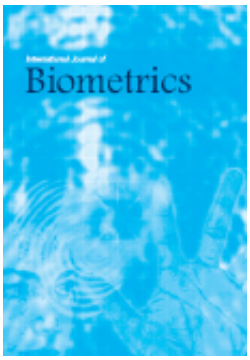


International Journal of Biometrics

ISSN online: 1755-831X - ISSN print: 1755-8301
https://www.inderscience.com/ijbm

Robust perceptual fingerprint image hashing: a comparative study

Wafa Birouk, Atidel Lahoulou, Ali Melit, Ahmed Bouridane

DOI: 10.1504/IJBM.2023.10051692

Article History:

Received:	03 December 2020
Last revised:	16 July 2021
Accepted:	14 September 2021
Published online:	15 December 2022

Robust perceptual fingerprint image hashing: a comparative study

Wafa Birouk*

Computer Science Department,
Faculty of Exact Sciences,
University of Bejaia,
06000, Bejaia, Algeria
Email: brk.wafa@gmail.com
*Corresponding author

Atidel Lahoulou and Ali Melit

Computer Science Department,
University Mohammed Seddik Benyahia,
18000, Jijel, Algeria
Email: atidel.lahoulou@gmail.com
Email: ali_melit@yahoo.fr

Ahmed Bouridane

Cybersecurity and Data Analytics Research Center,
University of Sharjah,
Sharjah, UAE
Email: abouridane@sharjah.ac.ae

Abstract: This paper presents a robust perceptual hashing scheme for biometric template protection where the input fingerprint image is mapped into a sequence of Boolean values. Our aim is to develop a method that relies on the use of four functions namely SIFT, Harris, DWT and SVD. After extracting the minutiae, the scale-invariant feature transform (SIFT) is applied in order to extract the robust features against geometric attacks. The resulting vector is then filtered using Harris criterion to maintain only the stable key-points. Next, the fingerprint template is produced by image binarisation and decomposed into blocks. The hash code is finally obtained by concatenating the singular values computed on the approximation coefficients of each image block. Similarity between hash codes is evaluated by the normalised Hamming distance (HD). Comparative analysis to three similar methods indicates that the proposed hashing scheme shows better performances in terms of discriminative capability as well as robustness against acceptable image manipulations, such as JPEG compression, gamma correction, speckle noise, Gaussian blur, shearing and slight rotation.

Keywords: fingerprint image; perceptual hashing; minutiae extraction; scale-invariant feature transform; SIFT; Harris; singular value decomposition; SVD; discrete wavelet transform; DWT; acceptable attacks.

Reference to this paper should be made as follows: Birouk, W., Lahoulou, A., Melit, A. and Bouridane, A. (2023) 'Robust perceptual fingerprint image hashing: a comparative study', *Int. J. Biometrics*, Vol. 15, No. 1, pp.59–77.

Biographical notes: Wafa Birouk his received Engineering and Master degrees in Computer Science at the University of Jijel, Algeria in 2005 and at the University of Bejaia, Bejaia, Algeria in 2010, respectively. She is currently a faculty member in the Department of Computer Science at the University of Jijel, Algeria and working toward his PhD in the Department of Computer Science at the University of Bejaia, Algeria. Her research interests include Biometric Security and privacy, perceptual hashing, image processing and protection.

Atidel Lahoulou is a faculty member in the Department of Computer Science at the University of Jijel, Algeria, with over 20 years of experience in academia. She earned her Doctor in Signals and Images from the Sorbonne Paris Nord, France since 2012 and her Habilitation Universitaire in 2017. She led a new masters program in Algeria on computer and multimedia forensics and is leading a research team on intelligent multimedia data processing. Her research interests include quality of experience, biometrics, machine learning and cybersecurity.

Ali Melit is currently a Professor at the Department of Computer Science at the University of Jijel, Algeria. He obtained his doctoral thesis in computer science at the University of Pierre and Marie curie, Paris 6 French. His research areas are: computer systems modelling and performance, queuing theory, optimisation and simulation, wireless networks and biometrics.

Ahmed Bouridane received his MEng in 1982 from Algiers, MPhil in 1988 from Newcastle and PhD in 1992 from Nottingham. He is a Professor of Machine Intelligence and the Director of Center for Data Analytics and Cybersecurity at the University of Sharjah, UAE. His research interests are in machine learning with applications to cybersecurity, imaging for forensics and security, quantitative pathology and bi-medical engineering, homeland security and video analytics; and video steganography and steganalysis. He has authored and co-authored more than 350 publications as well as two research books on imaging for forensics and security and on biometric security and privacy. He is a senior member of IEEE.

1 Introduction

Biometric systems aim at identifying and authenticating individuals in a reliable and fast way through the use of unique morphological characteristics (such as fingerprints, iris, face, etc.) and/or behavioural characteristics (such as voice, signature, etc.). From the early days, when identity protection was the driving force behind biometric research, challenges concerning security of biometric data have been raised.

Among existing biometric systems, fingerprint templates are the oldest and form the most widely deployed modality. The minutiae are the local characteristic points that depict fingerprint data. They are unique for each individual and permanent as the biometric traits are invariant over time. The extraction of these minutiae goes through several steps. Typically, it starts with a pre-processing step in order to improve the

quality of the fingerprint image, then an estimation of orientation field, fingerprint segmentation, image binarisation, ridge thinning, minutiae extraction and ends with a post-processing stage consisting of filtering the extracted points by retaining only the relevant minutiae key-points. Ridge endings and ridge bifurcations are typical minutiae key-points; they are the mostly considered amongst other types of data.

Although biometric fingerprint systems have been able to improve the security of traditional recognition systems, they are not entirely secure because the integrity of fingerprint data in databases is vulnerable to several types of unintentional (e.g., signal processing, etc.) and malicious attacks which may result in a decrease in the overall performances of the biometric-based systems when identifying and/or authenticating individuals. For this reason, several solutions have been proposed to protect the fingerprint minutiae template against attacks. Indeed, Mirmohamadsadeghi and Drygajlo (2013) introduced a template privacy protection technique that provides diversity, revocability, and irreversibility for the minutiae cylinder code (MCC) descriptors that represent the fingerprint minutiae template. Cappelli et al. (2010), Ferrara et al. (2012, 2014) and Liu and Zhao (2017) also proposed the use of MCC attributes to improve the accuracy of fingerprint recognition and reduce the size of the template. The authors used the minutiae positions to build a secure template, such as the location of each minutia is modified using its neighbouring minutiae and a set of keys (Ali et al., 2018). The technique is proven to be secure by testing on different attacks and robust as it takes into account the problem of rotation and translation that may occur during the fingerprints capture. Another family of solutions is based on biometric cryptosystems where the fuzzy vault and fuzzy commitment schemes (Nagar et al., 2008; Nandakumar, 2010) have been integrated to fingerprint template protection.

