Comparison of RADIAL variance based and Maar-Hildreth operator perceptual image hash functions on biometric templates

Bernard Vukelić
Polytechnic of Rijeka
Vukovarska 58, 51000 Rijeka, Croatia
bernard.vukelic@veleri.hr

Miroslav Bača
Faculty of Organization and Informatics
University of Zagreb
Pavlinska 2, 42000 Varaždin, Croatia
miroslav.baca@foi.hr

Abstract. *This paper presents a practical comparison between two perceptual hash functions, RADIAL Variance Based Hash and Maar-Hildreth Operator. Perceptual image hashing functions are used for image and visual content authentication. For the purposes of this paper the authors will compare the two functions to evaluate their resistance to several types of attacks on biometric templates.*

The main objective of this paper is to examine whether the implementation of perceptual hash functions could have an effect on similarity of these templates. pHash, an open source implementation of various perceptual hash functions, was used to benchmark these functions.

The results of this comparison and evaluation will be preliminary because only three most common biometrics characteristic templates will be considered. Robust perceptual image hashing methods will be used to overcome the abovementioned problems of a challenging developing biometric systems.

Keywords. perceptual hash functions, RADIAL Variance Based Hash, Maar-Hildreth Operator, biometric templates

1 Introduction

User recognition is a key element in information technology, especially in those systems which include an automated access control, such as e-commerce, Internet banking, physical and logical access control, forensics etc. Recognition is normally based on what a person owns, such as a key or a smart card; what a person knows, such as a password or a PIN; or what a person is, which includes physical characteristics (e.g. fingerprint or iris) or behavior (e.g. signature or walk). In terms of information technology, biometrics is defined as an automated measurement and the analysis of physical and behavioral characteristics of a person in order to determine this person's authenticity.

Depending on implementation, biometrics systems can recognize a person based on authentication or identification. Authentication is a process in which a person claims to be the person he says he is, which makes this person a genuine user. In that case, the biometrics system compares a sample only with this person's template, which is already stored in a database. If the collected sample and template have a high match score, the user is considered to be genuine. In contrary, the user is considered to be an impostor. The decision whether a person is genuine or not is normally based on match store threshold. Identification of a user is divided into two types – positive and negative. Positive identification is based on a comparison 1 : N, in which the collected sample is compared with all the templates in the database. It answers the following question: "Does the system recognize this user?". Negative identification is based on blacklists. It is commonly used in police investigations and pass border controls.

Match score results depend on biometrics characteristics, the method of sample collection representation, technical characteristics of the sensor and the users. Authentication is based on scores that can range between 0 % and 100 %. During the authenticating stage numerous errors can occur. In such case, it is necessary to correct those errors. The amount of correction required is a measure of the authentication confidence.

Hash functions are well-known in cryptography and are widely used for digital signatures. They basically summarize a message in a short and constant bit length digest, which uniquely identifies the original message. In case the biometric data is hashed, even the smallest change in the acquisition of the biometric (a very likely scenario) can lead to a completely different hash value. Thus, it may not match the original within the same matching threshold as that for the straight unhashed scenario. Cryptographic hashing has to be resistant to collision.

The purpose of perceptual image hashing is to define an image digest that satisfies two properties. On the one hand, the robust image digest characterizes the image in the sense that it uniquely identifies its content, i.e. the digests derived from a pair of visually distinct inputs have a low probability to be identical. On the other hand, the hashing process is robust in the sense that the digest is only slightly affected when the image changes due to compression or minor processing, i.e. visually indistinguishable images generate equal or similar digests. [5] Conversely to cryptographic hashing, robust hashing is thus able to deal with visually non-significant changes of the content, and supports common manipulations like compression or reformating (e.g. spatial or temporal subsampling). A good perceptual hash function should be: 1) robust: Manipulations that don't change the perceptual information should not change the hash value. 2) unique: Perceptually different inputs should have completely different hash values. 3) secure: It should be very hard to find (forge) perceptually different inputs having similar hash values. [1]

Perceptual image hashing functions extract certain features from image and calculate a hash value based on these features. These functions help establish the “perceptual equality” of image content. Image authentication is done by comparing the hash values of the original image and the image to be authenticated. It is expected that perceptual hashes are able to survive on acceptable content-preserving manipulations and reject malicious manipulations.

