Research Journal of Applied Sciences, Engineering and Technology 13(6): 481-494, 2016
DOI:10.19026/rjaset.13.3008
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: November 6, 2015 Accepted: January 13, 2016 Published: September 15, 2016

Research Article

An Overview of Multimodal Biometric Approaches Based on Digital Image Watermarking

Abdulmawla Najih, S.A.R. Al-Haddad, Abd Rahman Ramli and S.J. Hashim,
Mohammad Ali Nematollahi
Department of Computer and Communication Systems Engineering, Faculty of Engineering, Universiti Putra Malaysia, UPM Serdang, 43400 Selangor Darul Ehsan, Malaysia

Abstract: In this review study, a different multimodal biometric approach based on digital image watermarking is discussed. Although some of the multimodal approaches combined the score of each biometric system separately, applying biometric digital image watermarking is useful due to more security and simplicity issues In spite of difficulties to develop multimodal biometric systems, currently many studies are done to improve these systems. However, it seems it is required to have one review paper in this area for researchers who currently work in this field. The results show that embedding voice biometric in face image not only can improve the recognition performance, but also, can improve the security of the multimodal biometric systems.

Keywords: Biometrics, digital image watermarking, face recognition, multimodal systems, voice recognition

INTRODUCTION

In recent years, computer networks and different digital systems of documents record have wonderful development and the increasing use of computer and internet helps to distribute multimedia data such as text, image, sound and film. So protection of digital data against copyright and illegal distribution of digital document is one of the important issues which have allocated many types of research (Agarwal *et al*., 2014; Ghazy *et al*., 2015; Ghouzali, 2015).

Recent research shows that watermarking is one of the most effective methods for protecting of digital multimedia (Bhatnagar and Raman, 2012; Arya and Siddavatam, 2013; Agarwal *et al*., 2014). In a watermarking system, some additional information (watermark) hides in the signal so it can be used for rightful ownership, protecting copyright and etc. Additional information which adds to digital document as a watermark can be about noise, image, or a binary sequence. Certainly, this additional information should not destroy the quality of the main signal or omit simply from the main signal.

The problem is that the embedding of watermark information via watermarking algorithms is more complicated than set this information as a header file and the watermark perhaps reduced vocal and pictorial quality. Nevertheless, many companies are offering copyright protection and broadcast monitoring based on watermarking.

Watermarking techniques can be broadly classified into two categories: Embedding watermarks in the spatial domain or applied help from different transform domain techniques. In comparing to the transform domain, spatial domain needs shorter performance time and less hardware. The simplest technique which is performed in the spatial domain is using of Least Significant Bits (LSB) which directly modify the intensity of some selective pixe. Transform domain methods are more resistant than special domain algorithms because of providing the possibility to choose a transform with desired properties and use it to optimize embedding of watermark. In this domain, first, the information transfer to transform domain and then the watermark is embedded in transforming coefficient. As regards the watermark is typically propagated along the image in the spatial domain, so its read and modification would be so difficult for aggressors. Transform or frequency domain methods are mainly consisted of DFT (Kang *et al*., 2003), DCT (Wang and Alan, 2006) DWT (Fan and Yanmei, 2006; Vatsa *et al*., 2009; Fouad *et al*., 2010) CT (Mohan and Kumar, 2008) and SVD (Ghazy *et al*., 2015) or the combination of them (Navas *et al*., 2008).

Generally, face recognition has a wide applications (law enforcement application and commercial applications) such as access control, security issues, surveillance and bankcard identification. A formal approach has been proposed for classifying faces

Corresponding Author: Abdulmawla Najih, Department of Computer and Communication Systems Engineering, Faculty of Engineering, Universiti Putra Malaysia, UPM Serdang, 43400 Selangor Darul Ehsan, Malaysia

Table 1: Comparison among different biometric recognition technique

Biometric/ Attributes	FNMR (%)	FMR (%)	Database	Ease of use	Template size	Sensor cost	Long term stability	User acceptance	Variability
Face	6	6	CESG	M	1 kB	<100$	M	H	Head pose, Lighting, Background, Glasses, Hair, Facial expression, Age.
Voice	7	7	NIST	H	2-3 kB	<25 $	M	H	Illness, age, stress, environment.
Iris	2	0.0001	CESG	L	256 Byte	<400 $	H	L	Poor lighting, eye position.
Fingerprint	2	0.02	CESG	M	0.5 kB	<200$	H	M	Dryness, sensor noise, Dirt, Bruises .
Hand	3	0.3	CESG	H	0.1 kB	< 1500$	M	M	Injury, age.

H: High, M: Medium, L: Low

(Galton, 1889). In this technique, facial profiles are collected as curves next their norm has been calculated and finally other profiles classified by its deviation from the norm.This technique uses a vector of independent which can be measured with other vectors. Table 1 presents the comparison among various biometric techniques. As seen, face recognition has reasonable biometric technique overall.

In order to provide an experiment, various multimodal techniques are compared. For this purpose, the recognition rate, equal error rate, robustness, imperceptibility and capacity of each multimodal biometric system based on digital image watermarking are compared. In addition, the advantages and disadvantages of each technique are discussed.

Finally, the main objective of this study is providing an overview of the multimodal (Kalra and Lamba, 2014) biometric approach which are based on digital image watermarking.

LITERATURE REVIEW

In this section, we explain the techniques and the methods which are applied for image watermarking in the summary.

Discrete cosine transform: In general, we can express an image according to a sum of the cosine functions oscillating at different frequencies. Discrete cosine transform is a technique which transforms a signal from a spatial representation of a frequency representation.

The main application of this transform is signal compression, which is the key part in many standardized algorithms.The based line of compression standard algorithms such as JPEG and MPEG work with this established. The popularity of discrete cosine transforms in signal compression is basically related to its centralization property of energy in coefficient which has smaller indexes. Indeed, the coefficient values which have smaller indices play more influence in the calculation of image pixel value in spatial domain when the inverse discrete cosine transform is calculated.

The other reason of using discrete cosine transform is the widespread study on the basis of vision model in this domain which can be performed for better watermarking methods.

Discrete contourlet transform: Contourlet transform is presented by Do and Vetterli (2005). This transform can capture the intrinsic geometrical structure which is the key of the visual information.The main challenge of exploring geometry in the image comes from the discrete nature of the data. Thus, unlike other methods such as Curvelet that first develops a transform in the continuous domain and then discretize for sampling data (Ma and Plonka, 2010), the present method starts with a discrete domain construction and then studies its convergence to an expansion in the continuous domain.Specifically, it designs a discrete domain, multi-resolution and multi-direction expansion using non-separable filter banks, in much the same way that wavelets were derived from filter banks. This construction results in a flexible multi-resolution, localization and directionality for image expansion using contour segments.If we combine the wavelet transform which is a multi-resolution transform and applies to identify point discontinuity of images, to a directional filter bank, we have transformed point discontinuities into a linear structure. Such combination is called the Pyramidal Directional Filter Bank (PDFB) and its expansion is called Contourlet Transform (CT((Po and Do, 2006). Figure 1 illustrates a block diagram of contourlet transform which exploit an iterated combination of the Laplacian pyramid and the directional filter bank. Meanwhile, it has a worthwhile frequency decomposition that the spectrum is divided either radially and angularly. This resulting frequency division has been shown in Fig. 1.

