BULLETIN OF THE POLISH ACADEMY OF SCIENCES
TECHNICAL SCIENCES, Vol. 64, No. 4, 2016
DOI: 10.1515/bpasts-2016-0090

Verification of iris image authenticity using fragile watermarking

A. CZAJKA[1]*, W. KASPRZAK[2], and A. WILKOWSKI[3]

[1]Research and Academic Computer Network (NASK), 12 Kolska St., 01-045 Warsaw, Poland
[2]Institute of Control and Computation Engineering, Warsaw University of Technology, 15/19 Nowowiejska St., 00-665 Warsaw, Poland
[3]Faculty of Geodesy and Cartography, Warsaw University of Technology, 1 Plac Politechniki, 00-061 Warsaw, Poland

Abstract. This paper proposes and evaluates a watermarking-based approach to certify the authenticity of iris images when they are captured by a genuine equipment. In the proposed method, the iris images are secretly signed before being used in biometric processes, and the resulting signature is embedded into the JPEG carrier image in the DCT domain in a data-dependent way. Any alteration of the original (certified) image makes the signature no longer corresponding to this image and this change can be quickly identified at the receiver site. Hence, it is called fragile watermarking to differentiate this method from regular watermarking that should present some robustness against image alterations. There is no need to attach any auxiliary signature data, hence the existing, already standardized transmission channels and storage protocols may be used. The embedding procedure requires to remove some part of the original information. But, by using the BATH dataset comprising 32 000 iris images collected for 1 600 distinct eyes, we verify that the proposed alterations have no impact on iris recognition reliability, although statistically significant, small differences in genuine score distributions are observed when the watermark is embedded to both the enrollment and verification iris images. This is a unique evaluation of how the watermark embedding of digital signatures into the ISO CROPPED iris images (during the enrollment, verification or both) influences the reliability of a well-established, commercial iris recognition methodology. Without loss in generality, this approach is targeted to biometric-enabled ID documents that deploy iris data to authenticate the holder of the document.

Key words: biometric data authentication, iris recognition, steganography, watermarking.

1. Introduction

Biometric identification documents constantly gain a higher importance due to increasing security demands in personal authentication. This is especially evident in global trends towards inclusion of biometrics in large-scale authentication processes, like border control (use of e-passports), citizen services (use of biometric national IDs) or various frequent traveler programs (use of biometric-enabled loyalty cards). One of the things to take care of when implementing electronic personal documents is the trust that all system components (sensors, algorithms, transmission channels) originate from a trusted source, e.g., they were certified to be deployed in a given application scenario. It means that only certified biometric equipment should be able to generate genuine biometric samples, and this fact shall be verifiable by the biometric data recipients. A possible solution is to associate some auxiliary information (e.g., digital signature) with the biometric data and transmit this couple through the transmission channels. However, it works only when the channels are flexible and ready for additional data, which is rarely the case. For instance, iris images stored within the smart card must be compliant to ISO/IEC 19794–6 standard that defines iris biometric data exchange format. There is no extra space for authenticity data bounded to the image itself. Thus, the auxiliary information should be "invisible" to existing storage and transmission protocols.

In this paper, a watermarking-based approach is designed for authentication of biometric data [1, 2], i.e., to assure that the data was generated by a certified sensor. Fig. 1 presents a general idea of the proposed methodology. Note that the certification of iris images stored within the document memory (template images) is independent of the certification of devices used when a subject is being verified, i.e., generating verification images. The certification process is also independent of the biometric recognition, as both processes (certification and biometrics) must not interfere with each other.

In contrast to typical watermarking, which should be robust to small alterations in the carrier (for instance, with the aim of removing the watermark), this approach intentionally makes the

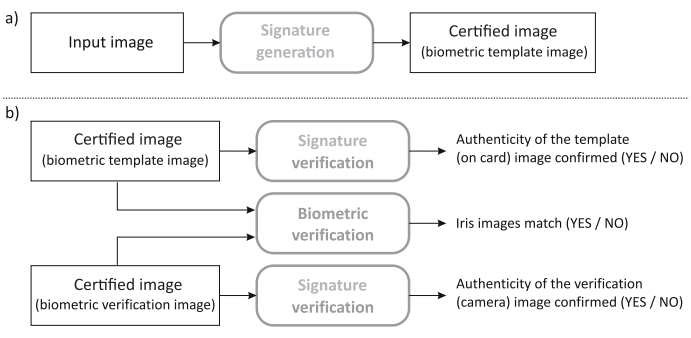

Fig. 1. The use of fragile watermarking for certification of iris images applied in biometric-enabled ID documents: a) signature embedding, b) signature extraction

*e-mail: aczajka@nask.pl

embedded watermark highly different for even tiny alterations in the iris image. Hence, it is further called fragile watermarking to differentiate it from a regular watermarking idea [3]. As the solution requires to use a hidden and undetectable watermark, it may be related to steganography techniques [4].

Since all the necessary information is embedded into the carrier image, no additional data must be stored or transmitted. Hence, this approach should comply with applications using already established rules of biometric data storage and transfer, like ICAO-compliant biometric e-passports[a]. Biometric-enabled identity documents typically allow for automatic face recognition, while travel documents recently include also fingerprints. The iris has been selected as the next candidate for biometric data, mostly due to its impressive reliability and large-scale implementation, such as the NEXUS program [5] operated for more than a decade at the US-Canada border, or UIDAI collecting iris images for more than a billion of citizens in India to generate a unique AADHAAR identification number [6].

The embedded data must be imperceptible to biometrics, i.e., must not interfere with biometric feature extraction and matching procedures. Obviously, from point of view of watermarking technology, the watermark should be undetectable by other users than a trusted one – the biometrics. Thus, the goal of this paper is to design a watermarking-based method, which is suitable for iris image biometrics, and to verify its image authentication ability by conducting experiments with a large data set of iris images that demonstrate a high robustness of an example iris recognition methodology independently of alterations introduced by the message embedding process. A positive verification result means that it is feasible to offer the image (and hence the sensor) certification based on fragile watermarking – a technique that is not affecting the established storage and transmission requirements. According to classification proposed by Bartlow et al. [7], it may also correspond to "asymmetric watermarking", as our approach can ensure image integrity and nonrepudiation of origin.

This paper presents several unique elements when compared to the existing works. First, besides of the original iris images, their cropped versions are also tested, as suggested by ISO [8] for practical implementations of iris recognition methods. Second, the fragile watermarking is applied to the gallery and probe samples independently. This makes it possible to generate four variants of biometric comparisons: the watermarking may be applied at either the enrollment or the verification transactions, at both transactions or at neither of those. Third, one of the largest, publicly available data sets (BATH) is used at the evaluation stage comprising of 32 000 images collected for 1 600 distinct eyes. Fourth, the commercial, well-established iris recognition method (MIRLIN) is employed instead of an open source, academic solutions. It is also worthwhile that the presented approach was implemented in a form of working demonstrator and combined with biometric-enabled, ICAO travel document, what provides a proof-of-concept for theoretical and experimental work presented in the paper.

The paper is organized as follows. Section 2 summarizes recent approaches to iris image certification (including application of steganography, watermarking and PRNU). Section 3 delivers a brief characteristics of the iris recognition process and describes a tool and data set used in this work. In Section 4 it is explained how a unique digital certificate of the image is embedded into the same image and how it is later extracted. Section 5 presents experimental results related to the reliability of the signature embedding method, the uniqueness of generated signatures and the negligible impact of the watermarking alterations onto an iris recognition technique. Advantages and limitations of the proposed approach are discussed in Sec. 6.

2. Past work

Watermarking (and steganography) may co-exist with iris recognition in different combinations and scenarios. Depending on where the biometric data is available, the existing approaches can be roughly categorized into three groups: hiding biometric templates in digital images, digital signing of the biometric samples, and transferring complex biometric data through a single channel (biometric templates embedded into the biometric samples).