Perceptual image hashing system generally comprises of four pipeline stages: the *Transformation* stage, the *Feature extraction* stage, the *Quantization* stage and the *Compression and Encryption* stage as shown in Figure 1. [2]

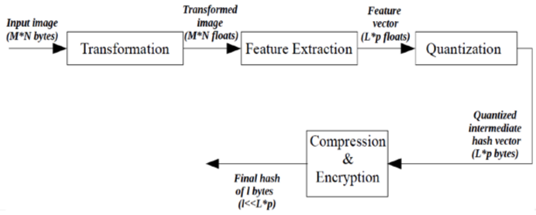

Input image (M*N bytes)
Transformation
Transformed image (M*N floats)
Feature Extraction
Feature vector (L*p floats)
Quantization
Quantized intermediate hash vector (L*p bytes)
Compression & Encryption
Final hash of l bytes (l<<L*p)

Figure 1. Perceptual image hashing system [2]

Because it defines a vector that identifies the image contents, robust hashing is an obvious solution for content identification and indexing. Since the requirement of bit-by-bit hashes equality is usually hard to achieve, most of the proposed schemes compute distances and similarities between perceptual hashes. The most often used are the Bit Error Rate (BER), the Hamming distance and the Peak of Cross Correlation (PCC). The first two measure the distance between two hash values, whereas the latter measures the similarity between two hash values. [2]

This paper will examine whether the implementation of perceptual hash functions could have an effect on similarity of biometrics templates. The results of this evaluation will be preliminary because only three most common biometrics characteristics will be considered. The authors will use RADIAL (Radial Variance Based Hash) function, which was introduced by Lefebvre et al [4] and Marr-Hildreth Operator Based Hash. pHash, an open source implementation of various perceptual hash functions, was used to benchmark these functions.

The focus of the research were the biometrics systems which are used for negative identification, such as blacklist, watch list or suspect list, e.g. systems used by public security officials in order to identify individuals of interest for crime prevention (airports, disease control, border pass control etc.). Such systems generally must satisfy the following criteria:[8]

- can identify a single person from a large population of people,
- do not change over time,
- fast to acquire and easy to use,
- can respond in real-time needed for mass transit locations,
- are safe and non-invasive,
- can scale in millions and maintain top performance,
- are affordable.

However, in many real-world applications, such biometrics systems often face significant limitations due to sensitivity to noise, data quality, nonuniversality, lighting and other environmental conditions.

Perceptual hash functions are used in a similar way to biometrics systems - both are just a kind of pattern recognition application.The implementation of these functions on a biometrics template will result with a negative classification of non-similar templates in a database in a short period of time. The templates with the smallest visual similarity will be rejected. The main objective of this research and the authors’ motivation was to find whether pHash functions are able to extract all biometrics templates which are the most similar to the original sample, and to implement them in biometric systems. The precise identification can be determined based on these templates.

2 Radial Variance Based Hash

Lef`ebvre and Macq [4] proposed a perceptual image hash function based on the Radon transform [5]. Few years later, both authors pointed out in [6] that their previously proposed algorithm suffers from certain issues. So, they introduced a new algorithm [6] to solve these problems.

The Radon transform is the integral transform which consists of the integral of a function over a straight line. It is robust against various image processing steps and geometrical transformations. In [5] a new visual content descriptor, based on the Radon transform, was presented. α denotes the angle of the used projection line. x denotes the coordinate of a pixel along the x-axis and y denotes the coordinate of a pixel along the y-axis. In order to extend the Radon transform to discrete images, the line integral along *d = x · cos α + y · sin α* can be approximated by a summation of the pixels lying in the one pixel wide strip: [3]

$$d - \frac{1}{2} \leq x \cdot cos\alpha + y \cdot sin\alpha \leq d + \frac{1}{2}. \qquad (1)$$

The algorithm proposed in [6] uses the variance instead of the sum of the pixel values along the line projections. The variance captures luminance discontinuities along the projection lines much better. Such discontinuities result from edges, that are orthogonal to the projection direction. The so-called radial variance vector *(R[α])* is therefore defined as follows. Let *Γ(α)* denote the set of pixels *(x, y)* on the projection line corresponding to a given angle α. Let *(x', y')* denote the coordinates of the central pixel of the image. *(x, y) ∈ Γ(α)* if: [3]

$$-\frac{1}{2} \leq (x - x') \cdot cos\alpha + (y - y') \cdot sin\alpha \leq \frac{1}{2}. \qquad (2)$$