In some works, cancellable biometrics has gained a lot of interest for the protection of fingerprint minutiae (Lee and Kim, 2010; Wang et al., 2017b; Sandhya and Prasad, 2015; Wang and Hu, 2016; Jin et al., 2014; Wang et al., 2017a). In this approach, the original biometric is not stored but is transformed scheme using a one-way function. The transformation can be operated either in the original domain (the fingerprint image) or in the feature domain (the minutiae). The use of watermarking as a technique to hide information in the image was one of the proposed solutions to secure the fingerprint template as in Chouhan and Khanna (2011).

More recently, perceptual hash functions have been employed for securing fingerprint data against various attacks. These functions require four fundamental properties (Mihçak and Venkatesan, 2001); namely: randomisation, independence of perceptually different images, invariance of perceptually similar images and discrimination of perceptually different images. It remains challenging to have a trade-off between the robustness and discriminative capabilities of a method based on perceptual hash.

In this paper, we introduce a robust and discriminative hash model for integrity protection of fingerprint templates saved in the database. Since it is now possible to recover the original fingerprint image from the coordinates of the minutiae (Ali et al., 2018), our model belongs to the class where the hashing function is not directly applied on the minutiae points but on a vector of statistical features extracted from the fingerprint template. The proposed scheme is more secure and consists of generating a fingerprint image hash code that satisfies the robustness and discrimination criteria based on SIFT and Harris functions for the feature extraction/selection phase and on DWT and SVD functions for the hash code generation phase.

Our contribution consists in a two-fold filtering of the fingerprint key features computed using the SIFT technique. The first filter discards the SIFT features that are too distant from the minutiae points using the Euclidian distance as similarity distance measure. This generates a vector of SIFT key-points that are robust against some geometric transformations such as shearing and rotation. The generated subset of features is filtered again using the Harris function in order to keep only the stable key-points that are robust against a set of acceptable attacks such as encoding, luminance changes, noise and blurring.

The remainder of this paper is organised as follows: a description of the fingerprint hash methods that have been proposed in the literature is presented in Section 2. Section 3 presents our hash method setup and Section 4 gives the experimental results obtained after tests and validation over specialised database. The performances of the proposed method are benchmarked and compared to a set of perceptual hashing methods in the literature, in Section 5 followed by some concluding remarks.

2 Related work

The first class of hashing methods relies on randomisation technique to build robust perceptual hash codes since randomness somehow increases the level of security. To this end, Li et al. (2012) used random Gabor filtering and dithered lattice vector quantisation (LVQ) for image hash construction. It has been observed that the use of random Gabor filter for features extraction improves the robustness of features against rotation manipulation. Similarly, using LVQ as a quantifier improves discrimination level as well as robustness against several acceptable manipulations such as JPEG compression and median filtering. Yuling et al. (2016) presented an image hashing method based on Radon transform and invariant features to generate a hash by combining both local features, based on the invariant moments, and global features. The proposed method performs well for images discrimination and is robust against JPEG compression, filtering, noise contamination, scaling, translation and rotation.

Zhao et al. (2013) also used local and global characteristics for the construction of their hash. Local features include position and texture information of salient regions, while the overall features represent the luminance and chrominance characteristics of the image and are based on Zernike moments. Experimental results demonstrate that the generated hash is robust against the content-preserving attacks and shows good discriminative capabilities. The improvement of the technique proposed in Zhao et al. (2013) has led to the implementation of a new perceptual image hashing method that has been introduced by Ouyang et al. (2016) using quaternion Zernike moments (QZMs). Their method gives a short and robust hash code against content-preserving attacks.

Other researchers define another class of image hashing schemes where the features extraction step is given higher importance in the whole process. For example, in Lv and Wang (2012) proposed to take advantage of the scale-invariant feature transform (SIFT) detector since this transform is robust against geometrical transformations. They combine it with the Harris function in order to generate only stable key-points against the manipulations, given that the Harris criterion improves the robustness of SIFT features against attacks such as the additive noise and blurring. On the other hand, they used the shape context technique to calculate the perceptual hash code. The image hashing method proposed in Lv and Wang (2012) has proven its robustness against rotation, cropping,

shearing, and Gamma correction. It is, however, sensitive to additive noise, blurring, JPEG compression and scaling. Ouyang et al. (2017) implemented an image hashing algorithm based on SIFT and QZMs introduced in Ouyang et al. (2016). The hash of the proposed method is short but is, at the same time, robust against content-preserving operations like JPEG compression, wide angles rotation, average filtering, median filtering and motion blurring.

Image frequency-domain transforms such as singular value decomposition (SVD) and discrete wavelet transform (DWT) have also been incorporated into some image hashing schemes. Neelima and Singh (2016) suggested a new image hashing method based on SIFT and SVD, where SIFT function is first applied to the entire image. After that, the image is decomposed into blocks and the key-points resulting from SIFT are subjected to a SVD decomposition. Here, the maximum singular values of the blocks are concatenated to generate the final hash. This method has been found to be robust against JPEG compression, Gaussian low-pass filtering, rotation combined with cropping, scaling and Gamma correction but it is not resilient to rotation when it is the only attack. Hernandez et al. (2011) proposed the use of the input image normalisation technique and SVD decomposition to construct the perceptual hash of the images. Their results show that the image normalisation technique based on invariant moments and used as a pre-processing step, as well as the double decomposition by singular values (SVD) in the hash construction increases its robustness against the content-preserving operations such as rotation, JPEG compression and scaling.

In the case of the use of DWT in image hashing, methods have been proposed in Govindaraj and Sandeep (2015) and Karsh et al. (2017). Govindaraj and Sandeep (2015) generated the hash by using ring partition and DWT. Their method is robust against content-preserving operations like rotation, Gamma correction, JPEG compression, scaling, Gaussian low-pass filtering and brightness adjustment. Karsh et al. (2017) used DWT-SVD and spectral residual model to obtain an image hash robust to rotation, scaling, Gamma correction, JPEG compression, brightness adjustment and contrast adjustment.