The methods of the first group embed biometric templates into some non-biometric data, e.g., third-party digital images. Such embedding processes may have different purposes. They may serve as a proof of intellectual property or allow for image integrity check after transmission. Wang et al. [9] use iris codes and an elliptic curve point embedding technique to achieve a semi-fragile watermark. Their method detects unacceptable image manipulations and simultaneously accepts legitimate manipulations such as lossy compression. In this approach, however, the iris code can be replaced with any other binary string when generating the watermark, since the embedded template is not compared to a newly acquired iris image.

Na et al. [10] propose to use 2D Gabor filtering to generate iris codes, which serve as secrete messages embedded into third-party images by a DCT-based steganographic method. The authors deploy the CASIA v.1.0 dataset of 756 iris images (captured for 108 distinct eyes) and the Lena standard image as the host image to present the robustness of iris code extraction process under selected host image alterations. The authors report little deterioration in the iris code extraction when cropping, compressing and blurring the image holding the embedded code.

Fouad et al. [11] hide the shuffled iris codes into coefficients of the discrete wavelet transform of the host image. To increase robustness of code extraction, the code is embedded multiple times, and the majority voting is applied during code extraction to estimate the true iris code bits. The authors evaluate their approach by applying a series of image deformations (JPEG compression, low-frequency filtering, scaling and rota-

[a]ICAO, the International Civil Aviation Organization, is a United Nations specialized agency developing standards deployed in civil aviation, e.g. related to biometric passport data exchange and storage

tion) prior to extracting the hidden iris code. However, this approach seems to be robust to JPEG compression only, since the iris recognition error rates increase a few times when the remaining alterations are applied.

The approach proposed by Majumder et al. [12] also belongs to this first group, except that instead of typical iris codes, the authors employ gray-scale 8-bit data representing the average of normalized iris image intensity calculated in radial directions. A discrete wavelet transform and singular value decomposition are used to embed and extract the watermark. Authors analyze various deformations (called: attacks) of the host image for a small subset of the BATH database (20 subjects). Assuming that the watermark is correctly extracted for at least 90% of images, the authors achieve 0.4% of false acceptances and 9.8% of false rejections of the detected iris templates.

The methods of the second group embed non-biometric data into biometric samples. Typical aim of the approaches in this group is to authenticate the iris image origin, e.g., the camera used to acquire the data, or to authenticate the image itself, e.g., as a sample originating from a trusted dataset.

Dong et al. [13] is probably the first work which estimates how digital watermarking is affecting the iris recognition accuracy when non-biological data is embedded into iris images. The authors used the ICE v.1.0 dataset (1426 iris images) cropped to a 320×320 resolution, and tested different capacities of the iris image (in terms of strength of embedded information). No significant deterioration is reported when images are affected by moderate watermark strengths, yet for severe embedding (0.98 bit per pixel) the authors report an increase in EER (equal error rate) not more than by 3%. Although the authors applied a (visible) watermarking technique, and not steganography, this pioneering work suggested that iris recognition shows high robustness when embedding non-biological data into the biometrically analysed image.

Lock et al. [14] use seven different watermarking techniques and evaluate their impact onto an iris recognition method (OSIRIS) in two scenarios: the watermark is embedded only at the verification transaction, or the watermark is embedded at both the enrollment and verification transactions. The authors conclude that the fragile watermarking significantly affects the tested iris recognition method when the embedding strength exceeds 0.5 bpp (bit per pixel).

Several steganography algorithms, dedicated for bitmap- or JPEG-images, were evaluated by Wilkowski et al. [15], e.g., JSteg, OutGuess, f5 and STEGIDE, using a face image dataset. Results for different hidden message sizes were obtained, starting from 256 bytes up to 16384 bytes, showing that the distance between the original carrier image and the same image with embedded signature is insignificant when compared to distances between any two original carrier images.

The methods of the third group aim at delivering a multimodal biometric information when a single data transmission channel is used. For instance, transmission of iris images may be enriched with auxiliary liveness detection data, or biometric templates generated for some other biometric mode. Agrawal et al. [16] propose a DCT-based steganography to hide iris codes in face images. The steganography method proposed by the authors reveals some degree of degradation in the embedded message. The experiments performed for 7 different iris codes embedded into 6 different face images demonstrate a lower performance of biometric recognition of the extracted features when compared to the use of original iris codes.

Hammerle-Uhl et al. [17] provide an experimental study of how different watermarking methods influence iris recognition. The authors claim that regular watermarking, that presents some robustness against image alterations, degrades biometric accuracy. This is certainly unsurprising if the embedded message is large enough to prevent from being excluded from an image. In our approach we use small embeddings, when compared to the image size and information capacity, not influencing the iris recognition accuracy, yet carrying full digital signature of the image.

It is worth noting that the biometric data source authentication (e.g., a camera acquiring the iris samples) may be implemented with no watermarking or steganography. Debiasi et al. [18] decided to employ a noise intrinsically embedded by cameras into each acquired image, expressed as photo response non uniformity (PRNU), instead of embedding an extra information into the iris images. This approach has an important advantage of using solely the iris image generated by the sensor – no auxiliary data is embedded into the image. However, a low accuracy of the sensor identification can prevent this approach from real-world practical applications, as the authors report equal error rates as high as 20%, and the ability to achieve perfect PRNU recognition for selected datasets only.

It is also obvious that a lossy image compression (typical in various steganography techniques operating in frequency or wavelet domains) may influence the recognition rates. However, iris recognition seems to be robust for image distortions resulting from image compression, as shown by Daugman et al. [19], Jenisch et al. [20], Rathgeb et al. [21] and Grother et al. [22].

3. Iris recognition

3.1. Brief characteristics. Iris recognition has fascinated the biometric community since 1993, when the first method of iris code extraction was proposed by Daugman [23], and later significantly improved [24] to finally form a *de facto* standard in iris features extraction and matching.

Biology speaks in favor of the iris as biometric characteristics. The iris tissue is a complicated, three-dimensional trabecular meshwork of pectinate ligament and elastic collagenous connective tissue, nerves and blood vessels formed due to highly random morphogenesis, mostly completed by the eight month of the gestation. It offers highly individual features different even for identical twins. Daugman's pioneering idea was related to the test of independence. Namely, assuming high entropy of the random variable representing similarity between different eyes, a failure of the independence test can be used as an oracle for accepting one's identity. Daugman proposed to use two-dimensional Gabor filtering to highlight those individual features of the iris, which are agnostic to deformations and image noise.

Only the phase component of a decomposed iris image is coded to a binary sequence of the same structure and length for every iris image, irrespectively of the iris and pupil size, making the comparison process straightforward and fast. Due to outstanding accuracy and speed of the iris-code-based approach, this idea remains an inspiration for others researchers resulting in coexistence of various Daugman-like solutions deploying different filtering kernels and segmentation techniques, yet still transforming the iris image to the binary code. One of such exemplary tool, used in this work, is shortly presented in the next subsection.

3.2. Iris recognition tool. To evaluate the influence of fragile watermarking processes on the deterioration of iris images, a well established commercial iris recognition methodology is used: MIRLIN (Monro Iris Recognition Library, [25]), which is offered on the market as a Software Development Kit (SDK). It applies the discrete cosine transform calculated for local iris patches to deliver the binary iris code [26, 27]. Similarly to Daugman's approach, the iris codes are compared to each other by calculating the fractional Hamming distance, i.e., a raw Hamming distance normalized by the number of valid iris code bits corresponding to non-occluded iris regions.