Let I(x,y) denote the luminance value of the pixel (x,y), the radial variance vector R[α], where α = 0,1,...,179, is then defined by:[3]

$$R[\alpha] = \frac{\sum_{(x,y)\in\Gamma(\alpha)} I^2(x,y)}{\#\Gamma(\alpha)} - \left(\frac{\sum_{(x,y)\in\Gamma(\alpha)} I(x,y)}{\#\Gamma(\alpha)}\right)^2 \qquad (3)$$

Marr-Hildreth Operator Based Hash wavelength function calculates the perceptual hash based on information about corners. The query-image hash string is compared with the training set images. Similarity is measure in the basis of hamming distance score. The normalized hamming distance is used to measure the distance between two hash values. Based on the score the similar images are retrieved. If the hamming distance score is too far when compared to query-image hash string then it is neglected. Hamming distance is a measurement of two different strings. The strings can be collection of characters, numbers or binary coded numbers. [9]

Let A denote an alphabet of finite length. P and Q are the finite string which belongs to A. where P = $(p_1,p_2,p_3.......p_n)$, Q = $(q_1,q_2,q_3......q_n)$ The Hamming distance (Δ) of two string P and Q is defined as: [10]

$$\Delta(p,q) = \sum_{p_i \neq q_i} 1, i = 1,2,3 \ldots \ldots \ldots n$$

If the bit of two strings are not same then record as 1 else record as 0 and at last sum the number of one's and zero's to find out the hamming distance score. [10]

3 Evaluation

To evaluate the robustness and collision resistance of proposed hashing methods, we experimented Radial Variance Based Hash function and Marr-Hildreth Operator Based Hash wavelength function on 3 biometrics characteristics templates taken from the database BIT CASIA [7] – fingerprint, iris and palm.

The objective of this research was to find an effect of perceptual hash functions on each template. All the three templates are 8-bit grey level images. In order to improve performance, the images were set to similar image resolution, which is presented in Table 1.

For each of the 3 images of the dataset, we considered 4 image processing attacks, generating 101 images or intra images. "Attack" is a term for operation of modification or manipulation of an original image template. Since pHash is defined as a visual alteration, a modification operation should not alter the essential content of a biometric template.

After the modification, the biometric template is still expected to be detected as authentic by perceptual hash function.

Manipulation is defined as an operation that alters the essential content of a biometric template. After manipulation, the biometric template is expected to be detected as not authentic (impostor) by perceptual hash function.

The attacks which were tested in this paper were the following:

- Brightness: (-30 % – +30 %).
- Compression: JPEG compression with scale of 10 % (10 % – 100 % quality factor)
- Geometric scaling (factors = 0.1) from 100 % – 10 %, and
- Rotation with centered cropping (-20 % – +20 %) and 90° and 180°.

Brightness operation is commonly used method for image manipulation. In biometric systems it is a common problem due to environmental factors. JPEG compression, scaling and rotation are some of the most commonly used image operations which users employ to modify their images. For example, they can be used in order to reduce the file size of templates which are being saved in biometric database. The rotation operation was used to demonstrate the robustness of perceptual image hash functions. The 90° – 180° rotation operation was used because it hardly changes the human perception of a template. The processed images were compared to the original images to determine similarity.

Template	Iris	Finger	Palm
Enviroment	indoor	indoor	indoor
Resolution	320x240	328x356	320x280

Table 1. Description of biometric characteristics templates used

4 The Results

The following tables and figures represent similarity results. At first, the image is converted to grey scale. After that pHash implements a few additional image pre-processing steps. That is, as suggested by the two function parameters sigma and gamma, blurring and gamma correction. Of the discussed perceptual image hash functions, the radial variance based image hash function is the only one which does not normalize the image with respect to resolution. Comparing two hash values is done by calculating the PCC between the two hash values.