Contourlet transform is a unique transform in which the number of directional bands can be determined by the user. In usual, the main image decomposes up to level 5 including 1, 2, 4, 8 and 16 under the directional band in which L is the low-frequency band of image and W, X, Y and Z are directional partial bands.

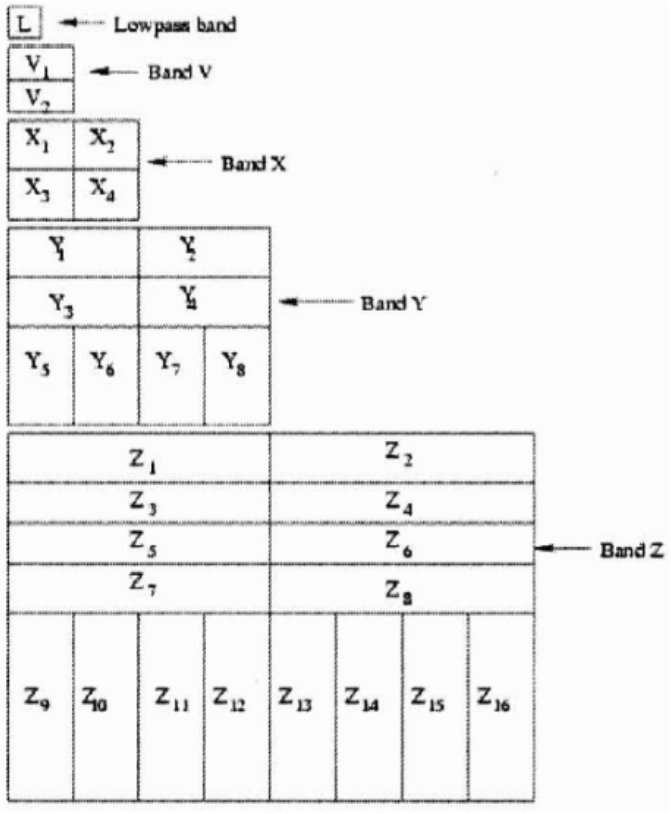

Fig. 1: Directional decomposition of different level contourlet transform (Narasimhulu and Prasad, 2010)

Singular value decomposition: One of the most important tools for separation and resolution to simplify the solution of linear big devices is singular value decomposition. This method is an extension of eigenvalue decomposition of square apertures, with this difference, that in this method we can transform each matrix with any dimension to the product of three matrices which one of them is diagonal and two other matrixes are also orthogonal matrices. This method is a popular technique in linear algebra which has applications in matrix inversion, obtaining a low dimensional representation of high dimension data. This technique has been used in a vast range of applications such as pattern recognition, watermarking and data compression.In watermarking applications, the watermark is usually embedded in eigenvalue matrices.In this method, a real matrix $A_{m\times n}$ with rank k can be decomposed such that:

$$A = USV^T \quad (1)$$

where, $U_{m\times m} = [U_1, \ldots, U_m]$ and $V_{n\times n} = [V_1, \ldots, V_n]$ are orthogonal matrices and $S_{m\times n}$ is a diagonal matrix which the elements on its diagonal are nonzero singular values of AA^T or A^TA matrix.If the watermark embeds in orthogonal matrices, it will become perceivable and is not resistant against different attacks.

MATERIALS AND METHODS

Face recognition systems are just small part of the facial image processing application which is currently applied in many biometric for security purposes. Many biometrics including palm fingerprint, face, signature, voice and iris have used it. However, gathering information in all these systems required to cooperate user. There is a possibility in face recognition systems to gather facial information from webcams without subject‘s cooperation which can be assumed as a non-collaborative biometric system.

Face recognition systems are widely applied in security systems. Face recognition systems can be used for authentication, person verification, video surveillance, preventing crime and security activities.

In real world condition, a face recognition system has complexity due to image processing problems can be considered as a complex system with huge effects of occlusion, illumination and imaging condition on the live images.

Face recognition systems should be applied face recognition as well as face detection. Face detection uses detection applications to find the position of the face in the image.

The recognition section applies recognition algorithms to classify given images and recognize the

Fig. 2: Steps of face recognition system applications

new face image. These face images usually have some known properties like; same resolution and are consist of same facial feature components. The standard face recognition algorithms have been used in order to detect eyes, eyebrows, nose and mouth.

First, the image should be captured by the camera for face recognition purpose. The second step in a face recognition system is face detection from the acquired image of the previous step. In the third step, face recognition system illustrates the results according to the result of the recognition algorithms which is the identity of the input image. The final step is a person‘s verification or identity as a result of the face recognition system.

The steps in the face recognition system which will be applied in this thesis, is shown in Fig. 2.

The input face image, which is fed to face recognition system, is in digital form. When the face image is captured, the feature should be extracted from it. This Feature extraction of facial image which can be divided into two main categories: appearance-based and knowledge-based approaches.

Basically, knowledge-based approaches are based on the specific features of the face. However, an appearance-based approach has been applied the whole feature in the facial image. In this thesis, appearance approach is used due to the generality and robustness.

Face recognition can be classified into two main groups, including static and video image. Although some biometric systems use behavior pattern, face recognition verifies a person based on physiological characteristics. Face recognition is a non-invasive method which does not need direct contact for user-friendly. In the face recognition system, three steps are included):

- A image is captured by the sensor.
- A computer has normalized the image to the system image database.
- The comparison has matched the similarity between the normalized image and database image set.

Three processes are considered for face recognition systems. First, the availability of the face in image or video must be detected which is known as face detection. Second, the feature should be extracted from the image which is called feature extraction process. Third, this feature should be compared with face model, which is already trained; it is known as face recognition process. All these processes can be seen in Fig. 3.

Voice recognition system: Voice is the most important form of human communication as it reveals valuable information about a person. Voice recognition is a kind of speech recognition system with voice identification which involves identifying an unknown voice by using a population of known voices. This system also has voice verification, as the most popular type of general biometric verification method which aims to verify the identity of a given voice from a population of known voices.

Voice recognition is designed as a system of pattern recognition. Firstly, a speech signal is sampled, quantized and filtered. Then, it is used for the extraction of acoustic features. Secondly, this system uses the acoustic features for training a voice model. In the recognition) testing (phase, the extracted features from a test speech signal are matched with a voice model for scoring. Enrollment and recognition phases in an online recognition system which can be online voice verification with the result of acceptance or rejection or online voice identification with the result of voice ID. The demand for voice recognition applications comes from various fields, namely, tele-commerce, automobile industry, robotics, forensics, airports, smart homes, office environments and law courts.The voice recognition system may not be popular for on-site application where the person needs to be in front of the system to be recognized due to its inability to provide a certain level of reliability and security as compared to other biometric recognition techniques such as iris printing and fingerprinting. However, this system is still

