54
Salt&Pepper (0.005)	0.72	0.80	0.51
Salt&Pepper (0.01)	0.72	0.69	0.51
JPEG compression (10 %)	0.72	0.55	0.56
JPEG compression (30 %)	0.72	0.61	0.55
JPEG compression (50 %)	0.72	0.70	0.54
JPEG compression (70 %)	0.72	0.79	0.55
JPEG compression (90 %)	0.72	0.95	0.54

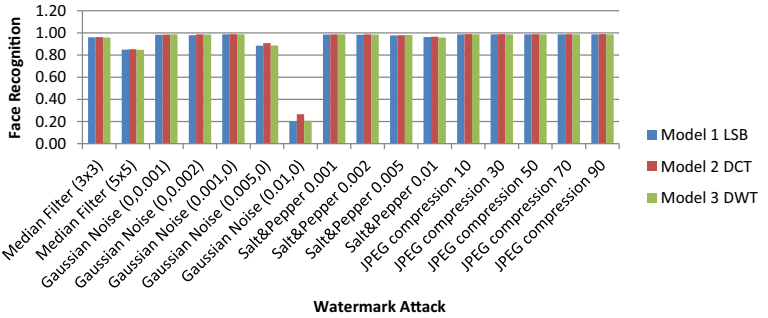


Fig. 15 Face recognition rate comparison with methods of Model 1, Model 2 and Model 3 under various attacks

In the initial part of the experiment, the three models are evaluated based on face recognition accuracy as well as watermark robustness against signal processing attacks, essentially by adding noises, some effects of which are illustrated Fig. 14.

The face recognition rate is measured using the PCA algorithm to investigate the effect of the watermarking. The correlation factor, as given by the following equation [30], is computed to measure the similarity between the embedded watermark denotes as w and $\hat{w}$ is the extracted watermark for watermark detection.

$$\rho(w,\hat{w}) = \frac{\sum_{i=1}^{N} w_i \quad \widehat{w}_i}{\left(\sqrt{\sum_{i=1}^{N} w_i^2}\sqrt{\sum_{i=1}^{N} \hat{w}_i^{\,2}}\right)} \tag{4}$$

6.6.1 Experiment A – face recognition rate

The experiment results are given in Table 7, which shows the face recognition verification accuracy rate of the three models when exposed to the various noise attacks. The results show that all the models produce high recognition rates with little difference amongst them under normal circumstances when no attacks are taking place. Nonetheless, Model 2 (PCA-DCT) still has the best recognition rate at 98.91 %.

When under attack, the results show that the recognition rate slightly decreases for all the models except for under the Gaussian Noise (0.01.0) attack, where all the recognition rates

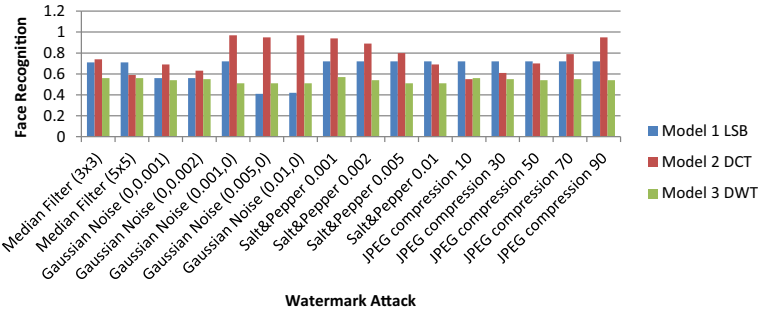


Fig. 16 Watermark detection rate comparison with methods of Model 1, Model 2 and Model 3 under various attacks

drop tremendously. This is obviously because the face image cannot be recognized anymore as the attack is simply too heavy and has destroyed the image. In the rest of the table, it can be seen that, overall, Model 2 has better results when compared with the two models.

6.6.2 Experiment B - watermark detection (Robustness)

In this part of the experiment, the robustness of the three models is measured to find out the immunity of the watermark against attempts to remove or degrade unintentionally, with the same types of digital processing attacks. Table 8 gives the results, showing clearly that Model 2 outperforms the other models. *[Note also here that the detection rate of 0.75 and above is considered acceptable, as the watermark can still be fully recovered* [2]*.]*

The results from Tables 7 and 8 can be re-represented as in the following Figs. 15 and 16 for a better presentation to compare the performance of the three models.

The results from the above show that the PCA-DCT combination (Model 2) is the best combination amongst the three for the watermarked face recognition scheme, showing both high recognition and watermark detection rates as well as robustness against various attacks.

Experiment 1 is for the main objective, experiment 2 is towards non-degradation, supported by experiment 5, as the claim also includes a proposal for a secure face recognition and watermarking combination. Experiment 3 is a pre-requisite for all the other experiments, while experiment 4 is for computing robustness of the watermarked face recognition scheme.