The peaks of cross-correlation (PCCs) in Radial Variance Based Hash range from 0 to 1. All the PCCs closer to 1 represent higher image similarity. The threshold was set to 0.85.

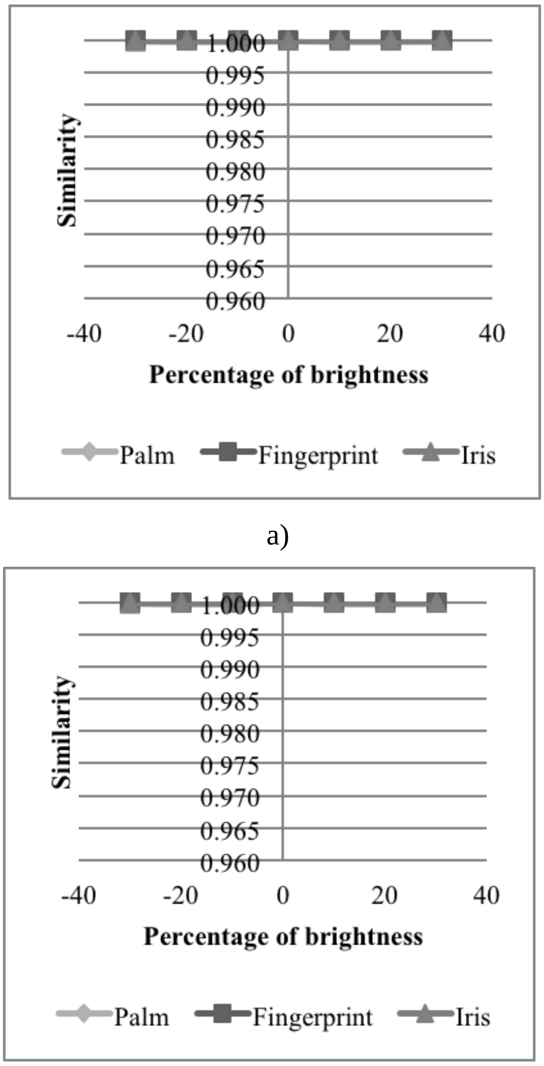
Marr-Hildreth Operator Based Hash wavelength function gives results in opposite order (results closer to 0 represent higher similarity) than Radial Variance Based Hash function, which was set as a reference. In order to compare the results, they had to normalized in the following way (eg. 4) :

$$n_1=1-n \qquad (4)$$

where *n* represents the result given by Marr-Hildreth Operator Based Hash function, and *n_1* represents the normalised result. Tolerance threshold for this function is usually 0.40, but, since the authors have set normalization of results, tolerance threshold was 0.60. In Figure 2 it can be observed that, in the first attack (brightness attack), fingerprint was the most robust, and palm was the most sensitive to changes -30 – +30 % of brightness. It should be noted that all the three images are above threshold of 0.85, i.e. they are recognized as identical. In all three biometrics templates it can be observed that RADIAL hash functions are considerably robust to brightness attack (positive and negative shift). Total minimum shift confirms function robustness, which can be seen in Table 2. Marr-Hildreth Operator Based Hash wavelength function deviates when it comes to positive and negative shifts in brightness attack. All the three templates share an anomaly – after a certain degree shift the curve starts to incline. Although the value is high above threshold (0.85), this indicates that the function can provide unexpected results when it comes to greater brightness shifts. Palm is the most sensitive to brightness shift (Figure 3).

Template	Palm	
Similarity	RH	MH
Max.	0.999990	0.979167
Min.	0.999968	0.963542

Table 2. Minmum and maximum values (results of brightness attack) of palm biometric characteristic template for RADIAL Hash (RH) and Marr-Hildreth Operator Based Hash (MH) wavelength function.



a)

b)

Figure 2. Results of brightness attack: a) RADIAL Variance Based Hash and b) Marr-Hildreth Operator Based Hash wavelength function