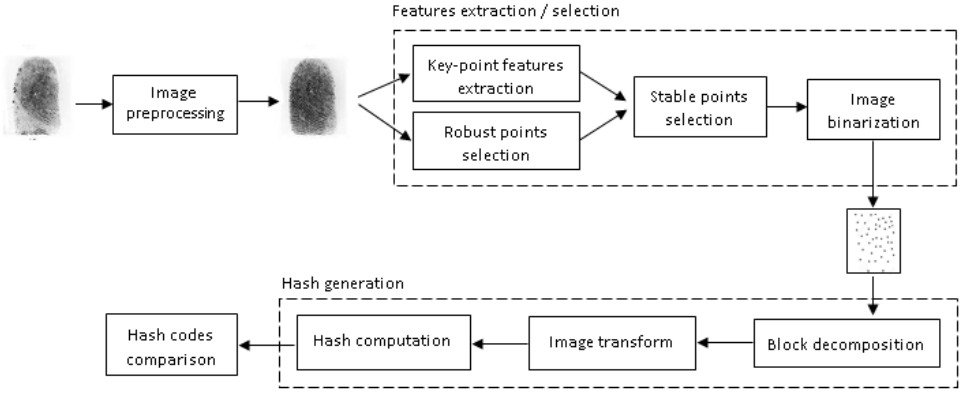
The perceptual hashing methods discussed in Li et al. (2012), Yuling et al. (2016), Zhao et al. (2013), Ouyang et al. (2016), Lv and Wang (2012), Ouyang et al. (2017), Neelima and Singh (2016), Hernandez et al. (2011), Govindaraj and Sandeep (2015) and Karsh et al. (2017) are all implemented and tested on natural images. Nevertheless, in the context of protecting the integrity of fingerprint images which is the scope of the present work, a few works have been done. The protection of the minutiae-based fingerprint templates through the perceptual hashing has received great attention in biometric research. Jin et al. (2009) described random triangle hashing method to protect the minutiae template. The constructed hash is robust against minor translation and rotation attacks as all the minutiae are translated into a pre-defined space based on a reference minutia. The equal error rate (EER) for authentication applications is minimised and the hash conveys only information about the number of minutiae contained in each triangle as well as their orientations. In Yang et al. (2010), the authors generated a secure hash for fingerprint template protection that is based on the minutiae vicinity. Each minutia key-point is firstly subjected to a geometric alignment. Afterwards, a randomisation technique is applied to the aligned points in order to increase the security of the hash. Das et al. (2012) proposed a new secure fingerprint hashing method based on minimum distance graph (MDG) built from a core point and a set of minutiae. This method is robust to rotation and translation during the authentication procedure.

More recently, some researchers have exploited the potential of shape context-based models in securing fingerprint minutiae. For example, Muthu et al. (2014) proposed a fingerprint hashing method that is robust against different manipulations; where the idea consists in combining the minutiae with the characteristic points selected by SIFT-Harris to have only the robust and stable minutiae of the fingerprint image. Afterwards, the geometric distribution of the key-points is integrated in shape context as in Lv and Wang (2012) to construct the hash. The proposed method has a good robustness against translation, Gaussian blur, JPEG compression, median filtering and rotation. Abdullahi et al. (2018) described a new fingerprint hashing method that integrates the minutiae orientations as well as their descriptors in a shape context model, in order to generate a robust and compact hash. The proposed scheme has proven its robustness against noise addition, blurring and geometric distribution, as well as its higher discriminative capabilities when compared to existing methods.

3 The proposed perceptual hashing method for fingerprint images

The structure of the proposed hashing method for fingerprint images is depicted in Figure 1. The system consists of a three-phase procedure and the steps are presented in the next subsections.

Figure 1 Diagram of our proposed robust fingerprint image perceptual hashing



3.1 Image pre-processing

A fingerprint image is first pre-processed using a median filter without normalisation of the image. This step is useful in reducing random noise and thus enhancing the visual quality of the input data which implies improving the results of later processing.

3.2 Features extraction

The accuracy of this step is fundamental for the whole system performance. It is divided into four major stages:

- *Key-point features extraction:* On the one hand, a vector of feature points is extracted using the SIFT algorithm (Lowe, 2004) which is known to be robust against some geometric transformations such as translation, rotation, scaling. On the other hand, the fingerprint minutiae are extracted from the image using the methods in Kaur et al. (2008).
- *Robust points selection:* Further, the Euclidean distance d is used as similarity measure between the two types of features – SIFT point-based and minutia-based – to select robust statistical features.
- *Stable points selection:* Given the geometric invariance of the SIFT key-point features extracted earlier, the Harris-corner-points method (Harris and Stephens, 1988) is applied in order to select a subset of key-points that are more stable against acceptable image distortions arising from additive noise, blurring and compression (Lv and Wang, 2012). SIFT-Harris points are selected using the threshold *Th* given in the formula below (Lv and Wang, 2012):

$$Th = \frac{\alpha}{N} \sum_{i=1}^{N} H_i^{\sigma}(x, y) \tag{1}$$

  where N is the total number of SIFT points of the previous stage, α whose values belong to the [0.1, 0.5] interval is a tuning parameter to adjust the robustness of extracted points, σ is the standard deviation of the Gaussian kernel window used to compute the autocorrelation matrix (Lv and Wang, 2012), and H is the Harris function for the (x, y) SIFT key-point spatial coordinates. Each robust point is considered to be also stable if their Harris criterion is above the threshold *Th*, otherwise it is discarded.
- *Image binarisation:* Given the vector of SIFT-Harris features, the fingerprint image I is transformed into a binary image I_b such as Neelima and Singh (2016):

$$I_b(i, j) = \begin{cases} 0 & \text{if pixel } I(i, j) \text{ is SIFT-Harris key-point} \\ 255 & \text{else} \end{cases} \tag{2}$$

3.3 Hash generation and comparison

The hash generation phase consists of four stages: block decomposition, image transform, hash computation and finally hash codes comparison.

- *Block decomposition:* Since the length of the generated hash value depends on the number of image blocks, we need to resize the input images to a standard size. Thus, the binary image (I_b) is beforehand padded to form a square array (I_b') of $N \times N$ pixels and then partitioned into q non-overlapping blocks B^k where $k = 1, 2, 3, \ldots, q$ (Neelima and Singh, 2016).
- *Image transform:* Since the image blocks contain only one type of information, which are the robust-stable feature points, we do not need to process the entire image information. We use only the approximation coefficients in the LL sub-bands of the blocks by applying the DWT. In this paper, we use a two-level decomposition of (Daubechies 2) wavelet. The LL coefficients are then selected for SVD in order to

get an optimal compact representation of the fingerprint key-points prior to hash generation.

- *Hash computation:* Our hash code is a q-bits string whose values are generated according to the maximum singular values of the blocks following the formula employed in Neelima and Singh (2016) below:

$$Hash_{(k)}(B^k) = \begin{cases} 1 & \text{if } Max(SV(B^k)) \geq avg \\ 0 & \text{else} \end{cases} \tag{3}$$

where $Max(SV(B^k))$ is the maximum singular value of the k^{th} block, avg is the average of all maximum singular values of all q blocks of the padded binary image $(I_b^{'})$ and $k = 1, 2, 3, \ldots, q$.

- *Hash codes comparison:* Two hash codes are compared using the Hamming distance (HD)-based similarity measure.

4 Experimental results

The proposed perceptual hashing method for fingerprint images is evaluated and validated over the FVC2002/DB1_A database Second International Competition for Fingerprint Verification Algorithms (2002) which comprises of 800 digital fingerprint images collected from 100 subjects. Each volunteer contributed with eight samples all enrolled with 500 dpi resolution using an optical sensor device. All images of the database are of size 388 × 374 pixels. For the implementation settings, all the tests have implemented with MATLAB 2013b, on a 2.10 GHz Intel Core i3-2310M laptop processor and 4.0 GB RAM.