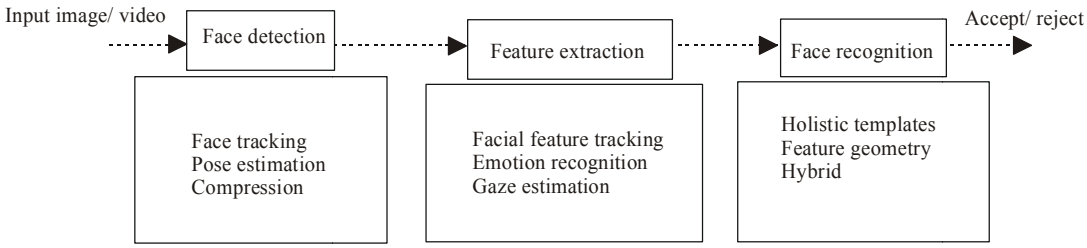

Fig. 3: Different processes in face recognition systems

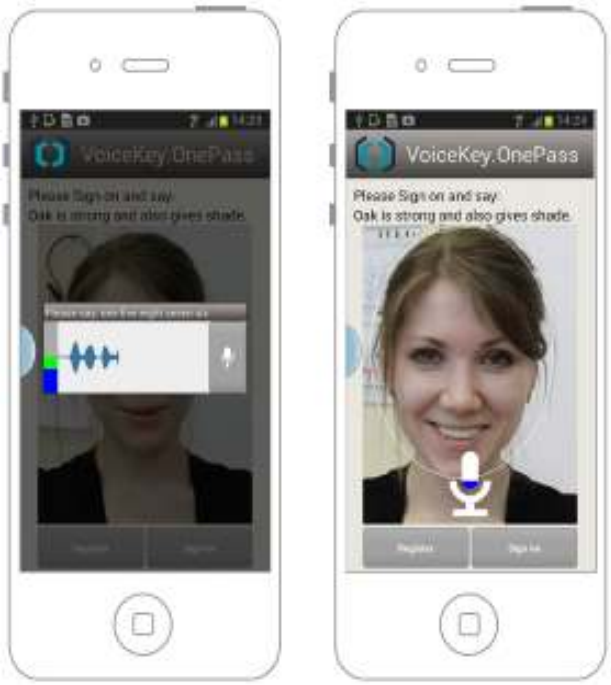

Fig. 4: IOS apps of voice key for smart phone (SPEECHPRO, 2015)

popular for online applications where the person can access the system through a remote terminal such as telephone or network (Bimbot *et al*., 2004). Online voice recognition is also feasible for biometric system developers due to three main reasons (Fazel and Chakrabartty, 2011). Firstly, speech is easy to be produced, captured and transmitted as it has a lower cost compared to other biometric recognition techniques. Secondly, the speech is non-invasive and does not need direct contact with or to be perceived by an individual. Thirdly, speech can reveal information about an individual‘s gender, age and emotion which is hidden from other biometric recognition techniques such as iris printing and fingerprinting (Fazel and Chakrabartty, 2011). Traditionally, the main application for voice recognition is to be useful wherever there is a need to recognize a voice conversation over voice channels such as telephone, wireless phone, or Voice over IP (VoIP). Secure and robust recognition is the primary concern of an online voice recognition system for commercial applications. In this thesis, the main interest is increasing the security of communication channel and recognition performance of voice recognition systems. Figure 4 shows a multimodal biometric IOS app based on face recognition and voice recognition systems.

RESULTS AND DISCUSSION

A multimodal approach has been proposed by the combination of signature and face image through image watermarking (Arya and Siddavatam, 2013). Two cascading Lifted Wavelet Transform (LWT) is used to embed two biometrics. In this approach, two biometric including face and offline handwritten signature are embedded in a host image. In Vatsa *et al*. (2006), a technique has been proposed by a combination of fingerprint and face images. For this purpose, the face image is embedded in fingerprint image through robust biometric image watermarking. In the developd image watermarking technique, a combination of Least Significant Bit (LSB) and DWT has been applied in order to improve the security of biometric systems. In this approach, fingerprint image was used as host image which carries facial features as embedded watermark. Although this approach has outperformed than LSB and DWT separately, it still has the lack of enough robustness against geometrical attacks. Another approach (Ghouzali, 2015) has been developed by embedding fingerprint minutia into the face image by using block wised DCT image watermarking. For watermark bits extraction, Orthogonal Locality Preserving Projections (OLPP) have applied, which is getting a projection matrix of the watermark data.

In Chaudhary and Nath (2015), a new multimodal approach has been proposed by the combination of voice, face and iris without watermarking. Although it can improve the accuracy, the time and cost are the main issues. Another multimodal verification technique has been proposed by the combination of voice recognition and face recognition system (Soltane *et al*., 2010). In this technique, fusion decision on the score of

Table 2: Comparison among various multimodal approaches

Technique	Image watermarking	Advantages	Disadvantages
Face+Fingerprint (Vatsa *et al*., 2006)	LSB+DWT	Easy to use	Accuracy, semi-blindness, not robust to geometrical attacks
Iris+Face+Voice (Chaudhary and Nath, 2015)	None	High verification performance.	High time, memory and cost. Low security due to lack of using watermarking.
Face+Voice (Soltane *et al*., 2010)	None	Easy to use	Low security. Low verification performance.
Face+Handwrite Signature (Arya and Siddavatam, 2013)	LWT	Simplicity.	Need high capacity image for watermarking both face and signature. Lack of integrated image watermarking technique. Low security and feasibility.
Face+Voice (Wang *et al*., 2013)	DCT-QIM	Reasonable verification, Tamper Detection, robust against attacks.	Degrade face image quality due to embed huge watermark data.
Face +Fingerprint (Ghouzali, 2015)	Block wise-DCT	Embed low watermark data. Efficient watermark Extraction approach.	Low image imperceptibility. Low verification rate.
Face+Voice+handwrite Signature (Inamdar and Rege, 2014)	DCT-DWT	High verification performance.	Low imperceptibility, Low cost. High complexity, time and memory.
Face+Voice (Vatsa *et al*., 2009)	RDWT	High imperceptibility	Low robustness. Low imperceptibility. High complexity

face and voice has been applied to improve the performance of verification. In Wang *et al*. (2013), a multimodal person authentication technique has been developed by the combination of MFCC and facial features. Then, a double image watermarking technique based on DCT and QIM is applying to embed MFCC into the face image. This image watermarking technique embeds the fragile watermark where eyes, mouth and nose are located which can be considered as salient facial regions. However, the robust watermark is embedded into background face image. Although it would be an efficient approach, it cannot embed both fragile and robust watermarks into the face image due to huge capacity of watermark data. Other multimodal approach has been proposed based on voice and faces biometric features (Vatsa *et al*., 2009). In this approach, phase congruency is applied to preserve the most important region of the face image. Then, three level Redundant Discrete Wavelet Transform (RDWT) is applied to embed the MFCC features of the voice into the red and blue channels of a color face image. Finally, a multimodal approach is presented by combining facial, voice and offline handwritten signature through double image watermarking. For this reason, Gabor face, LPC of the voice and Chaotic logistic map of the offline signature are embedded inside a host image by using three-stage image watermarking (Inamdar and Rege, 2014). Although the proposed technique has high verification rate, it still needs more complexity due to the usage of three stage image watermarking and various sensors which seems unrealistic approach. Moreover, the quality of the host image is not considered in this approach because embedding three watermark data can seriously degrade the quality of the watermarked image.

Table 2 presents various multimodal approaches based on digital watermarking techniques. As seen, almost all multimodal approaches have been applied face and voice recognition as one of the basic approaches for biometric systems. Although all the systems have some pros and cons, there were not a strong digital watermarking technique which can provide capacity, invisibility and robustness criteria. Furthermore, the degradation effect of the embedded watermark can degrade the face recognition system performance. Moreover, it can be seen that multimodal biometric recognitions based on face and voice are becoming a hot topic in security science which need a huge effort to integrate it into real words.