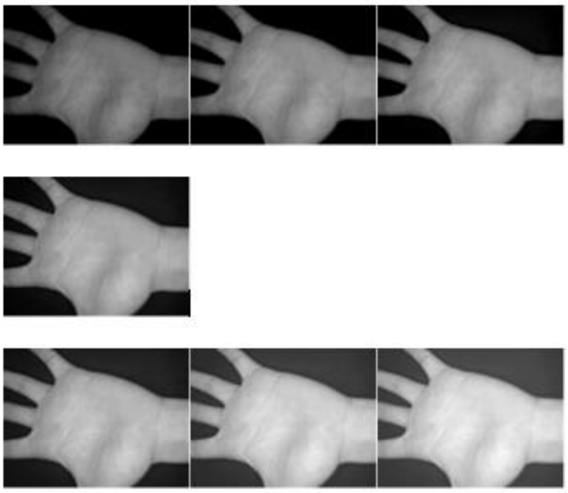
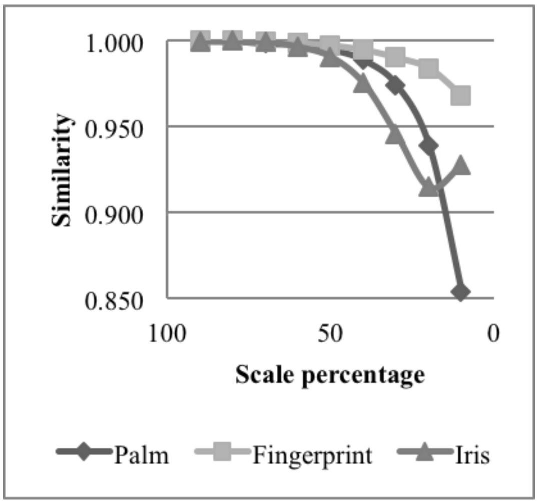
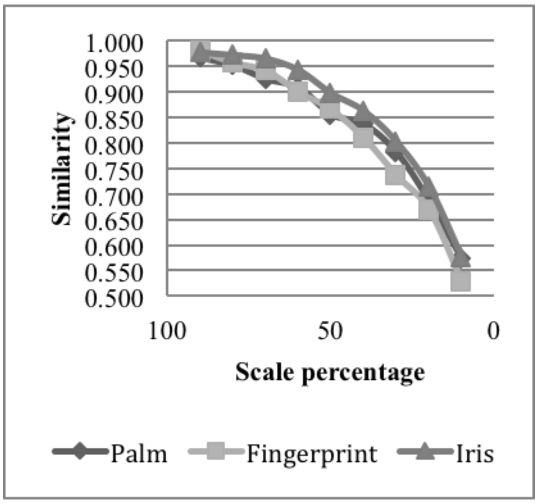


Figure 3. Brightness attack on palm template from -30 % to +30 %.



a)



b)

Figure 4. Results of scale attack: a) RADIAL Variance Based Hash and b) Marr-Hildreth Operator Based Hash wavelength function

Figure 4 shows the results of scale attack. The height was adjusted proportionally. Bicubic interpolation was used. The x-axis comprises of degrees (10 – 100) and y-axis comprises of similarity. It can be seen that all the three images are resistant to scale attack. When a high value (10 – 20 %) is reached, all the three characteristics decrease in similarity to the original. Palm is the most sensitive because it is evident that its value is closest to threshold. Figure 4 also shows that Marr-Hildreth Operator Based Hash wavelength function is very sensitive to scale attacks. When a value (10 – 20 %) is reached, none of the templates is recognized as similar because their values are below threshold.

Figure 5 shows the comparison between the original image of iris (320x240 px) and two images which show a 90 % scale change. Although the scale size is very small, RADIAL function showed 0.92 similarity, which is considered similar to the original according to the threshold of 0.85.