The performance of our proposed hashing method depends on several parameters; namely the size of the test sample, the maximum Euclidean distance between minutiae and SIFT key-points and the size of image blocks. This yields to experimenting on multiple combinatorial configurations for different values of the setup parameters as shown in Table 1.

As explained in Section 3, the first step of our method is to apply a median filter to the input image in order to enhance its quality. Afterwards, two vectors of features are extracted related to minutia-based and SIFT-based key-points, respectively. Then the SIFT descriptors' vector is filtered with respect to the minutiae; where only the closest SIFT key-points to the minutiae are selected. The point-wise matching is based on the Euclidean distance d as similarity measure. Here, we have tested three different values of Euclidean distance $d = 15, 30, 45$.

The generated subset containing the fingerprint image features, which robust to geometric transformations, is once again filtered by the Harris-corner-based method to get descriptors that are also resilient against additive noise, blurring and compression. The input image is then binarised according to the spatial coordinates of the SIFT-Harris key-points. Here, pixels corresponding to feature-points are assigned a value one and all other pixels are assigned a value zero.

At this stage, the block-based approach is followed. Hence, the black-white image is padded to a square array and decomposed into non-overlapping blocks. The DWT and SVD are then applied on each block to generate the hash code whose length equals the

number of blocks. Indeed, choosing a small block size increases the hash length and vice versa. We have tested four different block sizes as can be seen in Table 1.

After experimenting on the different configurations, the parameters' values (104, 15 and 32 × 32) in Table 1 have been found to give good trade-off for the system overall performances. Hence, the maximum Euclidean distance d between the extracted minutiae and the SIFT descriptors is set to $d = 15$. The blocks size is set to 32 × 32 and the sample of 104 images corresponding to the fingerprints of 13 randomly selected subjects has been retained. For this configuration, the binary images of 388 × 374 pixels are padded to 416 × 384 pixels and decomposed into (13 × 12 blocks) which implies that the length of our hash code is 156 bits.

Table 1 Different tested values of setup parameters

Setup parameters	*Tested values*			
Sample size	80 (10 subjects)		104 (13 subjects)	
Euclidean distance (*d*)	15	30		45
Blocks' size	16 × 16	*32 × 32*	46 × 46	56 × 56

In the following subsections, we will be interested in evaluating the performances of our method in terms of perceptual robustness and discriminative capabilities of the generated hash code.

4.1 Perceptual robustness

In order to analyse the perceptual robustness of our hashing method, we have randomly selected 13 subjects each having eight fingerprint sample images from the FVC2002DB1_A database. We have applied nine different attacks on the 104 images as summarised in Table 2. The attacks are JPEG compression, Gamma correction, additive noise (Gaussian noise, salt and pepper noise and speckle noise), blurring attacks (Gaussian and motion blur) and geometric attacks (shearing and rotation). In our simulations, rotation attacks have been divided into two groups: rotation_1 and rotation_2 with different ranges of angle degrees as shown in Table 2. For each distortion, we have provided the parameters we have manipulated as well as their levels and the number of generated versions of distorted images. Indeed, for each test image we have created 84 attacked copies that are intended to be perceptually similar to the original one.

The validation of the robustness performance of our method starts by computing the hash code for both the original fingerprint image and its attacked versions, for each distortion type and distortion level. Then, the normalised HD is calculated between each pair of original/attacked images. The obtained results are illustrated in Figure 2, where the y-axis represents the mean value of the HDs of the pairs of images for each parameter value of the attack represented on the x-axis.

It can be seen from Figure 2 that the values of the mean HDs between original and attacked fingerprint images are quite reasonable except for the following distortions: Gaussian noise [Figure 2(c)], salt and pepper noise [Figure 2(d)] and rotation between ±15° and 90° angles [Figure 2(j)]. These results comfort with the principle of perceptual hashing that maps visually identical images to the same or similar hash codes.

Table 2 Applied distortions and parameters' values

Manipulation		*Parameter description*	*Parameter values*	*Number of versions*
Encoding	JPEG compression	Quality factor	10, 20, 30, 40, 50, 60, 70, 80, 90	9
Luminance changes	Gamma correction	Gamma (γ)	0.75, 0.9, 1.1, 1.25, 1.3	5
Additive noise	Gaussian noise	Variance (v)	0.001, 0.005, 0.010, 0.015, 0.020, 0.025, 0.030, 0.035	8
	Salt and pepper noise	Noise density	0.01, 0.02, 0.03, 0.04, 0.05, 0.06, 0.07, 0.08	8
	Speckle noise	Noise variance (N_v)	0.001, 0.002, 0.003, 0.004, 0.005, 0.006, 0.007, 0.008, 0.009, 0.01	10
Blurring	Gaussian blur	Standard deviation (σ)	0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, 5	10
		Window size (w_s)	$w_s = 3$	
	Motion blur	Length of motion in pixels (len)	$len \in (1, 2, 3)$	9
		Angle of the movement ($\theta°$)	$\theta \in (0°, 45°, 90°)$	
Geometric attacks	Shearing	Shearing angle ($\theta°$)	0.01, 0.03, 0.05, 0.07, 0.09	5
	Rotation_1	Rotation angle ($\theta°$)	±1, ±2, ±3, ±4, ±5	10
	Rotation_2	Rotation angle ($\theta°$)	±10, ±15, ±30, ±45, ±90	10
Total				*84*

In Table 3, we present the hash similarity statistics of the proposed hashing method under different distortion types. Here again, it can be easily underlined that Gaussian noise, salt and pepper and rotation_2 are not acceptable distortions for perceptual hashing as they induce noticeable visual changes on the fingerprint images and, consequently, significant variabilities in the hash codes.

In order to determine which of the aforementioned unacceptable distortions is/are the most annoying, we have carried out tests on the perceptual robustness of the proposed hashing method. We calculate the rate of true detection of similar images with different threshold values over all sets of attacked images (column a of Table 4) and then over subsets as described in Table 4 (columns b to d). We finally estimate the true detection of similar images over subset of images that undergo acceptable attacks (column e).

For all tested hash similarity thresholds θ [0.06, 0.20], our model performs better in terms of robustness against the above distortions for visually similar fingerprint images as highlighted in bold in Table 4. The acceptable attacks considered in case e are: JPEG compression, Gamma correction, speckle noise, Gaussian blur, motion blur, shearing and rotation between ±1° and ±5° angles.