Multi-resolution decomposition: There are many transformation techniques in the frequency domain such as Fourier Transform (FT), Discrete Cosine Transform (DCT) and wavelet which is used to decompose an image into the frequency domain. However, the wavelet transform is the most common transformation for image watermarking (Lin *et al*., 2008; Bhatnagar and Raman, 2012; Agarwal *et al*., 2014; Ma *et al*., 2014; Yassin *et al*., 2014). DWT represents an analog signal which can be decomposed by the wavelet function in the time-frequency domain. Figure 5 presents some basic Multi-resolution techniques for signal decomposition. As seen, there are many multi-resolution tools have been presented which shows strong time-frequency analysis of these approaches. The most recent multi-resolution approaches may be applied for image watermarking.

Recursive method like Mallat‘s pyramid algorithm (Mallat, 1989) can be used to compute wavelet coefficients. Figure 6 illustrates two dimension wavelet transform in just one level. As seen, wavelet transform decomposes the image into four frequency regions such as Low-Low (LL) High-Low (HL), Low-High (LH) and High-High (HH) (frequency bands. This process can be continued for further decomposition. This technique

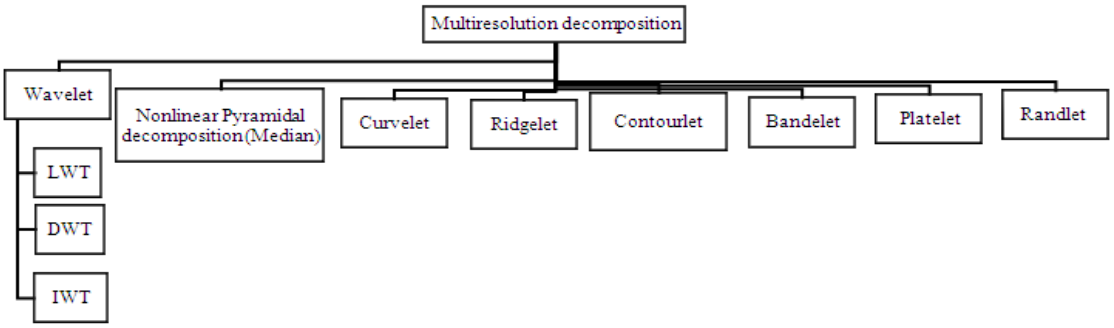

Fig. 5: Multi-resolution techniques

Fig. 6: Single level two dimension DWT

can be simply computed by applying successive low pass and high pass filters. Therefore, image is decomposed with time-frequency analysis technique which can provide multi-resolution and non-stationary analysis of image processing applications like digital watermarking (Mallat, 1989).

Fundamentals of digital image watermarking: Watermarking is a technique and the art of hiding additional data such as watermarked bits, logos and text messages in the host signal, images, videos, audios, speeches or texts, without any perceptibility of the existence of the additional information. The additional information which is embedded in the host signal can be extractable. It also must resist against various intentional and unintentional attacks.

The major challenge in using digital image watermarking is the requirements involved, which are capacity, invisibility and robustness. These requirements oppose one another and to make them meet is difficult.

Types of digital image watermarking: There are two main types of digital Image watermarking in terms of robustness:

- Robust digital image watermarking in which embedding and additional information must resist compression, transmission, geometrical, scaling, rotating and manipulation attacks.
- Fragile digital image watermarking in which additional information must be destroyed if any attack or transformation takes place, like for paper watermarks in bank notes. These watermarks do not survive any kind of copying and can be used to indicate the bill‘s authenticity. Reaching for fragility is more difficult than robustness.

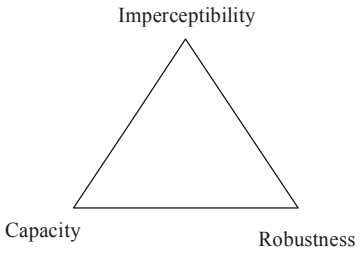

Fig. 7: Requirements of digital image watermarking (Mat Kiah *et al*., 2011)

Three categories are found in terms of source and extraction module for digital image watermarking:

- Blind image watermarking which does not need any extra information such as the original image, logo or watermarked bits. However, in some applications, key uses are needed for generating random sequences.
- Semi-blind image watermarking which may need extra information for the extraction phase like access to the published watermarked signal that is the original image after just adding the watermarks.
- Non-blind image watermarking which needs the original image and the watermarked image.

Requirements of digital image watermarking: The major challenge in using digital image watermarking is due to the requirements which are capacity, imperceptibility invisibility and robustness. These requirements oppose one another and to make them meet is difficult. Figure 7 shows the requirements of digital image watermarking.

Digital image watermarking in terms of robustness: In order to evaluate the robustness of the image watermarking technique, the differences between embedded and extracted watermarks must be computed. Thus, many researchers provides the robustness test which be expressed by Bit Error Rate (BER). The BER measure how embedded and extracted watermark are different which is formulated as in Eq. (1):

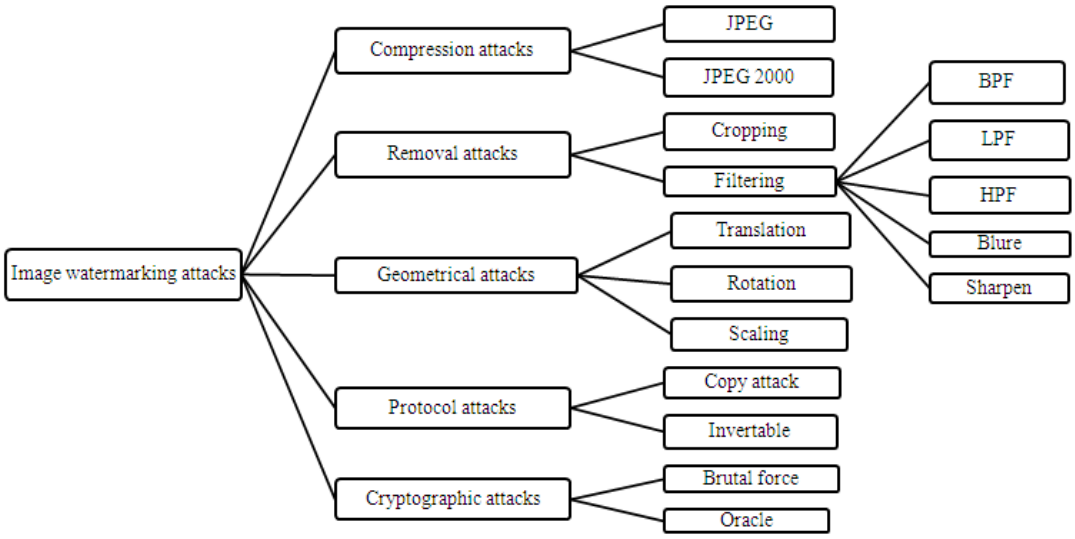

Fig. 8: Classification of different attacks for image watermarking

$$BER(W,\hat{W}) = \frac{Number\_of\_error\_bits}{Number\_of\_total\_bits} = \frac{1}{N}\sum_{i=1}^{N} W(i) \otimes \hat{W}(i) \quad (1)$$

where, corresponds to the XOR operation to find different bits between embedded and extracted watermarks and N shows the watermark‘s length.