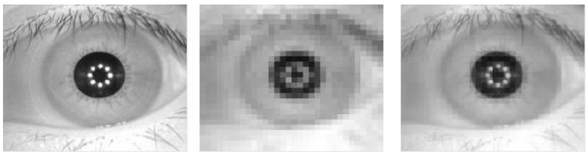


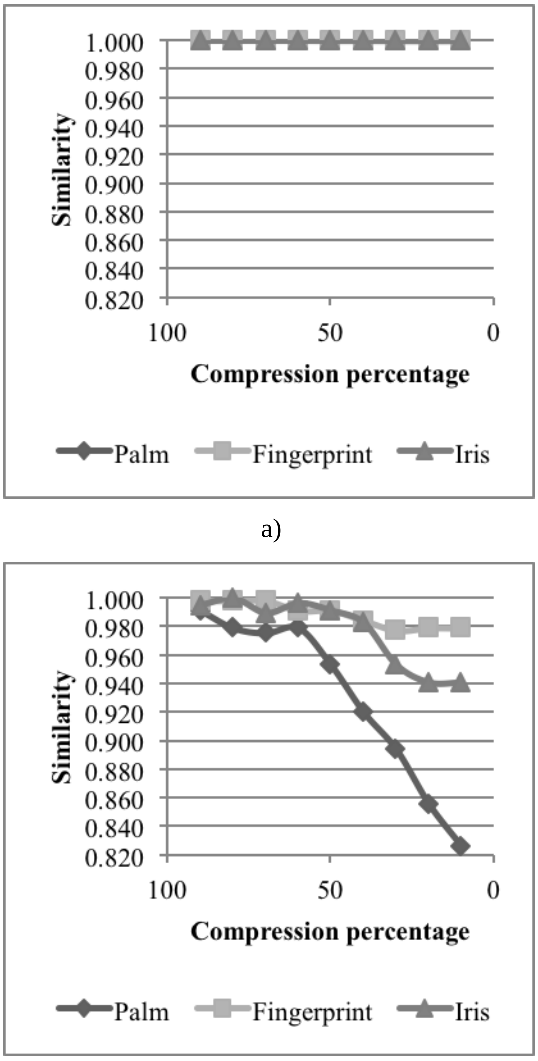
Figure 5. 100 % (320x240 px) and 10 % (32x24 px) scale = 0.92 similarity by RADIAL hash

Figure 6 shows the results of compression JPEG image compression attack. It can be seen that all the characteristics are resistant to this type of attack because there is almost no change in similarity despite the increase of image compression. The RADIAL Variance Based Image Hash function is almost not influenced at all by the quality parameter. Even when using a quality parameter of 10 %, the average distance score of this hash function is negligible. Figure 6 also shows that Marr-Hildreth Operator Based Hash wavelength function is more sensitive than RADIAL Variance Based Image Hash function to scale attacks. When a value (10 – 20 %) is reached, none of the templates is recognized as similar because their values are below threshold. Regardless of the sensitivity, the similarity results are in positive range. The Marr-Hildreth Operator Based Image Hash function performs the worst when it comes to palm.

Table 2 shows that the result of similarity deviation is very small and the image size is different (21.754 bytes compared to 14.847 bytes). The results are almost the same.

JPEG image quality	RH	MH	Image size (Bytes)
100 %	1.00000	1.00000	21.754
…	…	…	…
10 %	0.999937	0.826389	14.847

Table 2. Compression attack JPEG image quality for palm



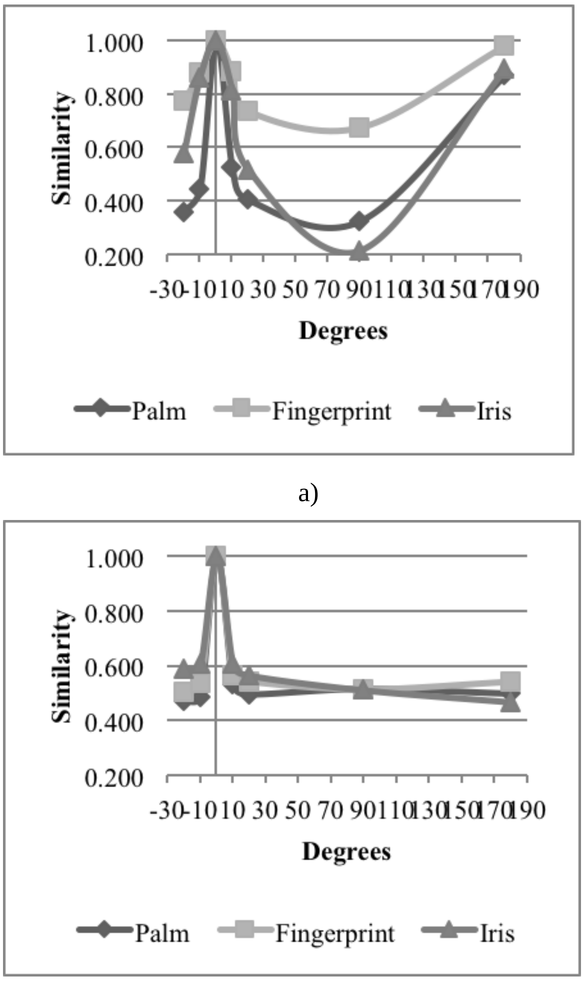
a)

b)