Comparison of same-eye images yields close-to-zero fractional Hamming distances, while the distance for two different eyes should oscillate around 0.5 (like in comparison of two sequences of heads and tails obtained in independent coin tosses). Due to rotation compensation that typically is realized by shifting the iris code and finding the best match, the distribution of impostor comparison scores is skewed towards smaller values (about 0.4). The advantage of the MIRLIN SDK is the ability to process all ISO kinds of iris images. Especially, the software performs well for CROPPED images (ISO KIND 3) and hence it is a convenient tool for this research.

3.3. Dataset of iris images. In this work, the BATH-1600 iris image database \cite{BATH} was applied – to our knowledge, still the largest public dataset of iris images. This set consists of two subsets: the main corpus, gathering good quality images (used in this work), and the bad image subset, containing samples that should not be used in iris recognition. The latter samples were added for research purposes, presenting e.g., closed eyes, off-axis gaze, large motion blur, high disruptions due to interlace scanning, etc. Since there is no formal definition of the bad and good quality for BATH samples, it can be only assumed (but not guaranteed) that the images in the main corpus comply with ISO quality requirements [29]. The main corpus consists of 31 990 images acquired for 1 600 irides of 800 distinct persons, hence in almost all cases 20 samples for each eye are available.

The application scenario, followed in this paper, assumes that the fragile watermarking will be deployed to authenticate biometric data stored in personal, electronic biometric documents. It means that the space available for data storage is one of the serious constraints. Typical smart cards used in biometric eID's offer only up to a few hundreds of kB for biometric data storage, with 32 kB being a good estimate of what can be expected in present deployments. Hence, it is clear that raw camera images (of unknown resolution, thus unknown size) cannot be used and a reformatting (including a data compression step) is necessary. ISO proposes a few possibilities to deal with data storage and transmission limitations [8], among which three image formats are important: UNCROPPED (a.k.a. KIND2 or VGA), CROPPED (a.k.a. KIND3) and CROPPED_AND_MASKED (a.k.a. KIND7). UNCROPPED images have a fixed resolution of 640×480 pixels and correspond to the most common resolution offered currently by iris recognition cameras. Two latter formats require an iris segmentation to be done prior to image reformatting, and the JPEG compression is suggested to minimize the final image size. While cropping the image requires only rough position of the iris center and its diameter, to generate the CROPPED_AND_MASKED image one must approximate the pupil, iris and occlusions (to mask and remove elements not used in iris recognition). This format can deliver very compact iris images ($<$ 3 kB), but due to ambiguities in masking procedures, it is suggested to use it only in case of serious storage constraints [30]. On the other hand, the size of UNCROPPED images, even when an image is severely compressed, leads to data files that exceed 32 kB, thus being useless due to eID storage constraints.

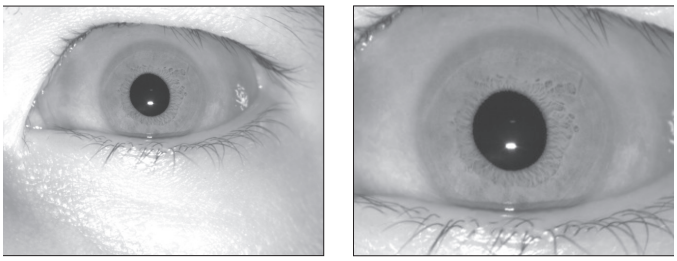

Fig. 2. A sample UNCROPPED iris image (left) and its CROPPED version (right) originating from the BATH database

Hence, in this work, the CROPPED images were considered as biometric data stored within electronic documents, while UNCROPPED images were used to present a reference performance. Since a native image resolution in the BATH dataset equals 1280×960 pixels, the image intensity was averaged within 2×2 pixel quadrants to generate UNCROPPED samples. To build the CROPPED samples, the MIRLIN software was used, as briefed in Sec. 3.2. Due to iris segmentation errors reported by the MIRLIN software, 31 780 CROPPED images were created out of 31 990 samples in total, certainly with no guarantee that the segmentation accuracy was always satisfactory. Sample UNCROPPED and CROPPED images are shown in Fig. 2.

4. Fragile watermarking

4.1. Application context. The primary aim of this work is to provide a method of iris image certification without a need to attach an auxiliary data to the certified iris image. That is, some portion of the original image must be replaced with the

authentication information. To achieve this goal the watermarking embedding is deployed to hide the digital signature and make it invisible for both humans and machines (i.e., iris recognition methods). This embedding process is much more successful (i.e., the hidden message is more difficult to be detected by hostile attackers) when performed in a transformed domain (e.g., frequency domain) than in the original image space. Hence, in this paper the fragile watermarking is applied to JPEG images.

The fragile watermarking approach is not competitive to PRNU-based certification, and can even serve as a supplementary transmission channel for sensor-related properties that generate the PRNU patterns. However, PRNU at its current development stage is difficult to be applied in practice, since accuracy of the PRNU pattern identification is limited (see for instance Debiasi et al. [18] reporting 20% of the equal error rate in recognition of PRNU patterns). The recognition of PRNU-related data should not be confused with biometric recognition, which certainly is not perfect, but needs high accuracy rates in practice.

In the proposed approach, the signature partly depends on the image content and partly on the private key. This yields the security level comparable to that in digital signatures based on public key infrastructure (PKI), which offers a high reliability in verification of the signature. An alteration within the iris image that is stenographically signed will be easily detected at the signature verification stage, as one neither can replace the iris image and retain a valid signature within the modified file (what is guaranteed by the cryptography algorithm [31]), nor generate two different iris images that would result in the same signature (what is experimentally verified in subsection 5.2).

However, one needs also to show that the available data volume in the iris image is more than enough to store hidden information and the inclusion of such authentication information into the carrier does not mislead the biometric identification system. All these issues – the safety and uniqueness of embedded signature, the capacity of iris images and the transparency of embedded signature in biometric identification – are investigated in this work.

4.2. Approach

4.2.1. RSA and JPEG. Prior to presenting the fragile watermarking authentication scheme deployed in this work, let us briefly remind two relevant parts of the embedding procedure: the RSA signature generation scheme [31], and the JPEG image encoding method. The RSA is probably the most commonly used algorithm for digital signature generation. Let a private key key_s is available for signature generation. Driven by the private key, the RSA first generates a public key as a pair of numbers $key_p = (n, e)$, where $n = pq$ is a product of two randomly chosen different prime numbers. The signature s of a message m is generated with the help of a publicly known redundancy function $R(m)$ and the private key, namely

$$s = R(m)^{key_s} \bmod n$$

Verification of the signature s of the message m is performed by comparing a deciphered message (obtained with the use of the public key)

$$m' = R^{-1}(s^e \bmod n)$$

with the original message m.

JPEG is currently the most common standard for static image compression using frequency domain representation. The lossy compression in JPEG consists of the following steps:

1. The RGB image is converted into the YCbCr color space, with a subsampling of chrominance values, e.g., a group of four pixels is encoded by a pair of Cb and Cr chrominance values.
2. Each block of 8×8 pixels is transformed by the discrete cosine transform (DCT) into 64 DCT coefficients, representing different frequency components in horizontal and vertical direction.
3. DCT coefficients are quantized by dividing their quantization table values (followed by rounding).
4. The 'zig-zag' ordered coefficients are run-length encoded by considering the DC and AC values, while the resulting bitstream is entropy-encoded using Huffman coding.