Since BER is showing the error for extracting watermark, the high amount for BER shows the less robustness for the watermarking technique. The BER should be computed under various conditions which are known as attack such as noisy, compression, quantization and resembling which provide more fair and valid robustness for the developed image watermarking. The following attacks are common during the image transmission, compression and manipulations which is shown in Fig. 8.

Image attacks: Removal attacks are watermarked attacks that point during evacuating the watermark indicator from the watermarked picture without endeavoring should break that security of the watermarking calculation. This kind of watermark ambush, doesn't endeavor and will figure out those encryption strategies utilized or how the watermark needs to be being installed. It brings about a harmed watermarked image, consequently a harmed watermark signal, the place no basic post preparing could recuperate those watermark indicators from the assaulted information. Incorporated in this class are noising, histogram equalization, smudge and hone attack.

Geometry attack would rather uniquely in relation to evacuation strike. As opposed to pointing to uproot or extremely harm those watermark signals, this sort from claiming attack means on misshape the watermark indicator. It will be Nonetheless morals still hypothetically time permits to that identifier should recoup those first watermark if the point of interest of the geometry assault might make secured and also a countermeasure connected. That methodology from claiming to correct this sort of ambush will be often alluded with similarly as synchronization. However, those unpredictability of the required synchronization methodology could be a chance excessively awful prohibitively exorbitant which is more moderate. Incorporated in this class about watermark strike are picture rotation, scaling, interpretation, which is more, skewing.

The point of claiming cryptographic attack is should split those security systems clinched alongside watermarking schemes and subsequently find an approach with uprooting those inserted watermark majority of the data or an implant misdirecting watermarks. A standout amongst the strategies in this classification may be those brute-force quest strategy. This system extensively endeavors should split the watermark security amount about knowing time permits measures to Eventually Tom's perusing utilizing an expansive scan of the serious mystery data. In turn, the method is called the Prophet attack, which will be used to make a non-watermarked sign at a watermark identifier gadget will be accessible.

Protocol attack is a further sort about watermark ambush. Inasmuch as the opposite sorts from claiming attack point during destroying, distorting alternately extracting the watermark signal, protocol attack include those attacker‘s own watermark signs on to that information being referred to. This brings about ambiguities on the valid proprietorship of the information being referred to. Protocol attack targets the whole idea of utilizing watermarking systems similarly as an answer will copyright insurance.

Table 3: MOS grades (Rec, 1996)

MOS	Quality	Quality scale
5	Excellent quality	Imperceptible
4	Very good quality	Perceptible, but not annoying
3	Fair	Slightly annoying
2	Poor quality	Annoying
1	Very poor quality	Very annoying

Another protocol attack is the duplicate attack: As opposed to destroying the watermark, the duplicate attack estimates a watermark from watermarked information Also duplicates it on some other data, known as those focus information. That assessed watermark is adjusted of the nearby Characteristics of the focus information on fulfilling its intangibility.

Compression attacks: While the image/video is distributed to the public, there is very common to compress it or change the format. Different lossless and lossy techniques such as LZW, JPEG, JPEG 2000 and MPEG have been applied to the image in order to reduce the size. Therefore, the watermark could be enough robustness against common compression attacks.

Digital image watermarking in terms of capacity: Payload known as capacity of the watermark is the maximum numbers of bits carry by carrier in the digital image. It is measured in bit per second (bps).

Digital image watermarking in terms of imperceptibility and invisibility: Imperceptibility or invisibility is the most important issue in digital watermarking science. It means after watermarking the quality and visibility of the watermarked image must not seriously degraded (Akhaee *et al*., 2010; Arya and Siddavatam, 2013; Agarwal *et al*., 2014; Zong *et al*., 2015; Ghazy *et al*., 2015). There are two conventional methods to measure invisibility which are divided into objective and subjective methods.

Objective measurement: The most common objective technique for invisibility of the watermarked image is Peak to Signal Noise Ratio (PSNR). PSNR is defined as in Eq. (2):

$$\mathrm{PSNR}(w,\hat{w}) = 10\log_{10}\frac{MAX_W^2}{\frac{1}{mn}\sum_{i=1}^{m-1}\sum_{j=0}^{n-1}[w(i,j)-\hat{w}(i,j)]^2} \quad (\mathrm{dB}) \tag{2}$$

where, $w, \hat{w}$ are the original and watermarked image and $M \times N$ is the image size and MAX_W is the maximum possible pixel value of the image which is 255.

Subjective measurement: Subjective measurement is not fully correlated with the Human Visual System (HVS) which is based on subjective aspects. Thus, subjective methods are developed to better validate and evaluate the watermarked image. Although many subjective methods have been conducted, Mean Opinion Score (MOS) is the most simple, general and available method. For this purpose, the watermarked image quality is measured by using the proposed method of the International Telecommunications Union (ITU-T) (Rec, 1996). This technique is based on reporting the dissimilarities between the quality of the original and watermarked images. Table 3 presents MOS grades based on the quality of the image:

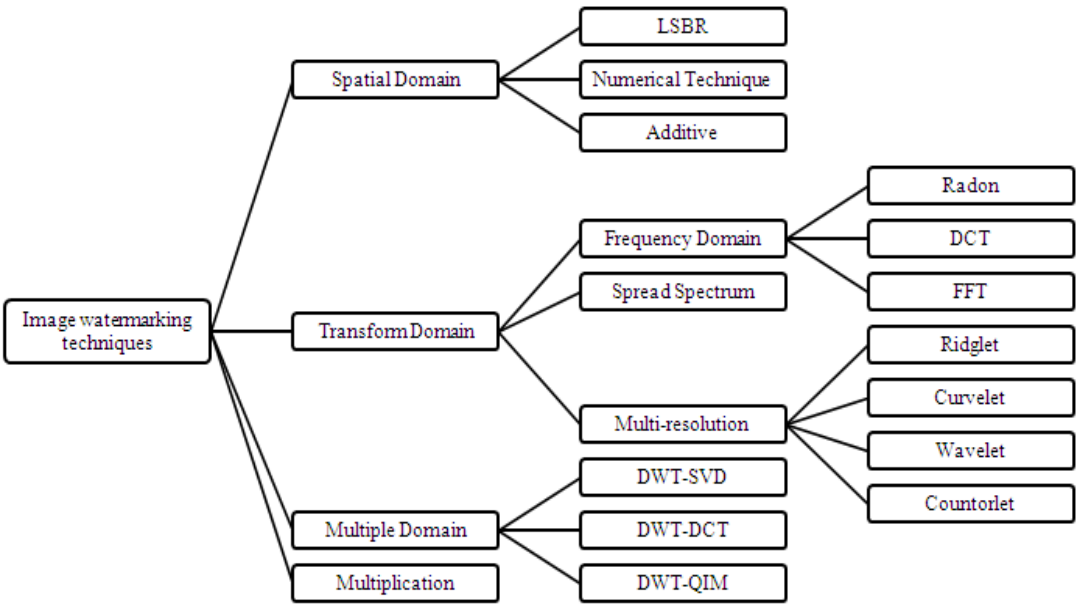

Fig. 9: Image watermarking techniques

Image watermarking techniques: Various domains, including the spatial domain, transform domain and multiple domains are applied for digital image watermarking. Other techniques are available like multiplication method which applies statistical methods to change the distance between two sets of the variance, the energy, or the mean of the signal for embedding the watermark data. However, the main techniques for digital image watermarking can be classified into the following categories spatial domain, transform domain, multiple domain and multiplication method. Figure 9 presents an overview of the different categories and subcategories for each digital image watermarking technique.