Figure 2 Robustness performances under, (a) JPEG compression (b) Gamma correction (c) Gaussian noise (d) salt and pepper noise (e) speckle noise (f) Gaussian blur (g) motion blur (h) shearing (i) rotation_1 (j) rotation_2 (see online version for colours)

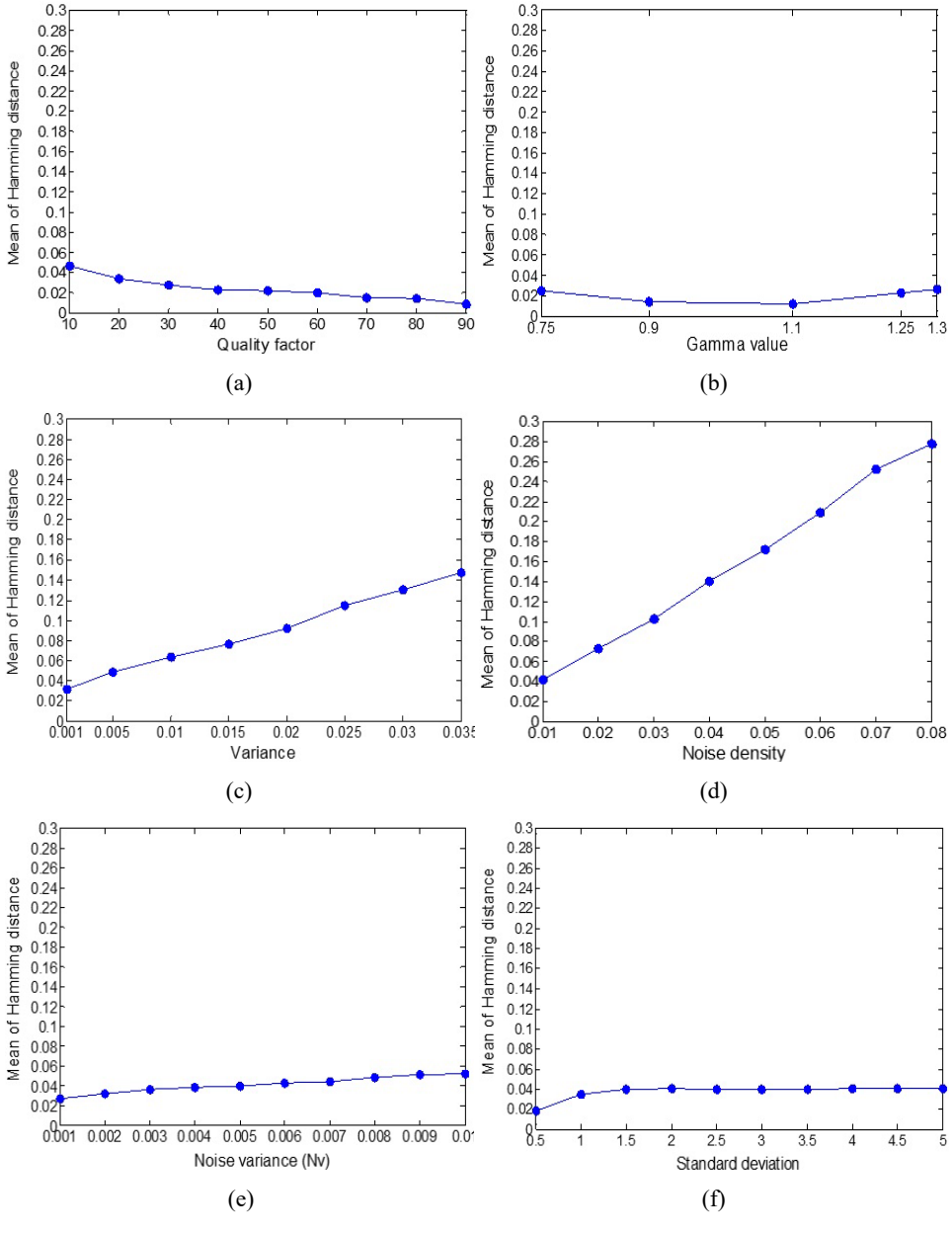
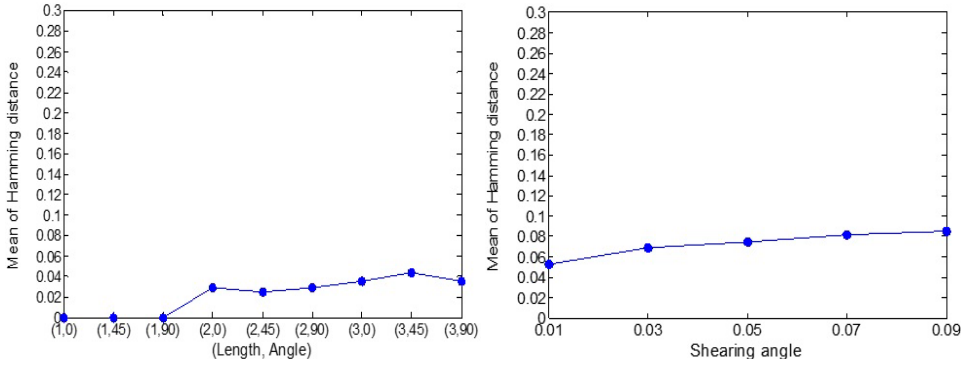
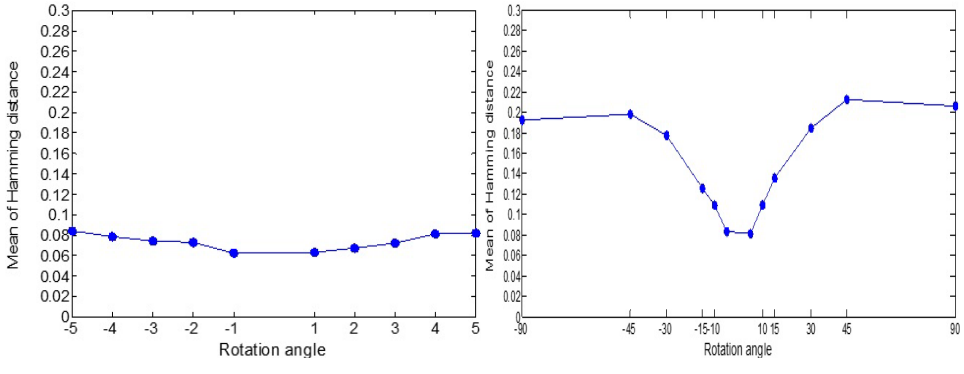


Figure 2 Robustness performances under, (a) JPEG compression (b) Gamma correction (c) Gaussian noise (d) salt and pepper noise (e) speckle noise (f) Gaussian blur (g) motion blur (h) shearing (i) rotation_1 (j) rotation_2 (continued) (see online version for colours)



(g) (h)



(i) (f)

Table 3 Statistics of HDs for the proposed hashing method

Manipulation	*Minimum*	*Maximum*	*Standard deviation*	*Mean*
JPEG compression	0	0.0669	0.0142	0.0234
Gamma correction	0	0.0653	0.0134	0.0198
Gaussian noise	*0.0232*	*0.2452*	*0.0398*	*0.0881*
Salt and pepper noise	*0.0689*	*0.2916*	*0.0439*	*0.1585*
Speckle noise	0.0044	0.1250	0.0205	0.0411
Gaussian blur	0.0051	0.0929	0.0198	0.0372
Motion blur	0	0.0576	0.0117	0.0220
Shearing	0.0076	0.1615	0.0304	0.0726
Rotation_1	0.0051	0.1551	0.0317	0.0735
Rotation_2	*0.0224*	*0.2868*	*0.0509*	*0.1514*

The last column of Table 4 presents performance results in terms of discriminative capabilities discussed in the next subsection.