7 Conclusion

This paper has presented a proposal for a watermarked face recognition scheme with a suitable and viable combination of a face recognition system and a watermarking system, namely a PCA—DCT system that will ensure the authenticity of the data being transmitted in the face recognition system, which will then increase its level of security. The contributions from this research constitute a meaningful solution step to the security problems associated with biometric techniques and to the area of digital image processing. In addition, it is hoped that the outcome of this research will stimulate further research by opening up more research gaps in the area of combining biometric and watermarking techniques.

The PCA-DCT combination is shown not to degrade the performance of the individual systems, and the proposed watermarked face recognition scheme will ensure the authenticity of the data being transmitted in the face recognition system at the 8 vulnerable positions where data may be intercepted and/or reinserted. Moreover, the watermarking scheme is shown to be robust against signal processing attacks, and in particular the watermark cannot be easily removed by an attacker.

Within the proposed watermarked face recognition scheme, a logo and a timestamp are embedded as watermarks. The logo serves as an authentication item if the face image is stolen, while the timestamp works as a session ID, which is the main security enhancer. When a face image or feature set is stolen from within the process and then reinserted back to the system, it will be immediately recognised as coming from a different session and will be rejected.

With positions a and h (in Fig. 1) being not within the scope of this research, and that positions e, f,g, h being not relevant for reinsertions, the remaining $7 \times 4 = 28$ situations have been found to be fully secured. This means that within the $8 \times 8 = 64$ total vulnerable positions:

- $7 \times 4 = 28$ are fully covered with this proposal
- $8 \times 4 = 32$ are irrelevant
- $2 \times 2 = 4$ are left for future work

References

1. Adler A (2003) Sample images can be independently restored from face recognition templates. http://www.site.uottawa.ca/»adler/publications/2003/adler-2003-fr-templates.pdf. Accessed 12.05.15
2. Al-Haj A (2007) Combined DWT-DCT digital image watermarking. J Comput Sci 3(9):740–746
3. Bansal R, Sehga P, Bedi P (2012) Securing fingerprint images using a hybrid technique. Proceedings of the International Conference on Advances in Computing, Communications and Informatics 557-565
4. Bedi P, Bansal R, Sehgal P (2012) Multimodal biometric authentication using PSO based watermarking. Proc Technol 4:612–618
5. Behera B, Govindan V (2013) Improved multimodal biometric watermarking in authentication systems based on DCT and phase congruency model. Int J Comput Sci Netw 2(3):123–129
6. Chen CH, Chang LW (2005) A digital watermarking scheme for personal image authentication using eigenface. Lect Notes Comput Sci 3333:410–417
7. Gonzalez RC, Woods RE (2002) Digital image processing. Prentice Hall, Upper Saddle River
8. Gunsel B, Uludag U, Tekalp AM (2002) Robust watermarking of fingerprint images. Pattern Recogn 35(12):2739–2747
9. Henniger O, Scheuermann D, Kniess T (2010) On security evaluation of fingerprint recognition systems. International Biometric Performance Testing Conference (IBPC), pp. 1–10
10. Hill C (2001) Risk of masquerade arising from the storage of biometrics. Master's thesis, Australian National University
11. Hoang T, Tran D, Sharma D (2008) Remote multimodal biometric authentication using bit priority-based fragile watermarking. 19th International Conference on Pattern Recognition
12. Inamdar V, Rege P (2014) Dual watermarking technique with multiple biometric watermarks. Sadhana 39(I): 3-26
13. Isa MRM, Aljareh S (2012) Biometric image protection based on discrete cosine transform watermarking technique. IEEE Proc. of International Conference on Engineering and Technology (ICET), pp. 1-5
14. Isa MRM, Aljareh S, Zaharin Y, Minoi JL (2016) A watermarking technique to improve the security level in face recognition systems: an experiment with Principal Component Analysis (PCA) for Face Recognition and Discrete Cosine Transform (DCT) for Watermarking. IEEE International Conference on Information and Communication Technology – 2016 (ICICTM'16)
15. Islam MR, Sayeed MS, Samraj A (2008) A secured fingerprint authentication system. J Appl Sci - Asian Netw Sci Inf 8(17):2939–2948
16. Jafri R, Arabnia HR (2009) A survey of face recognition techniques. J Inf Process Syst 5(2):41–68
17. Jain AK, Uludag U (2002) Hiding biometric data. IEEE Trans Pattern Anal Mach Intell 25(11):1494–1498
18. Jain AK, Uludag U, Hsu RL (2002) Hiding a face in a fingerprint image. Pattern Recogn 16(3):756–759
19. Kekre HB, Sarode T, Natu S (2015) Biometric watermarking using partial DCT-Walsh wavelet and SVD. 2015 Third International Conference on Image Information Processing (ICIIP). IEEE
20. Li C, Ma B, Wang Y, Zhang Z (2010) Protecting biometric templates using authentication watermarking. In: Qiu G, Lam KM, Kiya H, Xue X-Y, Kuo C-CJ, Lew MS (eds.) PCM 2010. LNCS, 6297:709–718
21. Ma B, Li C, Wang Y, Zhang Z, Wang Y (2010) Block pyramid based adaptive quantization watermarking for multimodal biometric authentication. 20th International Conference on Pattern Recognition 1277–4
22. Moon D, Kim T, Jung SH, Chung Y, Moon K, Ahn D, Kim SK (2005) Performance evaluation of watermarking techniques for secure multimodal biometric systems. In: Hao Y, Liu J, Wang Y-P, Cheung Y-M, Yin H, Jiao L, Ma J, Jiao Y-C (eds.) CIS 2005. LNCS (LNAI) 3802:635–642
23. ORL (2002) The Database of Faces. http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html. Accessed 12.03.12
24. Park KR, Jeong DS, Kang BJ, Lee EC (2007) A study on iris feature watermarking on face data. In: Proceedings of the ICANNGA 2007. Lect Notes Comput Sci 4432:415–423