Spatial domain: A few systems need be formed to watermark embedding in spatial space. Additive, Least Significant Bit (LSB) replacements as well as Singular Value Decomposition (SVD) are well-known in spatial domain image watermarking. These methodologies utilize straightforwardly on the pixel qualities of the original image.

In this way, a pseudo-random number sequence Pattern noise generated and then embedded directly to image pixel intensity. This pattern is usually an integer value such as (-1, 0, 1) or sometimes float value. For ensuring that the mark can be extracted, using an established pattern noise is the key that the correlation between the numbers of the Keys will be a little different. Embedded binary Sequence W ϵ {0, 1} in the original image can show picture using the following equation (Zeng and Liu, 1999):

Watermarked image = Original Image+α×W

where α is the intensity of the watermark. For watermark detection, which is none blind, the cross correlation between W and watermarked image which is passed or attacked, has completed.

In LSB technique, less relevant maintenance information of an image is modified, which does not affect perceptibility of an image. The basic idea here is the LSB of an 8-bit grayscale image can dispose of the first and then the labs are instead of permuted binary symbols of the same original size.

Instead of frequency transformation, there is strong mathematical decomposition which can be more efficient than basic frequency transformation techniques. Singular Value Decomposition (SVD) is one of these strong numerical technique which is widely applied in image watermarking techniques. The SVD can decompose a rectangular matrix into three basic matrixes such as left eigenvector, eignevlaue and right eigenvector as in Eq. (3). The eigenvalue matrix is a diagonal matrix which the eigenvalues are ordered as descending order like of σ) I (>σ)i+1).

$$A = USVT = 11, \ldots, Unm[\times]S11, \ldots Snn\ [\times]v\ 11, \ldots, Vr\ n\ [T] \quad (3)$$

Basically, small manipulation of the eigenvalues cannot seriously affect the quality of the image signal. Therefore, adding the watermark in eigenvalues can be robust and most possible approached. However, providing enough tradeoff among capacity, invisibility and robustness of this technique can be a challenging problem.

Transform domain: Currently, there are many attentions in applying transformation domain for image watermarking. Instead of modification of pixel value in the special domain, transform domain is modified in the transform value of the images. There are many transformation tools which are widely based on frequency transformation such as DFT, DCT and Wavelet transform. Although watermarking in the transform domain is stronger than the special domain, a huge amount of complexity, time and memory are the main disadvantages of transform domain. For example, DCT needs a huge amount of computational complexity to transform an image to the DCT-domain. Therefore, the majority of digital image watermarking approaches has only applied a block with small size i.e., 8×8 to consume computer resources. Also, Fast Fourier Transform (FFT) is the efficient implementation of DFT.

In Ghazy *et al*. (2015), a comparison has been made to evaluate the robustness of the spatial and transform domains. It is shown that the robustness of the watermark is increased when it is embedded in the transform domain. Furthermore, embedding the watermark in the frequency domain can seriously improve the extraction process under geometrical and non-geometrical image‘s attacks. In Yassin *et al*. (2014), wavelet transformation has been done to computer different sub-bands in the digital image. Then, the watermark bits are embedded by applying Quantization Index Modulation (QIM) which not only provides blindness, but also, it shows good robustness in terms of various types of attacks. However, it cannot provide better capacity for embedding a biometric watermark in the image.

In Akhaee *et al*. (2010), an image watermarking is proposed based on contourlet transformation. By using contourlet transform, the visibility of the watermarked image has been improved due to HVS is less sensitive to an edge where the watermark is embedded in this technique. In Khan *et al*. (2007) and Park *et al*. (2007) two main research on watermarking have been done to embed the watermark in magnitude and phase of Fourier domain respectively.

Another digital image watermarking is proposed based on RDWT (Vatsa *et al*., 2009). This technique applied red and blue components of the color image in order to reduce the visibility of the watermark in watermarked image. In this technique, the watermark

bits are inserted semi-blindly after RDWT is applied on the image. Although it seems this technique has fair capacity due to embedding MFFC feature, the robustness of this technique is not reasonable which can be robust in real channel transformation.

Generally, transform domain has some advantages as compared to the spatial domain. First, it can be more robust due to embed the watermark in low-frequency region. Second, it is more robust under different attacks. Third, the amount of injected dissertation can be controlled which is more difficult to achieve for spatial domain.

Multiple domains: In this part, multiple transformations have been reviewed. In this technique, the image watermarking has been developed based on the combination of different transformations in the direction to provide more robustness. There are different methodologies which are fully described here. A blind DWT-DFT image watermarking technique has been proposed which can provide enough robust against JPEG compression and affine transformation but, the lack of robustness against filtering, the median is the main limitation of this approach. Another approach proposed based on DCT-DWT for image authentication where compression is taken place. This image authentication has applied temper detection in the special part of the image which can provide soft authenticator as well as chrominance. The other watermarking technique is developed by the combination of DCT and SVD. In this approach, Local Peak Signal-to-Noise Ratio (LPSNR) has been applied to robust the watermark against Stir Mark 4.0 attack.

Same DCT and SVD image watermarking technique are developed in order to improve the robustness against different signals processing manipulation such as noise, JPEG compression, median filter, low pass filter and contrast enhancement. Recently, the combination of DWT and SVD is also proposed for authenticity and copyright protection of digital images. The main advantage of this method is that information cannot be extracted without the original image. Also, LWT-SVD robust image watermarking approach has been developed. Although this approach can provide enough robustness against geometrical attacks, it cannot provide enough invisibility.

Multiplication: Multiplication watermarking techniques are widely used for media watermarking. Basically, multiplication can be embedded in both special domain and transformed domains. Also, it is very common for image watermarking due to simplicity during embedding and extraction. A few approaches have been developed for image based on multiplication. This is due to mathematical difficulty in the threshold for watermark extraction. In Akhaee *et al*. (2009), image watermarking technique has been developed base on scaling. The watermark is adapted somehow it cannot see by HVS. For extraction, Maximum-likelihood (ML) technique is applied which is mathematically computed. Not only this technique can provide robustness but also, it can provide enough imperceptibility. Another approach has been developed based on statistical modeling of multiplication a constant in contourlet transform of the image (Akhaee *et al*., 2010). Since the watermark is embedded in the edge of the image, the watermark is embedded by more robustness which can provide less BER in respect to AWGN, JPEG and filtering attacks. Furthermore, ML optimum detector and decision threshold are mathematically developed in order to reduce the BER at the receiver side. In Xiang *et al*. (2008), image watermarking technique is developed based on statistical modeling of the image histogram means and shape. This technique has provided good robustness against translation, scaling, cropping, random bending and rotation attacks.

Challenges in digital image watermarking: Digital Image watermarking is a trade-off between robustness, impermeability Invisibility and capacity. Depending on the applications, some techniques focus on robustness. However, other applications emphasize imperceptibility and invisibility. In many applications, the irrelevant visual segments of the image are attempted to be removed. This removal is a basic challenge for image watermarking algorithm so as to preserve its robustness. Watermarking should occur in perceptually every relevant image part. However, the limitation in the number of visually relevant segments is another concern for watermarking. In some applications, the capacity becomes more important to achieve. Furthermore, the capacity of image watermarking is reduced as compared to that of audio due to the fewer samples. For example, every second of audio file has 4, 4100 sample which is reduced to 100×100 = 10,000 for the image. This embedding capacity can be further reduced when image compression techniques are applied.