4.2 Discriminative capabilities

At this stage of performance evaluation, we have carried out experiments on the same sample of images used for perceptual robustness analysis. It consists of a set of 104 images from the FVC2002/DB1_A database Second International Competition for Fingerprint Verification Algorithms (2002) which corresponds to eight fingerprint images of 13 randomly selected subjects. In order to estimate the discriminative capabilities and the collision probability of the proposed hashing method, the HD is computed between pairs of images of different subjects. Distributions of obtained HDs are depicted in Figure 3. Their mean and standard deviation values are μ = 0.21 and σ = 0.05, respectively.

Table 4 Performance results for perceptual robustness and discriminative capabilities with different threshold values

Threshold	*True detection of similar images (%)*					*False classification of different images (%)*
	a	*b*	*c*	*d*	*e*	
0.06	57.68	65.60	61.89	71.55	*76.59*	0
0.08	68.68	77.25	73.19	83.61	*87.95*	0
0.10	76.45	84.70	80.93	91	*94.40*	0.32
0.12	81.44	88.98	85.62	94.84	*97.46*	1.44
0.14	85.43	91.84	89.29	97.17	*99.05*	4.72
0.16	88.44	93.55	91.99	98.37	*99.68*	10.81
0.18	91.45	95.13	94.48	99.15	*99.97*	25.16
0.20	93.17	95.92	95.78	99.33	*100*	40.38

Notes: a all attacks
b all attacks except rotation_2
c all attacks except salt and pepper noise
d all attacks except rotation_2 and salt and pepper noise
e all attacks except rotation_2, salt and pepper noise and Gaussian noise.

The collision property is the probability that the distance (HD) between two different images is lower than a threshold θ and is calculated by the following formula (Qin et al., 2013):

$$\begin{aligned} \Pr_c &= \frac{1}{\sqrt{2\pi\sigma}} \int_{-\infty}^{\theta} \exp\left[-\frac{(x-\mu)^2}{2\sigma^2} \right] dx \\ &= \frac{1}{2} erfc\left(-\frac{\theta-\mu}{\sqrt{2\sigma}} \right) \end{aligned} \tag{4}$$

where *erfc*(.) is a predefined complementary error function, μ and σ are the mean and the standard deviation of the HDs between pairs of images of different subjects. The collision probabilities of our method are given for each threshold value in Table 5.

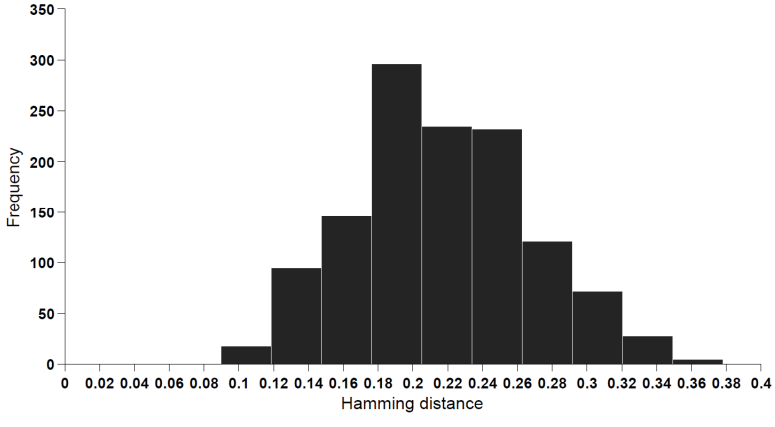
It is worth to note that the collision probability decreases with a decreasing threshold θ; which implies that the proposed hash function presents high discriminative capabilities.

Table 5 Collision probabilities under different thresholds θ

Threshold θ	*Collision probability*
0.06	6.8714×10^{-4}
0.08	2.6000×10^{-3}
0.10	8.2000×10^{-3}
0.12	2.2800×10^{-2}
0.14	5.4800×10^{-2}
0.16	1.1510×10^{-1}
0.18	2.1190×10^{-1}
0.20	3.4460×10^{-1}

Figure 3 shows that the distribution of most of the normalised HDs are above the thresholds $\theta = 0.10$, 0.12, 0.14 with 0.32%, 1.44% and 4.72% respectively, for the rate of different images that are falsely identified as similar images. As shown in Table 4, the true detection of similar images are 94.40%, 97.46% and 99.05% for threshold $\theta = 0.10$, $\theta = 0.12$ and $\theta = 0.14$ respectively while the false classification of different images are 0.32%, 1.44% and 4.72%.

Figure 3 Histogram of the distribution of HD between pairs of fingerprint images belonging to different subjects



It can be noticed that there is a trade-off between the high robustness and the high discrimination rate. By considering the threshold $\theta = 0.12$, we note that the error rate (1.44%) is acceptable if we want to maintain high robustness of our method. This implies that the perceptual hashing method has good discriminative capability.

Interpretation of the results in terms of robustness and discriminative capabilities of the perceptual hashing scheme requires the selection of the appropriate threshold that gives the best trade-off between the robustness and the discrimination rates. As can be noticed from Table 4, robustness performances, represented by the true detection of similar images rate, increase with higher threshold values while the discriminative capabilities (false classification of different images rate) decrease.

Thus, if the threshold is set to $\theta = 0.10$, the robustness attribute against the attacks is equal to 94.40% and the discrimination rate equals 0.32%. If the threshold is increased to $\theta = 0.12$, the two performance attributes get to 97.46% and 1.44% rates respectively. For $\theta = 0.14$, the true detection of similar images rate increases to 99.05% while the false classification of different images rate decreases to 4.72%.

5 Performance comparison

In this section, the demonstration of the performance of our hashing method consists in comparing it with existing well-known methods in the literature. The first hashing model Neelima and Singh (2016) is 46 × 46 bloc-based decomposition using the SIFT-SVD features extraction. The second one named GF-LVQ is introduced in Li et al. (2012) and is based on random Gabor filtering and dithered LVQ for image hash construction. The natural input images are normalised to 512 × 512 pixels size and decomposed into 40 rings. The hash computation in the third comparing method (Yuling et al., 2016) relies upon extracted Radon transform-invariant features using the same parameters as in Li et al. (2012). As for our method, the blocks size has been set to 32 × 32 after an array of experiments and the maximum Euclidean distance between minutiae and SIFT key-points has been selected to $d = 15$.