4.2.2. Signature computation and embedding. Let B denotes a sequence of all bits used to code the frequency coefficients $c_1, c_2, \ldots$ calculated for all 8×8 pixel blocks of the host image I. In order to embed a message into the host image, we select two sub-sequences $B_s \subset B$ and $B_e \subset B$ from the sequence of all image bits B, where B_s denotes a sequence of signable bits, and Be denotes a sequence of embeddable bits. Signable bits are used to calculate the signature, and in this approach they are the most significant bits of the frequency coefficients. In turn, embeddable bits are the least significant elements of the frequency coefficients and are used to transfer the watermarking information, i.e., the signature of the iris image. Fig. 3 presents the procedure of how the signature is embedded, and Algorithm 1 specifies the steps of this procedure. Implementations of the elementary functions are the following:

1. `SelectSignComponent()` and `SelectEmbedComponent()`. These functions retrieve sequences of bits B_s and B_e, respectively, from the stream of bits B used to calculate the image signature. The B_s is complementary to and disjoint with B_e, *i.e.,* $B_e \cup B_s = B$. Identical selection of bits must be performed by the encoder and decoder. The simplest way to

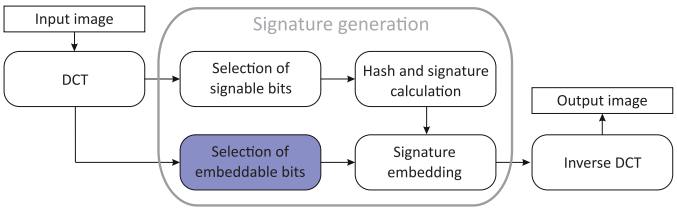

Fig. 3. Illustration of embedding a message (the image signature) into the host iris image

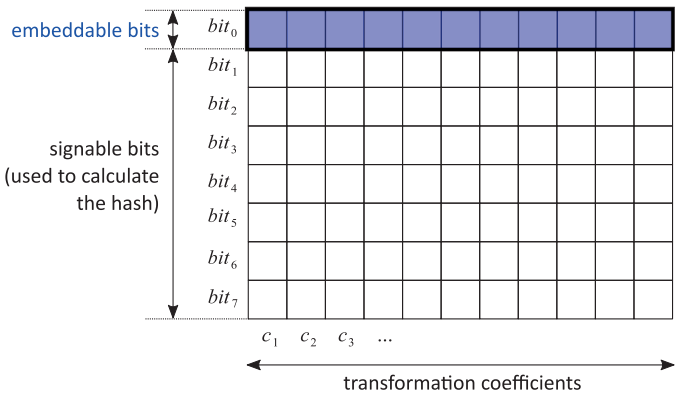

Fig. 4. Selection of bits for signature generation (hash) and embedding

guarantee this is to use the least significant bits for message embedding, while employing the most significant, remaining bits to calculate the signature. Fig. 4 illustrates the selection of bits for a series of DCT coefficients calculated for a single image block of 8×8 pixels. This requires first to select the appropriate DCT coefficients for embedding. The following options are potentially possible:

a) The use of zero-valued DCT coefficients: it provides a large capacity for watermark embedding, but deteriorates the compression rate and leads to image artifacts;

Data:
B – input bit sequence
padding – padding data
key_s – cryptographic private key
Result:
$\tilde{B}$ – output image bit sequence
begin
  $\tilde{B} := \mathsf{Clone}(B)$;
  $\tilde{B}_s := \mathsf{SelectSignComponent}(\tilde{B})$;
  $\tilde{B}_e := \mathsf{SelectEmbedComponent}(\tilde{B})$;
  $H_s = \mathsf{Hashing}(\tilde{B}_s)$;
  $m := [H_s \,|\, padding]$;
  $s := \mathsf{Sign}(m, key_s)$;
  $\mathsf{Embed}(\tilde{B}_e, s)$;
  return $\tilde{B}$
end

Algorithm 1: Embedding a message into the host image

b) The use of the DC-valued DCT coefficients: as the human perception is highly sensitive to low-frequency changes (including the DC value), this kind of embedding is generally useless in steganography and watermarking applications. What is more important, the iris recognition is known to use rather low image frequencies when extracting biometric features. Hence, this embedding may additionally interfere with biometric template creation;

c) Dispersing the embedded information within the entire set of DCT coefficients in a pseudo-random manner (this case is used in this paper): this approach scrambles the information and makes it harder to decipher. Also, this makes it harder to detect and separate the (allegedly non-present) embedded information from image noise by an hostile attacker using statistical analysis.

2. Hashing(). This function employs the SHA-1 method of the RSA to calculate the hash based on *signable* bits. The stream of bits B_s is partitioned into blocks b_1, b_2, …, b_n and a hash function

$$h(b_1, b_2, \ldots, b_n) : \mathscr{B}^{(\aleph)} \rightarrow \mathscr{H}$$

is used, to generate a short digest H_s of B_s. $\mathscr{B}^{(\mathbb{N})}$ is the set of finite sequences with entries in $\mathscr{B}$ and $\mathscr{H}$ is a finite set.

3. Sign(). This function generates the signature s based on an institutional private key key_s. The message m being signed is a concatenation of the SHA-1 hash with a padding data that may contain additional information helpful in image certification (for instance, the ID of the certifying institution).

4. Embed(). This function embeds the signature s into the carrier bit-stream B_e designated for embedding. In this work, two alternative approaches to information embedding were considered. In the first solution, called further SIMPLE, the selected original bits are simply *replaced* by the signature bits. In the second, more complex solution, a specific coding scheme like used in the STEGHIDE algorithm is adopted [32]. The advantage of the latter approach is a preservation of the first-order image statistics. In both cases, the number of least significant bits used for embedding can be freely set. In practice, in order to embed 1024 bits of a message (this length of the signature is chosen in this work), the use of a single LSB plane is sufficient (typically, only part of the least significant bits are utilized).

4.2.3. SIMPLE vs. STEGHIDE approaches. Since two different approaches are considered when embedding the image signature, we briefly provide key characteristics of each of the methods. Let $C = \langle c_1, \ldots, c_N \rangle$ be the sequence of the DCT coefficients calculated for the iris image being signed, where $c_i \in \mathbb{C}$ and $\mathbb{C}$ is the set of possible DCT values. There exists a function v that assigns a value to every sequence element $v : \mathbb{C} \rightarrow \{0, \ldots, u-1\}$. Let us assume that a secret message $s = \{s_1, \ldots, s_n\}$ is embedded, where $s_i \in \{0, \ldots, u-1\}$ is a message element and u is a power of 2 (effectively s_i represents a sequence of bits of constant length). In the SIMPLE method every message chunk s_i is embedded by replacing a predefined embeddable bit by the goal value.

In turn, in the STEGHIDE embedding algorithm the sequence of embeddable coefficients is partitioned into tuples of arbitrary size k (k-tuples). Only one value s_i is embedded into a single k-tuple and at most one embeddable coefficient in a tuple needs to be modified in order to encode an arbitrary value s_i. Now, during embedding, each k-tuple is not directly modified, but an effort is made to find another k-tuple in order to exchange information and to properly encode the embedded message into both tuples. Utilization of k embeddable values per tuple instead of only one decreases the carrier capacity but increases the flexibility in terms of the number of possible exchanges between

tuples. This enables to minimize the carrier image distortions caused by the embedded information.

Thus, the complex version of the Embed() used by STEGHIDE can be envisioned as a graph-search problem. The graph nodes represent k-tuples that require modification, while graph edges represent the possibility of information exchange between tuples, simultaneously satisfying the condition of correct encoding of the digital signature. Certainly, there can be many allowable connections among the graph nodes, Fig. 5 (left). However, after assigning the weights to the graph that correspond to the distortion level introduced by information exchange, it is possible to decide which tuples can, and which cannot exchange the information. The optimized matching of tuple pairs is realized as searching for a maximum decomposition of the graph into connected node pairs, Fig. 5 (right).