Table 4 shows deep concentration on recent biometric watermarking approaches in terms of blindness, capacity and watermarking domain. Furthermore, the applied biometric for watermarking have been presented. As seen, there is no any blind watermarking technique which can provide the large capacity. Also, the majority of these efforts has been done in the wavelet domain.

Table 5 summarizes the evaluation of the performance of each watermarking technique in terms of robustness, imperceptibility invisibility and capacity. As seen, none of them is ideal due to the nature of watermarking which is a tradeoff among these criteria. Whenever a criterion is an increase, other

Table 4: Comparison among various biometric watermarking techniques

Ref	Wm method	Type of biometric WM	Blindness	Capacity
Ratha *et al*. (2000)	Spatial	Fingerprint+Eigenface	Blind	Small
Vatsa *et al*. (2004)	DCT	Iris binary code	Blind	Small
Qi *et al*. (2010)	Correlation analysis	Palm	None-blind	Large
Vatsa *et al*. (2009)	RDWT	Voice	Semi-blind	Large
Fouad *et al*. (2010)	LSB+DWT	Iris	Blind	Small
Khan *et al*. (2007)	DFT	Fingerprint	Blind	Small
Park *et al*. (2007)	DFT	Iris	Blind	Small
Noore *et al*. (2007)	Wavelet	Face	Blind	Small

Table 5: Comparison of related image and video watermarking methods

WM Method	Capacity (No of WM Bits)	Robustness (BER) %	Imperceptibility (PSNR)	Blindness
Image watermarking methods	25	0.003	48.34	Semi
Histogram (Zong *et al*., 2015)				
Spatial domain (Cheung, 2000)	256	0.002	47.54	None-blind
DWT-DCT-SVD (Navas *et al*., 2008)	256	0.001	113.42	Semi
DWT-DFT phase (Kang *et al*., 2003)	256	0.050	76.11	Blind
DFT (Li *et al*., 2009)	256	0.260	60.52	Blind
SVD (Ghazy *et al*., 2015)	256	0.001	73.65	Blind
DWT (Lin *et al*., 2008)	64	0	44.25	Blind
DWT (Ma *et al*., 2014)	512	0	48.07	Blind
RDWT (Agarwal *et al*., 2014)	4096	0.35	41.53	Blind
Alternative video watermarking methods				
DCT (Wang and Alan, 2006)	256	0.004	60.24	Semi
Wavelet Packet (Bhatnagar and Raman, 2012)	6336	0.001	64.87	Blind
Ridgelet (Khalilian *et al*., 2009)	2304	0.03	44	Blind
DWT+NN (Li and Wang, 2007)	2304	0.02	39.08	Blind
DWT+spatial (Huai-Yu *et al*., 2004)	2304	0.05	N/A	Blind
DWT (Huai-Yu *et al*., 2004)	2304	0.11	40.07	Blind
DWT (Yassin *et al*., 2014)	2304	0.15	38.95	Semi
DWT+QIM (Yassin *et al*., 2014)	1024	0.02	45.25	Blind

criteria are decreased. Although the result of the proposed watermarking systems seems to be good, they are still reported under their assumption. In real environment condition, there is still a huge gap to use an efficient watermarking technique to embed the voice feature in the digital image.

CONCLUSION

Face and voice recognition systems are closely related to biomedical science. Prior technology in biometric only relied on one biometric. However, there are many vulnerable slots in single biometric systems security. Although cryptography can be successfully applied for encrypting the biometric template, it needs huge computational complexity. Moreover, it has provided limited protection against channel attacks. However, digital watermarking as a solution not only can enhance the security of the digital media like the image but also, it can embed the biometric feature in a biometric data which is know as biometric watermarking. With ever-growing of the PC and smartphone, it seems face and voices are two main parts of any digital systems. Therefore, studies on multimodal biometric watermarking based on voice and face are going to be a hot topic in biometric systems. Although there is a few studies have been conducted, some issues such as blindness, capacity, robustness and improving recognition performance are still remained as the different contribution for whom would like to work actively in this area.

In this chapter, various faces, voice, multimodal biometric and digital image watermarking techniques have been reviewed. The advantages and disadvantages of each technique are fully described. Basically, this chapter discussed the problems and foundation of the research on multimodal biometric watermarking has been constructed.

REFERENCES

Agarwal, H., B. Raman and I. Venkat, 2014. Blind reliable invisible watermarking method in wavelet domain for face image watermark. Multimed. Tools Appl., 74(17): 6897-6935.

Akhaee, M.A., S.M.E. Sahraeian, B. Sankur and F. Marvasti, 2009. Robust scaling-based image watermarking using maximum-likelihood decoder with optimum strength factor. IEEE T. Multimedia, 11(5): 822-833.

Akhaee, M.A., S.M.E. Sahraeian and F. Marvasti, 2010. Contourlet-based image watermarking using optimum detector in a noisy environment. IEEE T. Image Process., 19(4): 967-980.

Arya, M.S. and R. Siddavatam, 2013. Geometric robust multimodal biometric watermarking scheme for copyright protection of digital images. Int. J. Comput. Appl., 72(9): 40-52.

Bhatnagar, G. and B. Raman, 2012. Wavelet packet transform-based robust video watermarking technique. Sadhana, 37(3): 371-388.

Bimbot, F., J.F. Bonastre, C. Fredouille, G. Gravier, I. Magrin-Chagnolleau, S. Meignier, T. Merlin, J. Ortega-García, D. Petrovska-Delacrétaz and D.A. Reynolds, 2004. A tutorial on text-independent speaker verification. EURASIP J. Appl. Si. Pr., 2004: 430-451.

Chaudhary, S. and R. Nath, 2015. A new multimodal biometric recognition system integrating iris, face and voice. Int. J. Adv. Res. Comput. Sci. Softw. Eng., 5(4): 145-150.

Cheung, W.N., 2000. Digital image watermarking in spatial and transform domains. Proceeding of the IEEE TENCON 2000.

Do, M.N. and M. Vetterli, 2005. The contourlet transform: An efficient directional multiresolution image representation. IEEE T. Image Process., 14(12): 2091-2106.

Fan, L. and F. Yanmei, 2006. A DWT-based video watermarking algorithm applying DS-CDMA. Proceeding of the IEEE Region 10th Conference TENCON 2006. Hong Kong, pp: 1-4.

Fazel, A. and S. Chakrabartty, 2011. An overview of statistical pattern recognition techniques for speaker verification. IEEE Circuit. Syst. Mag., 11(2): 62-81.

Fouad, M., A. El Saddik and E. Petriu, 2010. Combining DWT and LSB watermarking to secure revocable iris templates. Proceeding of the IEEE 10th International Conference on Information Sciences Signal Processing and their Applications (ISSPA, 2010). Kuala Lumpur, pp: 25-28.

Galton, F., 1889. Personal identification and description. J. Anthropol. Inst. Great Britain Ireland, 18: 177-191.