It is worth noting that the normalised HD has been employed as hash similarity measure between the original images and their attacked versions in our model as well as models in Neelima and Singh (2016) and Li et al. (2012) while the robustness assessment of the model proposed in Yuling et al. (2016) relies on the Euclidean distance. The visualisation of the performance of the previously described hashing methods, in terms of perceptual robustness, consists in exploiting a receiver operating characteristics (ROC) graph (Fawcett, 2006), where the x-axis represents the false positive rate (FPR), while the y-axis represents the true positive rate (TPR). TPR and FPR are calculated as follows:

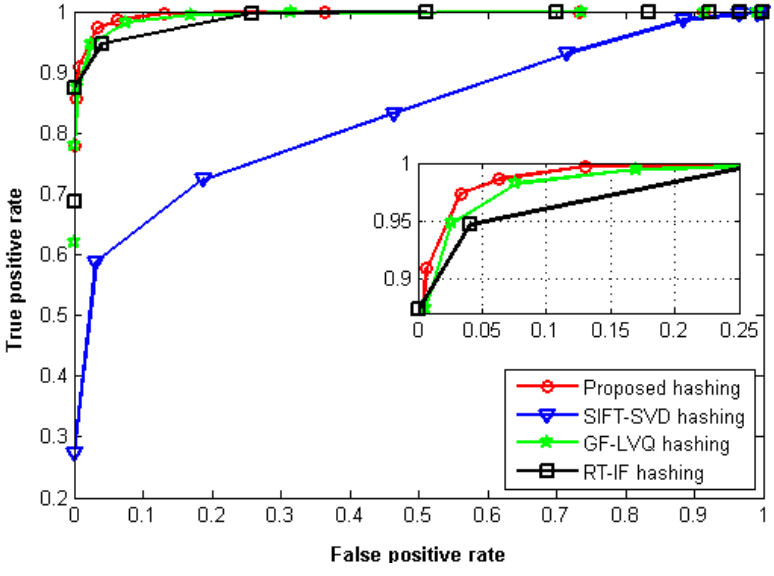
$$P_{TPR} = \frac{n_s}{N_{total-s}} \tag{5}$$

$$P_{FPR} = \frac{n_d}{N_{total-d}} \tag{6}$$

where n_s corresponds to the number of pairs of hash codes of visually identical images considered to be similar (their similarity measure is under the threshold θ), n_d is the number of pairs of hash codes of different images but considered to be similar, $N_{total-s}$ is the total number of pairs of visually identical images, whereas $N_{total-d}$ relates to the number of pairs of different images.

The generation of the ROC curve requires the computation of TPR and FPR for each hash method using the different threshold values. The hash method is considered the most robust if it has the highest TPR. However, if two methods have the same TPR, the one with the lowest FPR is considered the best. From the ROC curve presented in Figure 4, it can be observed that the proposed hashing method has the highest curve to the left. It can be concluded that the performance of our scheme is better that the other methods.

Figure 4 ROC comparison of the proposed hashing method with three existing hashing algorithms (see online version for colours)



6 Conclusions

A new solution for the fingerprint templates protection has been described in this paper. It is a two-stage key-points features selection followed by frequency domain transforms. The selected features are obtained using the SIFT in order to have the robust characteristic points that are closest to the minutiae points, and then filtered by Harris method to select the most stable key-points. The resulting binarised image is then decomposed into blocks where the DWT is performed on each block followed by the SVD. The hash code is generated by concatenating the singular values of each block.

According to extensive experimental tests, the proposed perceptual hashing methods is more robust than other methods under consideration against a large array of acceptable attacks including JPEG compression, Gamma correction, speckle noise, Gaussian blur, motion blur, shearing and slight rotation. It also shows very interesting low rates for false classification of different images.

References

Abdullahi, S.M., Wang, H. and Malik, A. (2018) 'Fingerprint image hashing based on minutiae points and shape context', *IJDCF*, Vol. 10, No. 4, pp.1–20, DOI: 10.4018/IJDCF.2018100101.

Ali, S.S., Ganapathi, I.I. and Prakash, S. (2018) 'Robust technique for fingerprint template protection', *IET Biometrics*, Vol. 7, No. 6, pp.536–549, DOI: 10.1049/iet-bmt.2018.5070.

Cappelli, R., Ferrara, M. and Maltoni, D. (2010) 'Minutia cylinder-code: a new representation and matching technique for fingerprint recognition', *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 32, No. 12, pp.2128–2141, DOI: 10.1109/TPAMI.2010.52.

Chouhan, R. and Khanna, P. (2011) 'Robust minutiae watermarking in wavelet domain for fingerprint security', *World Academy of Science, Engineering and Technology*, Vol. 60, pp.1612–1619, DOI: 10.5281/zenodo.1331413.

Das, P., Karthik, K. and Garai, B.C. (2012) 'A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs', *Pattern Recognit.*, Vol. 45, No. 9, pp.3373–3388, DOI: 10.1016/j.patcog.2012.02.022.

Fawcett, T. (2006) 'An introduction to ROC analysis', *Pattern Recognit. Lett.*, Vol. 27, No. 8, pp.861–874, DOI: 10.1016/j.patrec.2005.10.010.

Ferrara, M., Maltoni, D. and Cappelli, R. (2012) 'Noninvertible minutia cylinder-code representation', *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 6, pp.1727–1737, DOI: 10.1109/TIFS.2012.2215326.

Ferrara, M., Maltoni, D. and Cappelli, R. (2014) 'A two-factor protection scheme for MCC fingerprint templates', *BIOSIG 2014 – Proceedings of the 13th International Conference of the Biometrics Special Interest Group*, 10–12 September 2014, Darmstadt, Germany, GI, pp.171–178.

Fingerprint Verification Competition (FVC2002) Database DB1_A (2002) [online] http://bias.csr.unibo.it/fvc2002/databases.asp (accessed 22 October 2021).

Govindaraj, P. and Sandeep, R. (2015) 'Ring partition and DWT based perceptual image hashing with application to indexing and retrieval of near-identical images', *2015 Fifth International Conference on Advances in Computing and Communications (ICACC)*, IEEE, pp.421–425, DOI: 10.1109/ICACC.2015.90.

Harris, C.G. and Stephens, M. (1988) 'A combined corner and edge detector', *Proceedings of the Alvey Vision Conference, AVC 1988*, Alvey Vision Club, Manchester, UK, September, pp.147–151, DOI: 10.5244/C.2.23.

Hernandez, R.A.P., Miyatake, M.N. and Kurkoski, B.M. (2011) 'Robust image hashing using image normalization and SVD decomposition', *2011 IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS)*, IEEE, pp.1–4.

Jin, Z., Lim, M., Teoh, A.B.J. and Goi, B. (2014) 'A non-invertible randomized graph-based Hamming embedding for generating cancelable fingerprint template', *Pattern Recognit. Lett.*, Vol. 42, pp.137–147, DOI: 10.1016/j.patrec.2014.02.011.