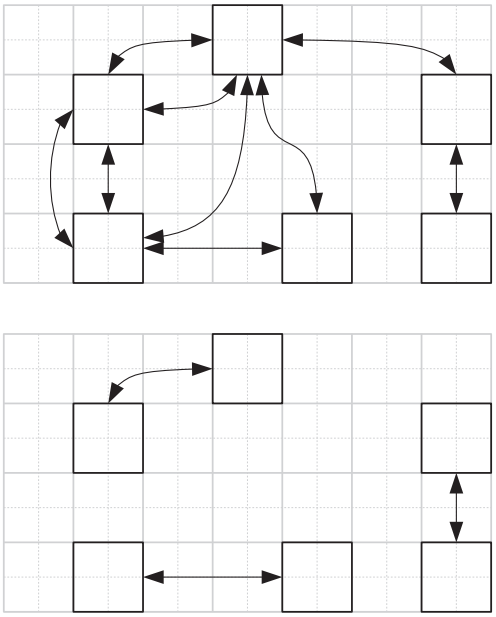

Fig. 5. Illustration of the 4-tuple exchange problem: a sample input graph (left) and the corresponding solution minimizing the distance related to visual differences between the original and the altered image (right)

4.2.4. Signature extraction and verification. The data flow for the opposite procedure of signature extraction and verification is presented in Fig. 6. Assuming that the same image is processed as used in the generation of a signature, the extraction of a hash from the embedded signature (placed in the embeddable bits) and its calculation based on signable bits should yield identical result, i.e., the signature is correct and the image is genuine. If this is not the case, the image was either not certified (there is no valid signature embedded into the image), or it was modified during transmission.

The signature extraction and verification procedure is given by Algorithm 2. First, a digest H_s is computed based on the set of signable bits B_s of the input image. Second, the signature s is extracted from the input image and it is verified whether the

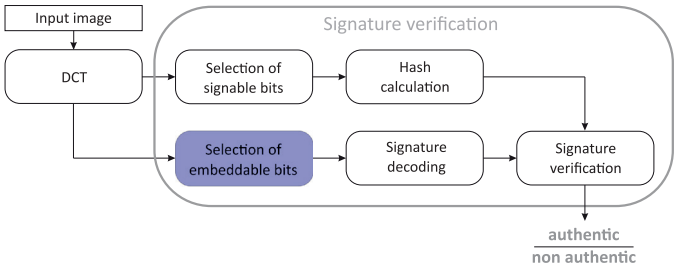

Fig. 6. Signature extraction and verification

Data:
B – input bit sequence
key_p – public key
Result:
r – boolean (*true* if verification is correct, *false* otherwise)
begin
  $B_s :=$ SelectSignComponent(B);
  $B_e :=$ SelectEmbedComponent(B);
  $H_s =$ Hashing(B_s);
  $s :=$ Extract(B_e);
  $r :=$ Verify(H_s, s, key_p);
  return r
end

Algorithm 2: Extraction and verification of the embedded signature

hash used to calculate s is identical to H_s. The implementation of SelectSignComponent(), SelectEmbedComponent() and Hashing() has been already described in Sec. 4.2.2, while the implementation of Extract() and Verify() is the following:

1. Extract(). This function retrieves a signature s from the bit stream B_e designated for embedding. This is performed by simply reading values of the host image bit stream.
2. Verify(). This function verifies whether the calculated digest H_s complies with a signature s stored in the selected bits of the input image. The verification is performed with the use of the RSA algorithm and the public key key_p.

4.2.5. Implementation details. Two approaches of information embedding, namely SIMPLE and STEGHIDE, were implemented in the Java SE environment. Cryptography tools, available in JDK 1.7, in particular the RSA signature generation/verification method, with a 1024-bit key and with the SHA-1 hash function [31, p. 434], were also utilized. The basic encoding/decoding of JPEG files was realized by the following packages: JPEGDecoder (by Helmut Dersch) and JPEGEncoder (by James R. Weeks, with further modifications by Andreas Westfeld).

5. Results

5.1. Comparison of signature embedding methods. Watermarking information always modifies the carrier (host) image, since some portion of the original data must be replaced by

the embedded message. Among two embedding schemes, described in Sec. 4.2.3, SIMPLE is trivial and more prone to attacks when compared to STEGHIDE, hence it is natural to use the latter method. In this subsection, the quality of both methods is observed with regard to a possible deterioration of the iris images originating from the BATH database.

Another JPEG-based, watermarking method, that uses the highly recognized OUTGESS algorithm, is compared with our implementations of the SIMPLE and STEGHIDE algorithms.

The following error measures are used:

- Mean squared error (MSE) and average absolute difference (AAD) computed for a three-component (RGB) color image I as

$$\mathrm{MSE} = \frac{1}{3MN}\sum_{m=1}^{M}\sum_{m=1}^{N}\sum_{k=\{R,G,B\}}\left(I_k(m,n) - I_k^*(m,n)\right)^2$$

$$\mathrm{AAD} = \frac{1}{3MN}\sum_{m=1}^{M}\sum_{m=1}^{N}\sum_{k=\{R,G,B\}}\left|I_k(m,n) - I_k^*(m,n)\right|$$

  where I^* is the iris image with embedded signature, I is the original (unaltered) iris image, $M = 640$ and $N = 480$.
- maximum absolute difference (MAD) defined as

$$\mathrm{MAD} = \max_{m,n,k}|I_k(m,n)|$$

  where $m = 1, \ldots, M = 640$, $n = 1, \ldots, N = 480$, and $k = \{R, G, B\}$.
- peak signal-to-noise ratio (PSNR) computed as

$$\mathrm{PSNR} = 10\log_{10}\frac{\mathrm{MAX}^2}{\mathrm{MSE}}$$

  where MAX = 255 and it is the maximum possible value of a pixel component (red, green or blue).
- relation MAD/MAX, which describes the fraction of the maximum possible pixel value corresponding to the MAD value.

Table 1 presents the amount of noise evaluated by the above measures, when 1024-bit messages are embedded into iris images. STEGHIDE approach performs best, while OUTGUESS gives a similar noise level. SIMPLE performs only slightly worse as the former two, as it mainly suffers from occasional noise peaks (expressed by higher *MAD*/*MAX*). One concludes that the storage space available in typical iris images is more than enough for embedding a signature and this embedding leads to a rather insignificant increase of the noise level for all three tested methods. Thus, the selection of the STEGHIDE scheme for further extensive experiments can be seen as an optimal choice.

Table 1
Comparison of noise levels introduced by embedding 1024-bit messages into iris images of resolution 640×480

Algorithm	PSNR [dB]	MSE	AAD	MAD/MAX (%)
SIMPLE	**51.33**	**0.479**	**0.327**	**1.57**
STEGHIDE	**51.52**	**0.458**	**0.313**	**1.18**
OUTGUESS	51.35	0.476	0.326	1.18

5.2. Uniqueness of signatures. An important question, related to the evaluation of the presented approach, deals with the uniqueness of the image digests generated by the hashing function for different images, but of the same type (*i.e.,* iris images). In particular, let us evaluate the number of different bits in every two digests generated for different iris images. In other words, can identical or very similar digests be generated for the CROPPED BATH images? On the one hand, the cryptography theory suggests that the probability of getting identical or very similar digests is close to zero. On the other hand, we operate on a very specific and narrow image type (standardized iris images).

The results obtained for digests generated for CROPPED iris images, originated from the BATH database, are shown in Tab. 2. An average number of disagreeing bits, observed for 31 990 CROPPED images, equals to 49.9%, where the minimum value is 41.25% (66 out of 160) and the maximum value is 57.5% (92 out of 160). Speaking in bit units, in the performed experiments, two digests differed at least on 66 bits for a total number of 160 bits, what makes it difficult to obtain identical (or even close) digests. When counting the difference of half-bytes, two digests differed at least on 34 half-bytes out of 40. The observation at the level of bytes shows that always 19 or 20 bytes were different. Thus, one can conclude that the generated digests are sufficiently unique to avoid unintentional mistakes in image certification in practice.

Table 2
Distances between digests (of length equal to 160 bits) obtained for CROPPED iris images originated from the BATH database

Distance (d), **where** d = number of different:	**Min**	**Max**	**Mean**	**Max possible**
bits	66	92	79.8	**160**
halfbytes	34	40	37.4	**40**
bytes	19	20	19.9	**20**

In general, the signature generation does not need to be bounded to the RSA tool. If available in the future, other cryptographic systems can be applied, taking advantage of new developed theory and algorithms [4, 33].