25. Poljicak A, Mandic L, Agic D (2011) Discrete Fourier transform - based watermarking method with an optimal implementation radius. J Electron Imaging 20(3):033008-1–033008-8
26. Putte T, Keuning J (2000) Biometrical fingerprint recognition: don't get your fingers burned. IFIP TC8/WG8.8, Fourth Working Conference on Smart Card Research and Advanced Applications, pp. 289–303
27. Ratha NK, Connell JH, Bolle RM (2000) Secure data hiding in wavelet compressed fingerprint images. Proceedings of ACM Multimedia 127–130
28. Ratha NK, Connell JH, Bolle RM (2001) An analysis of minutiae matching strength. Proceedings AVBPA 2001, Third International Conference on Audio- and Video-Based Biometric Person Authentication 223–228
29. Salahi E, Moin MS, Salahi A (2008) A new visually imperceptible and robust image watermarking scheme in contourlet domain. Proceedings of the IIHMSP
30. Sangeeta J, Anjali B (2010) Robust digital image-adaptive watermarking using BSS based extraction technique. Int J Image Process 4(1):77–88
31. Tzouveli P, Tsapatsoulis N, Ntalianis K, Kollias S (2002) Automatic face region watermarking using qualified significant wavelet trees. Proceedings of 9th International Workshop on Systems, Signal and Image Processing, Control Systems Centre Manchester, United Kingdom (November, 2002) 101–103
32. Vatsa M, Singh R, Mitra P, Noore A (2004) Digital watermarking based secure multimodal biometric system. in: Proceedings of IEEE International Conference on Systems, Man, and Cynernetics
33. Vatsa M, Singh R, Noore A (2007) Feature based RDWT watermarking for multimodal biometric system. Image Vis Comput
34. Viola P, Jones MJ (2004) Robust real-time face detection. Int J Comput Vis 57:137–154
35. Wang Z, Conrad A, Rahim H, Simoncelli E (2004) Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process 13(4)
36. Weilong C, Meng JE, Shiqian W (2005) PCA and LDA in DCT domain. J Pattern Recognit Lett 26:2474–2482
37. Wu L, Deng W, Zhang J, He D (2009) Arnold transformation algorithm and anti-Arnold transformation algorithm. Proc. of 1st International Conference on Information Science and Engineering (ICISE2009), pp. 1164–1167
38. Yan J, Liu L (2010) An information hiding algorithm based on RDWT for fingerprint biometric system. 2nd International Conference on Signal Processing Systems (ICSPS) 3(V3): 597–599
39. Zhang Z (2011) Improving security for facial image using fragile digital watermarking, face analysis, modeling and recognition systems. InTech 2011. http://www.intechopen.com/books/face-analysis-modeling-and-recognition-systems/improving-security-forfacial-image-using-fragile-digital-watermarking. Accessed 12.03.12

Mohd Rizal Mohd Isa received the BSc in Data Communication and Networking and MSc in Information Technology degrees respectively, from the Universiti Teknologi MARA (UiTM), Malaysia. He is currently doing his Ph.D degree at the University of Portsmouth, United Kingdom. His research interests include biometric systems and information hiding.

Salem Aljareh received his Ph.D. from Newcastle University, United Kingdom. Currently, he is a senior lecturer with the School of Engineering, University of Portsmouth, United Kingdom. His research interests are in network and information security includes mobile network security and information hiding.

Zaharin Yusoff is a professor in computational linguistics and a Fellow of the Academy of Sciences Malaysia (UPNM). He is currently serving at the University of National Defence Malaysia. He began his career at Universiti Sains Malaysia in Penang in 1980, and served there for 25 years, before moving to MIMOS, a research institution in Kuala Lumpur. He then moved to UNITEN, a private university, in 2007, before being appointed as the President of Multimedia University for 3 years. Since then, he held a position in a company, in parallel with a university appointment at Universiti Malaysia Sarawak, followed by his current position at UPNM. He has published numerous papers, won many research and commercialisation grants, graduated many postgraduate students, and led various initiatives nationally and internationally.