Jin, Z., Teoh, A.B.J., Ong, T.S. and Tee, C. (2009) 'Secure minutiae-based fingerprint templates using random triangle hashing', *Visual Informatics: Bridging Research and Practice, First International Visual Informatics Conference, IVIC 2009*, Proceedings, Springer, Kuala Lumpur, Malaysia, 11–13 November, Vol. 5857, pp.521–531, DOI: 10.1007/978-3-642-0503-7_49.

Karsh, R.K., Laskar, R.H. and Aditi (2017) 'Robust image hashing through DWT-SVD and spectral residual method', *EURASIP J. Image and Video Processing*, Vol. 2017, No. 1, p.31, DOI: 10.1186/s13640-017-0179-0.

Kaur, M., Singh, M., Girdhar, A. and Sandhu, P.S. (2008) 'Fingerprint verification system using minutiae extraction technique', *World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering*, Vol. 2, pp.3405–3410, DOI: 10.5281/zenodo.1082823.

Lee, C. and Kim, J. (2010) 'Cancelable fingerprint templates using minutiae-based bit-strings', *J. Netw. Comput. Appl.*, Vol. 33, No. 3, pp.236–246, DOI: 10.1016/j.jnca.2009.12.011.

Li, Y., Lu, Z., Zhu, C. and Niu, X. (2012) 'Robust image hashing based on random Gabor filtering and dithered lattice vector quantization', *IEEE Trans. Image Processing*, Vol. 21, No. 4, pp.1963–1980, DOI: 10.1109/TIP.2011.2171698.

Liu, E. and Zhao, Q. (2017) 'Encrypted domain matching of fingerprint minutia cylinder-code (MCC) with l1 minimization', *Neurocomputing*, Vol. 259, pp.3–13, DOI: 10.1016/j.neucom.2016.06.083.

Lowe, D.G. (2004) 'Distinctive image features from scale-invariant keypoints', *International Journal of Computer Vision*, Vol. 60, No. 2, pp.91–110, DOI: 10.1023/B:VISI.0000029664.99615.94.

Lv, X. and Wang, Z.J. (2012) 'Perceptual image hashing based on shape contexts and local feature points', *IEEE Trans. Information Forensics and Security*, Vol. 7, No. 3, pp.1081–1093, DOI: 10.1109/TIFS.2012.2190594.

Mihçak, M.K. and Venkatesan, R. (2001) 'New iterative geometric methods for robust perceptual image hashing', *Security and Privacy in Digital Rights Management, ACM CCS-8 Workshop DRM 2001*, Revised Papers, Springer, Philadelphia, PA, USA, 5 November, pp.13–21, DOI: 10.1007/3-540-47870-1_2.

Mirmohamadsadeghi, L. and Drygajlo, A. (2013) 'A template privacy protection scheme for fingerprint minutiae descriptors', *2013 BIOSIG – Proceedings of the 12th International Conference of Biometrics Special Interest Group*, GI, Darmstadt, Germany, 4–6 September 2013, pp.185–192.

Muthu, R., Bouridane, A. and Khelifi, F. (2014) 'Minutiae based fingerprint image hashing', *International Conference on Control, Decision and Information Technologies, CoDIT 2014*, IEEE, Metz, France, 3–5 November, pp.696–700, DOI: 10.1109/CoDIT.2014.6996981.

Nagar, A., Nandakumar, K. and Jain, A.K. (2008) 'Securing fingerprint template: fuzzy vault with minutiae descriptors', *19th International Conference on Pattern Recognition (ICPR 2008)*, IEEE Computer Society, Tampa, Florida, USA, 8–11 December, pp.1–4.

Nandakumar, K. (2010) 'A fingerprint cryptosystem based on minutiae phase spectrum', *2010 IEEE International Workshop on Information Forensics and Security, WIFS 2010*, IEEE, Seattle, WA, USA, 12–15 December, pp.1–6.

Neelima, A. and Singh, K.M. (2016) 'Perceptual hash function based on scale-invariant feature transform and singular value decomposition', *Comput. J.*, Vol. 59, No. 9, pp.1275–1281, DOI: 10.1093/comjnl/bxv079.

Ouyang, J., Liu, Y. and Shu, H. (2017) 'Robust hashing for image authentication using SIFT feature and quaternion Zernike moments', *Multimedia Tools Appl.*, Vol. 76, No. 2, pp.2609–2626, DOI: 10.1007/s11042-015-3225-x.

Ouyang, J., Wen, X., Liu, J. and Chen, J. (2016) 'Robust hashing based on quaternion Zernike moments for image authentication', *ACM Trans. Multim. Comput. Commun. Appl. (TOMM)*, Vol. 12, No. 4s, pp.63:1–63:13, DOI: 10.1145/2978572.

Qin, C., Chang, C. and Tsou, P. (2013) 'Robust image hashing using non-uniform sampling in discrete Fourier domain', *Digit. Signal Process.*, Vol. 23, No. 2, pp.578–585, DOI: 10.1016/j.dsp.2012.11.002.

Sandhya, M. and Prasad, M.V.N.K. (2015) 'k-nearest neighborhood structure (k-NNS) based alignment-free method for fingerprint template protection', *International Conference on Biometrics, ICB 2015*, IEEE, Phuket, Thailand, 19–22 May, pp.386–393, DOI: 10.1109/ICB.2015.7139100.

Second International Competition for Fingerprint Verification Algorithms (2002) [online] http://bias.csr.unibo.it/fvc2002/.

Wang, S. and Hu, J. (2016) 'A blind system identification approach to cancelable fingerprint templates', *Pattern Recognit.*, Vol. 54, pp.14–22, DOI: 10.1016/j.patcog.2016.01.001.

Wang, S., Deng, G. and Hu, J. (2017a) 'A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations', *Pattern Recognit.*, Vol. 61, pp.447–458, DOI: 10.1016/j.patcog.2016.08.017.

Wang, S., Yang, W. and Hu, J. (2017b) 'Design of alignment-free cancelable fingerprint templates with zoned minutia pairs', *Pattern Recognit.*, Vol. 66, pp.295–301, DOI: 10.1016/j.patcog.2017.01.019.

Yang, B., Busch, C., Bours, P. and Gafurov, D. (2010) 'Robust minutiae hash for fingerprint template protection', *Media Forensics and Security II, Part of the IS&T-SPIE Electronic Imaging Symposium*, Proceedings, SPIE, San Jose, CA, USA, 18–20 January, p.75410R, DOI: 10.1117/12.838998.

Yuling, L., Guojiang, X. and Yong, X. (2016) 'Robust image hashing using Radon transform and invariant features', *Radio Engineering*, Vol. 25, No. 3, pp.556–564, DOI: 10.13164/re.2016.0556.

Zhao, Y., Wang, S., Zhang, X. and Yao, H. (2013) 'Robust hashing for image authentication using Zernike moments and local features', *IEEE Trans. Information Forensics and Security*, Vol. 8, No. 1, pp.55–63, DOI: 10.1109/TIFS.2012.2223680.