Ghazy, R.A., A.M. Abbas, N. Al-Zubi, E.S. Hassan, N.A. El-Fishawy, M.M. Hadhoud, M.I. Dessouky, E.S.M. El-Rabaie, S.A. Alshebeili and F.E. Abd El-Samie, 2015. Block-based SVD image watermarking in spatial and transform domains. Int. J. Electron., 102(7): 1091-1113.

Ghouzali, S., 2015. Watermarking Based Multi-biometric Fusion Approach. In: El Hajji, S. *et al*. (Eds.), Codes, Cryptology, and Information Security. Lecture Notes in Computer Science, Springer International Publishing, Switzerland, 9084: 342-351.

Huai-Yu, Z., L. Ying and W. Cheng-Ke, 2004. A blind spatial-temporal algorithm based on 3D wavelet for video watermarking. Proceeding of the IEEE International Conference on Multimedia and Expo (ICME'04), 3: 1727-1730.

Inamdar, V.S. and P.P. Rege, 2014. Dual watermarking technique with multiple biometric watermarks. Sadhana, 39(1): 3-26.

Kalra, S. and A. Lamba, 2014. A survey on multimodal biometric. Int. J. Comput. Sci. Inf. Technol., 5(2): 2148-2151.

Kang, X., J. Huang, Y.Q. Shi and Y. Lin, 2003. A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression. IEEE T. Circ. Syst. Vid., 13(8): 776-786.

Khalilian, H., S. Ghaemmaghami and M. Omidyeganeh, 2009. Digital video watermarking in 3-D ridgelet domain. Proceeding of the 11th International Conference on Advanced Communication Technology (ICACT, 2009). Phoenix Park, 3: 1643-1646.

Khan, M.K., L. Xie and J. Zhang, 2007. Robust Hiding of Fingerprint-biometric Data into Audio Signals. In: Lee, S.W. and S.Z. Li (Eds.), Advances in Biometrics. Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, 4642: 702-712.

Li, J., X. Zhang, S. Liu and X. Ren, 2009. An adaptive secure watermarking scheme for images in spatial domain using fresnel transform. Proceeding of the 1st International Conference on Information Science and Engineering (ICISE, 2009). Nanjing, pp: 1630-1633.

Li, X. and R. Wang, 2007. A video watermarking scheme based on 3D-DWT and neural network. Proceeding of the 9th IEEE International Symposium on Multimedia Workshops (ISMW'07). Taichung, Taiwan, pp: 110-115.

Lin, W.H., S.J. Horng, T.W. Kao, P. Fan, C.L. Lee and Y. Pan, 2008. An efficient watermarking method based on significant difference of wavelet coefficient quantization. IEEE T. Multimedia, 10(5): 746-757.

Ma, B., Y. Wang, C. Li, Z. Zhang and D. Huang, 2014. Secure multimodal biometric authentication with wavelet quantization based fingerprint watermarking. Multimed. Tools Appl., 72(1): 637-666.

Ma, J. and G. Plonka, 2010. A review of curvelets and recent applications. IEEE Signal Proc. Mag., 27(2): 118-133.

Mallat, S.G., 1989. A theory for multiresolution signal decomposition: the wavelet representation. IEEE T. Pattern Anal., 11(7): 674-693.

Mat Kiah, M., B.B. Zaidan, A.A. Zaidan, A. Mohammed Ahmed and S.H. Al-Bakri, 2011. A review of audio based steganography and digital watermarking. Int. J. Phys. Sci., 6(16): 3837-3850.

Mohan, B.C. and S.S. Kumar, 2008. Robust digital watermarking scheme using contourlet transform. IJCSNS Int. J. Comput. Sci. Netw. Secur., 8(2): 43-51.

Narasimhulu, C.V. and K.S. Prasad, 2010. A hybrid watermarking scheme using contourlet Transform and Singular value decomposition. IJCSNS Int. J. Comput. Sci. Netw. Secur., 10(9): 12-17.

Navas, K.A., M.C. Ajay, M. Lekshmi, T.S. Archana and M. Sasikumar, 2008. DWT-DCT-SVD based watermarking. Proceeding of the 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE, 2008). Bangalore, pp: 271-274.

Noore, A., R. Singh, M. Vatsa and M.M. Houck, 2007. Enhancing security of fingerprints through contextual biometric watermarking. Forensic Sci. Int., 169(2-3): 188-194.

Park, K.R., D.S. Jeong, B.J. Kang and E.C. Lee, 2007. A Study on Iris Feature Watermarking on Face Data. In: Beliczynski, B. *et al*. (Eds.), Adaptive and Natural Computing Algorithms. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 4432: 415-423.

Po, D.D. and M.N. Do, 2006. Directional multiscale modeling of images using the contourlet transform. IEEE T. Image Process., 15(6): 1610-1620.

Qi, M., Y. Lu, N. Du, Y. Zhang, C. Wang and J. Kong, 2010. A novel image hiding approach based on correlation analysis for secure multimodal biometrics. J. Netw. Comput. Appl., 33(3): 247-257.

Ratha, N.K., J.H. Connell and R.M. Bolle, 2000. Secure data hiding in wavelet compressed fingerprint images. Proceeding of the ACM Workshops on Multimedia, pp: 127-130.

Rec, I., 1996. P.800: Methods for Subjective Determination of Transmission Quality. International Telecommunication Union, Geneva.

Soltane, M., N. Doghmane and N. Guersi, 2010. Face and speech based multi-modal biometric authentication. Int. J. Adv. Sci. Technol., 21(6): 41-56.

SPEECHPRO, 2015. Voice Key One Pass: Unique Multi-Model (Voice+Face) Biometric Authentication. Retrieved from: http://speechpro-usa.com/.

Vatsa, M., R. Singh, P. Mitra and A. Noore, 2004. Comparing robustness of watermarking algorithms on biometrics data. Proceeding of the Workshop on Biometric Challenges from Theory to Practice-ICPR Workshop, pp: 5-8.

Vatsa, M., R. Singh, A. Noore, M.M. Houck and K. Morris, 2006. Robust biometric image watermarking for fingerprint and face template protection. IEICE Electron. Expr., 3(2): 23-28.

Vatsa, M., R. Singh and A. Noore, 2009. Feature based RDWT watermarking for multimodal biometric system. Image Vision Comput., 27(3): 293-304.

Wang, S., R. Hu, H. Yu, X. Zheng and R. Damper, 2013. Augmenting remote multimodal person verification by embedding voice characteristics into face images. Proceeding of the IEEE International Conference on Multimedia and Expo Workshops (ICMEW, 2013), San Jose, CA, pp: 1-6.

Wang, Y. and P. Alan, 2006. Blind MPEG-2 video watermarking in DCT domain robust against scaling. IEE P-Vis. Image Sign., 153(5): 581-588.

Xiang, S., H.J. Kim and J. Huang, 2008. Invariant image watermarking based on statistical features in the low-frequency domain. IEEE T. Circ. Syst. Vid., 18(6): 777-790.

Yassin, N.I., N.M. Salem and M.I. El Adawy, 2014. QIM blind video watermarking scheme based on Wavelet transform and principal component analysis. Alexandria Eng. J., 53(4): 833-842.

Zeng, W. and B. Liu, 1999. A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images. IEEE T. Image Process., 8(11): 1534-1548.

Zong, T., Y. Xiang, I. Natgunanathan, S. Guo, W. Zhou and G. Beliakov, 2015. Robust histogram shape-based method for image watermarking. IEEE T. Circ. Syst. Vid., 25(5): 717-729.