5.3. Selection of JPEG compression level. Since the fragile watermarking method employs a JPG compression, one needs to set the compression (or quality) level, applied to CROPPED images, controlled by the JPG-Q parameter in the JPG encoder. In this work, a real biometric ID card prototype is used, which offers 32kB of storage for iris images in the ICAO-compliant DG4 container. Since iris recognition can work correctly for a single eye (either left or right), our experiments lead to the

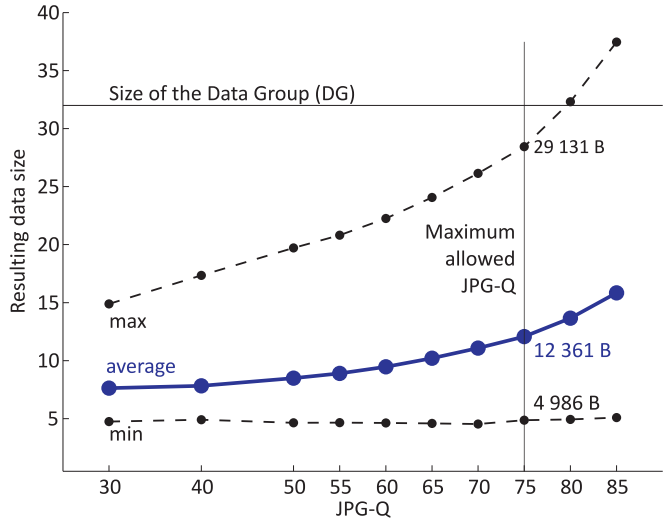

Fig. 7. Size of the CROPPED iris image with embedded signature versus the setting of compression/quality parameter JPG-Q. Solid line shows the average size, while dashed lines present the extreme values obtained for all BATH images processed to CROPPED format

conclusion, that setting the JPG-Q parameter to 75 guarantees that at least one cropped iris image can be stored within a card with 32 kB of memory available for iris data, Fig. 7.

Additionally, the effectiveness of fragile watermarking embedding applied to the CROPPED images was checked for different quality (and hence compression) levels, in particular for JPG-Q = 75. In order not to have a bias resulting from identical cryptography processing, for each BATH image with no segmentation errors reported by the MIRLIN SDK, a new, randomly generated 1024-bit key was used. Figure 8 shows that the number of unsuccessful embeddings has a logarithmic nature as a function of JPG-Q, and starts to be unacceptable for JPG-Q values less than 40 (when the error rate exceeds 10% of

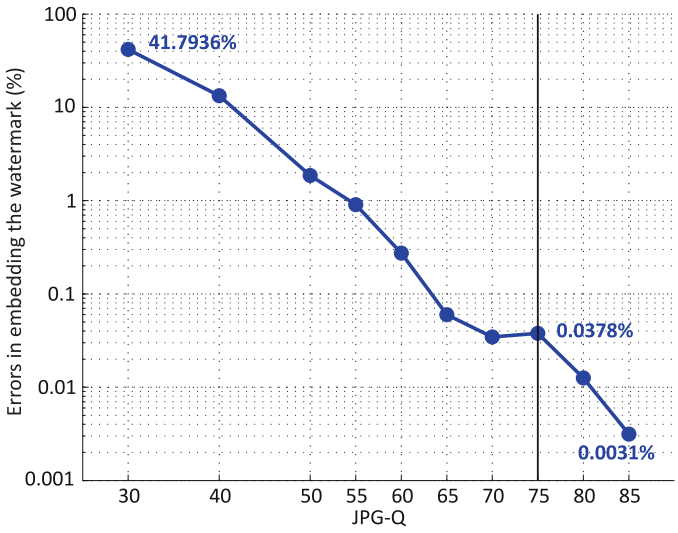

Fig. 8. Percentage of unsuccessful signatures generated by the STEGHIDE method for segmented, CROPPED iris images

images being rejected). It means that the applied watermarking method is sensitive to high compression levels. The maximum quality, for JPG-Q = 75, results in about 0.038% of unsuccessful signatures. After visual inspection we found that this error rate is caused by only 11 images (outside of those 31 780 samples for which MIRLIN did not report segmentation errors). Those 11 samples were wrongly segmented due to MIRLIN mistakes and the resulting CROPPED images were too small to perform the watermarking processes. These images would not pass a quality check implemented according to ISO/IEC 29794–6 [29]. Hence, the value JPG-Q = 75 is set as a final value in all further experiments.

5.4. Biometric performance for watermarked iris images

5.4.1. Scenarios. Four scenarios considered in this work (and possible to be applied in a real operational environment) are as follows:

s_1: neither the template image stored in the document memory, nor the verification images generated by the iris capture device are certified,

s_2: the template image is signed, but not the verification images,

s_3: opposite to s_2, *i.e.,* the template image is not certified, but the verification images are signed,

s_4: both the template and verification images contain the signature.

Note that there is no fragile watermarking employed in the scenario s_1, yet still the JPEG compression may be applied on both sides (document and camera). Hence, this scenario is used as a reference when evaluating the solutions using fragile watermarking.

5.4.2. Generation of comparisons and error estimators. The iris recognition method presented briefly in Sec. 3.2 was applied to all UNCROPPED and CROPPED images generated for the BATH samples (cf. Sec. 3.3) and finally the biometric reliability was evaluated in all four scenarios listed in Sec. 5.4.1. Each scenario may have a few implementation options (depending on the usage of compression and image cropping). One of these options, denoted as o_1 in each scenario, represents the basic, intended application of a given scenario in a biometric ID document system. The following paragraphs detail all the realized experiments for all considered options. When JPEG compression is mentioned, it means that the image was compressed and the JPG-Q quality was set to 75. To present the iris recognition accuracy under all options in four scenarios, standard biometric error point estimators are used, namely:

- FNMR (false non-match rate) is the percentage of images that have been mistakenly said to not match when they should be accepted, related to the number of all genuine (same-eye) attempts in the experiment,
- FMR (false match rate) is the percentage of images that have been mistakenly said to match when they should be rejected, related to the number of all impostor (different-eye) attempts.

Both FNMR and FMR are functions of the decision threshold, and their possible values range from 0 to 1 (or from 0 to 100% at the percentage scale). To calculate both error rates

the comparisons were planned very carefully so as to obtain as much independent comparison results as it is possible to be entitled to apply a statistical analysis of the results. Consequently, the set of 800 subjects in BATH dataset was divided into two disjoint subsets, each gathering samples acquired for 400 different persons. Since some dependency between left and right eyes has been already reported in the scientific literature, for each person only one eye (either left or right) was selected and the samples of the selected eye were used in matching. Next, for each eye three samples (out of 20 available) were randomly selected: two of them were used to generate genuine match scores, and the remaining one was used in impostor matching. Calculating the genuine scores for all 800 distinct eyes yielded 800 statistically independent genuine scores. To generate impostor scores, the templates from the first disjoint set of 400 eyes were selected, and matched with images of the second disjoint set of 400 eyes. The latter process yields 400 statistically independent impostor scores. The above procedure (i.e., rejecting the remaining 17 images of each eye) provides the largest possible set of statistically independent comparison scores. Adding additional comparison pair diminishes the independence (and hence makes the statistical assessment less significant).