Figure 6. Results of JPEG compression quality attack: a) RADIAL Variance Based Hash and b) Marr-Hildreth Operator Based Hash wavelength function

The results of rotation attack are shown in Figure 7. It comprises of two axis. X-axis comprises of degrees (-20 – +20°), 90°, 180°. PCCs are shown on y-axis. The research has shown that none of perceptual hash functions is robust to rotation attacks.

It can also be observed that negative and positive rotation shifts provide different results. Even a small rotation shift causes a result below threshold. Using this kind of image operation none of the tested image hash functions is robust.



a)

b)

Figure 8. Results of rotation attack on a) RADIAL Variance Based Hash function b) Marr-Hildreth Operator Based Hash wavelength function

5 Conclusion

The research showed that both perceptual hash image RADIAL Variance Based function and Marr-Hildreth Operator Based Hash wavelength function could be used with biometrics templates. Although it included only three characteristics, the results were significant because they showed that this function could be applied to different biometrics characteristics and biometrics systems. However, there are differences between these functions, which can be seen from the results of the research. When it comes to great brightness shifts, RADIAL Variance Based hash function provides unexpected results although the value is high above threshold (0.85). With regard to JPEG compression and scale operations, both functions are showing robustness, but none of the functions is robust to great rotation shifts. Although the Marr-Hildreth operator based hash function is behind the other function when it comes to robustness, it has more discriminative abilities.

The preliminary results of this research were based on a small number of biometric characteristics. In order to get more precise results, further experiments are required, such as using other biometrics characteristics, which will include both physical and behavioral characteristics as well as other template modifications and manipulations.

References

[1] Coskun B., Memon N.: Perceptual Hashing, Polytechnic institute of NYU, http://isis.poly.edu/projects/percephash, downloaded: March 25th 2014.

[2] Hadmi, A., Puech, W., AitEssaid, B. & Aitouahman, A.: Perceptual Image Hashing, University of Montpellier II, University of Cadi Ayyad,ETRITeam,www.intechopen.com/download/pdf/36921, downloaded: March 25th 2014.

[3] Zauner, C.: Implementation and Benchmarking of Perceptual Image Hash Functions. Master's thesis, Upper Austria University of Applied Sciences, Hagenberg Campus, 2010.

[4] Lef`ebvre, F., Macq, B., and Legat, J.D.: RASh: RAdon Soft Hash algorithm. In Proceedings of the European Signal Processing Conference (EUSIPCO), vol. I, pp. 299–302. European Association for Signal Pro- cessing, 2002.

[5] Radon, J.: On the determination of functions from their integral values along certain manifolds. IEEE Transactions on Medical Imaging, 5(4): pp.170–176, Dec. 1986.

[6] Standaert, F.X., Lef`ebvre, F., Rouvroy, G., Macq, B.M., Quisquater, J.J., and Legat, J.D.: Practical evaluation of a radial soft hash algorithm. In Proceedings of the International Symposium on Information Technology: Coding and Computing (ITCC), vol. 2, pp. 89–94. IEEE, 2005.

[7] Biometrics Ideal Test (BIT) databases, Tinieu T., Center for Biometrics and Security Research (CBSR), China, http://biometrics.idealtest.org/, downloaded: March 21st 2014.

[8] Al-Raisi Ahmad N., Al-Khouri Ali M.: Iris recognition and the challenge of homeland and border control security in UAE, Science direct, Telematics and Informatics 25, pp. 117–132, United Arab Emirates, 2008.

[9] Nagarajan S. K., Saravanan S.: Content-based Medical Image Annotation and Retrieval using Perceptual Hashing Algorithm, VIT University, India, IOSR Journal of Engineering, Vol. 2(4) pp. 814-818, 2012.

[10] Hamming, R.: Error Detecting and Error Correcting Codes, Bell System Technical Journal (26:2), pp. 147—160, 1950.