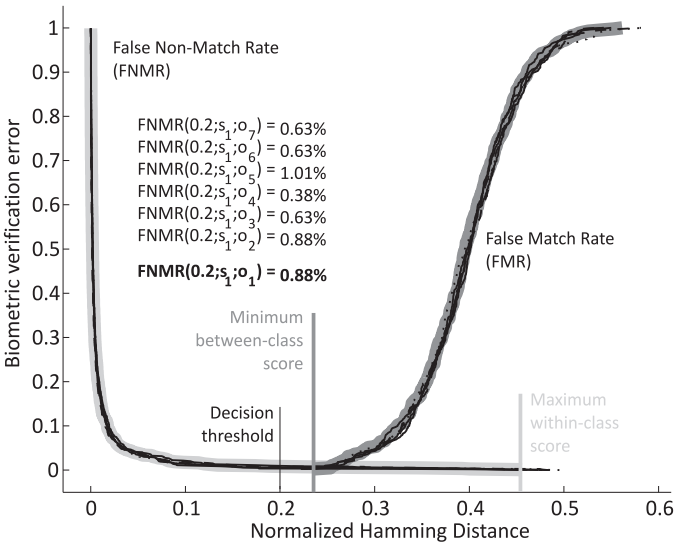

Fig. 9. The FMR and FNMR functions vs. the decision threshold (fractional Hamming distance) for all seven options in the first scenario (s_1). The base option o_1 results are is marked by thick gray lines, while the remaining options are shown as thin black lines. The selected decision threshold (HD = 0.2), guarantying the FMR = 0 in all experiments, is also presented. The FNMR(0.2) values are given for all options – the result for the base option o_1 is shown in bold

5.4.3. Results for Scenario 1. In the first, reference scenario (s1) the fragile watermarking is not used, while the compression or cropping still can be applied on both sites (enrollment to the biometric ID card, and verification). The following options are considered:

o1: enrollment: CROPPED images + JPG compression; verification: CROPPED and not compressed images,
o2: enrollment and verification use UNCROPPED and not compressed images,
o3: enrollment and verification use CROPPED and not compressed images,
o4: enrollment: CROPPED and not compressed images; verification: compressed CROPPED images,
o5: enrollment: CROPPED images + JPG compression; verification: UNCROPPED and not compressed images,
o6: enrollment: UNCROPPED images; verification: CROPPED images + JPG compression,
o7: enrollment and verification use CROPPED and compressed images.

Option o_1 realizes the basic combination of cropping and compression when neither the data on card, nor the verification images are signed. Option o_2 is a reference point when no compression and cropping are used. Figure 9 shows that the influence of the applied compression and image cropping on the iris recognition accuracy is marginal, since the FNMR (with the decision threshold equal to 0.2) presents similar values for all options. The conclusion may be even opposite, since comparing options o_1 and o_5 we may observe an increase in the accuracy once the image is CROPPED. This can be explained by a smaller area that must be searched for the iris when the image is being segmented.

In this scenario, comparisons between options o_3–o_7 and the option o_2 are particularly interesting, since they answer if cropping, compressing, or both processes at once applied on either site can impact the iris recognition. Two-sample, two-sided Kolmogorov-Smirnov test was applied to compare genuine and impostor scores calculated in the reference option o_2 and remaining options o_3–o_7. The null hypothesis is that scores in the reference and tested option are from the same distribution. The alternative hypothesis is that these scores are from different distributions. We get statistically insignificant difference when comparing genuine scores in options o_2 and o_3 (p-*value* = 0.89), that is image cropping has no effect on comparison score calculation. In the remaining combinations between o_2 and o_4–o_7 the null hypothesis was rejected (p-*value* $<$ 0.025). This means that compression used in our approach introduces small, but statistically significant differences in FNMR. In turn, KS test applied to impostors scores among options o_3–o_7 and the option o_2 returns p-*value* $\in (0.53; 0.98)$, what concludes as no statistically significant differences in impostor scores after application of JPEG compression.

5.4.4. Results for Scenario 2. In the second scenario (s2) the fragile watermarking is added at the enrollment site. The following two options are considered in this case:

o1: enrollment: CROPPED images + JPG compression + signature; verification: CROPPED and not compressed images,
o2: enrollment: CROPPED images + JPG compression + signature; verification: UNCROPPED and not compressed images.

Option o_1 presents the basic combination of cropping, compression and use of fragile watermarking in this scenario, when

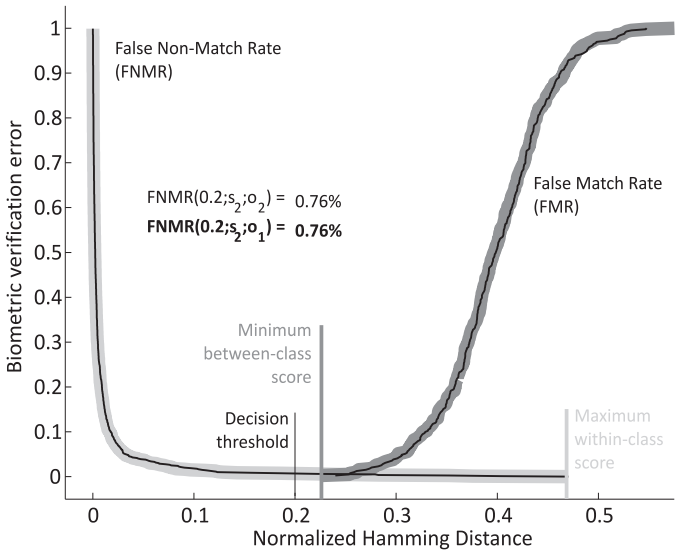

Fig. 10. Same as in Fig. 9, except that results for the second scenario s_2 are shown.

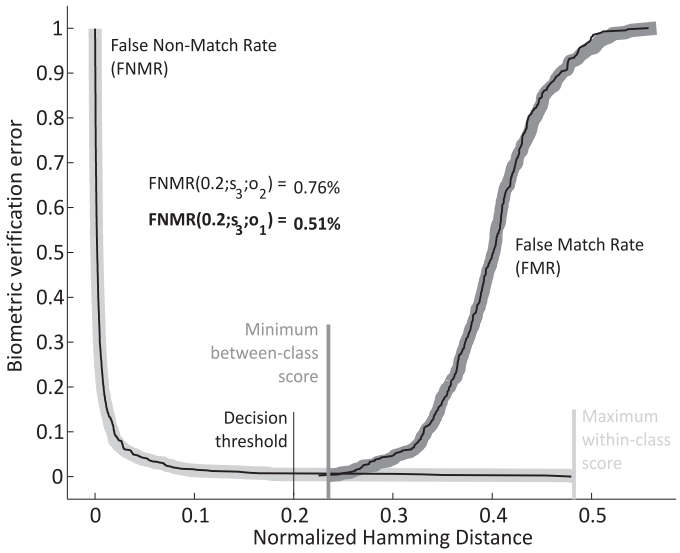

Fig. 11. Same as in Fig. 9, except that the results for the third scenario s_3 are shown.

only biometric data stored on the card are signed, and not the verification iris images. Figure 10 shows that there is no real difference between these two options. Even a little increase of accuracy is observed when compared to the base option o_1 of the first scenario s_1. It means that the digital signatures may be safely embedded into the enrollment data with no loss in iris recognition accuracy.

As in the first scenario, the KS test was applied and the following *p*-values were obtained: 0.2 for genuine and 0.99 for impostor scores distributions. This suggests that observed differences between options are statistically insignificant both in case of genuine and impostor scores.

5.4.5. Results for Scenario 3. The third scenario s_3 switches the usage of fragile watermarking with the scenario s_2. Namely, the signatures are embedded at the verification site only (and not when the subject is being enrolled). Again, two options in this scenario can be generated:

o_1: enrollment: CROPPED and not compressed images; verification: CROPPED images + JPG compression + signature;

o2: enrollment: UNCROPPED and not compressed images; verification: CROPPED images + JPG compression + signature.

As in the first two scenarios, the first option o_1 represents the basic combination of cropping, compression and use of fragile watermarking. Figure 11 illustrates that it is safe to embed the signature into the verification image generated by the certified iris camera. Similarly to the results in the first scenario, we may observe slightly better accuracy for CROPPED images when compared to results obtained for their UNCROPPED original images.

Application of KS test returns the following *p*-values when comparing the above two options: 0.49 for genuine scores and 0.91 for impostor scores. Again, no statistically significant differences between distributions in these two options can be observed.

5.4.6. Results for Scenario 4. In the last, and the most interesting fourth scenario s_4, both the on-card images and the verification images are certified. One basic option in this scenario is analyzed, namely both the enrollment and verification images are CROPPED, compressed and signed. Other options are not generated since the applied fragile watermarking method must be accompanied by image compression, while UNCROPPED images are not used for certification. Figure 12 illustrates quite identical FNMR(0.2) values as obtained for the base option o_1 of the third scenario s_3. They are even slightly better than results

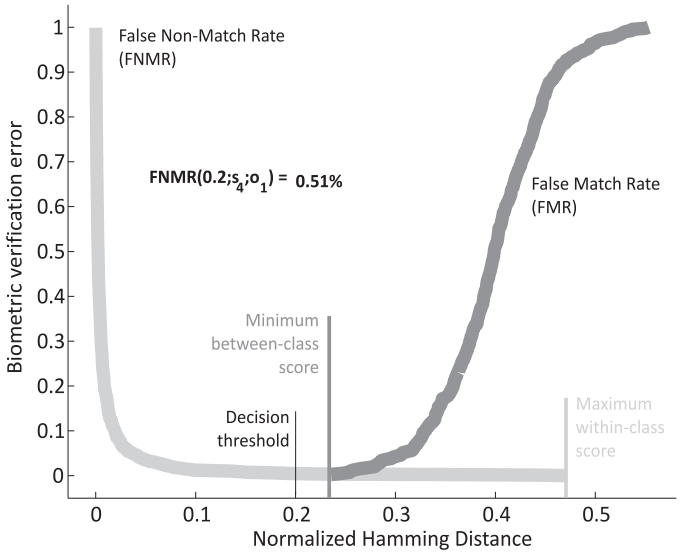

Fig. 12. Same as in Fig. 9, except that the results for the fourth scenario (s_4) are shown.

for the option o_7 in the first scenario s_1 (when CROPPED and compressed images are used at both sites, yet no watermarking is used). Differences in the FNMR are small, and they have rather a noisy character.

5.4.7. Comparison of scenarios. Finally, the KS test was applied for all four basic options o_1 defined in all four scenarios s_1 – s_4. All possible option pairs were compared (excluding self-comparisons s_k vs s_k). No statistically significant differences were observed in impostor scores for all possible scenario pairs (p-*value* $\in (0.61; 0.99)$). Also, there are no statistically significant differences in genuine scores where scenarios s_1 vs s_2, s_1 vs s_3, and s_2 vs s_3 are compared (p-*value* $\in (0.94; 0.99)$). However, results obtained in the scenario s_4 reveal statistically significant differences in genuine scores when compared to the remaining scenarios s_1, s_2 and s_3 (p-*value* $\in (0.006; 0.023)$). It means that application of fragile watermarking to both the enrollment and verification images introduces small, yet statistically significant differences in genuine score distributions.

6. Conclusions

We investigated the possibility to offer a secure and accurate iris image certification mechanism without the need of adding auxiliary data apart from the iris image itself. The proposed solution is not affecting (requires no change of) the existing transmission channels and storage means. Due to anticipated robustness of the iris recognition to some alterations in the biometric samples, a watermarking technique was adopted to hide a digital signature of the iris image within the same file, which is used further in biometric processing. The hidden signature is partially based on the iris data and results from the well-known RSA algorithm to ensure a cryptographically strong authentication of the certified image.

The adopted JPEG-based watermarking method utilizes most significant DCT components and a private key to generate and embed the signature. It integrates the signature seamlessly with the image by removing some less significant DCT components. This certainly generates the risk of image modifications that may prevent the biometric systems from accurate identity recognition. But the presented results clearly show that this hypothesis is not valid, at least for a dataset of 32000 iris images collected for 1600 distinct eyes, regardless of the place where the watermarking is applied (at the enrollment site only, during the verification only, or on both sites). The approach presented in this paper has also its implementation in a form of a demonstrator software and hardware incorporating the ICAO-compliant, biometric travel document, providing a proof-of-concept for theory and experiments presented in this paper.

One should be also aware of some limitations of this work. First, a signature of a fixed length was applied, hence the deterioration of the biometric performance as a function of the embedded message is unknown. Second, only one (yet well-established) iris recognition system was used to check the performance achieved for the altered images. There is thus a question if other biometric systems, using other image filtering and segmentation algorithms than the tested system, would be also robust to watermarking alterations. These doubts however generate interesting areas of further research.

Acknowledgements. This research was funded by NCBiR Agency, Warsaw, under BioPKI project, grant number O ROB 0027 01/ID 27/2. The manuscript preparation was supported by statutory funds of the author's home institutions (NASK and WUT).

References

[1] Digital Watermarking Alliance, home page: http://www.digitalwatermarkingalliance.org, (accessed April 15, 2016).

[2] P. Lipiński, "Watermarking software in practical applications", *Bull. Pol. Ac.: Tech.* 59 (1) 21–25 (2011).

[3] E. T .Lin, E. J. Delp, "A review of fragile image watermarks", *Proceedings of the Multimedia and SecurityWorkshop at ACM Multimedia*, 35-39 (1999).

[4] J. Blackledge, *Cryptography and Steganography: New Algorithms and Applications*, Center for Advanced Studies, WUT (2011).

[5] U.S. Customs and Border Protection, NEXUS Program: http://www.cbp.gov/travel/trusted-traveler- programs/nexus (accessed April 15, 2016).

[6] Unique Identification Authority of India, AADHAAR: https://uidai.gov.in (accessed April 15, 2016).

[7] N. Bartlow, N. Kalka, B. Cukic, A. Ross, "Iris digital watermarking" in: *Encyclopedia of Biometrics*, Springer US, Boston, MA, 778–787 (2009)

[8] ISO/IEC 19794-6, "Information technology – Biometric data interchange formats – Part 6: Iris image data". Final Draft International Standard (FDIS) (2011).

[9] M. Wang, K. Fan, X. Li, Q. Zeng, "A novel digital content protection scheme combining iris identity based digital signature and semi-fragile watermark", *International Conference on Communication Technology ICCT*, 1–4 (2006)

[10] W. Na, Z. Chiya, L. Xia, W. Yunjin, "Enhancing iris-feature security with steganography", *5th IEEE Conference on Industrial Electronics and Applications*, 2233–2237 (2010)

[11] M. Fouad, A. El Saddik, E. Petriu, "Combining DWT and LSB watermarking to secure revocable iris templates", *10th International Conference on Information Sciences Signal Processing and their Applications*, 25–28 (2010).

[12] S. Majumder, K. J. Devi, S. K. Sarkar, "Singular value decomposition and wavelet-based iris biometric watermarking", *IET Biometrics* 2 (6) 21–27, (2013).

[13] J. Dong, T. Tan, "Effects of watermarking on iris recognition performance", *10th International Conference on Control, Automation, Robotics and Vision*, 1156–1161 (2008)

[14] A. Lock, A. Allen, "Effects of reversible watermarking on iris recognition performance", *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, 8 (4) 574 – 579 (2014).

[15] A. Wilkowski, W. Kasprzak, "Steganographic authentication method for electronic IDs", Image Analysis and Recognition (ICIAR), *Lecture Notes in Computer Science*, Springer-Verlag Berlin-Heidelberg, 7950 726–733 (2013).

[16] N. Agrawal, M. Savvides, "Biometric data hiding: A 3 factor authentication approach to verify identity with a single image using steganography, encryption and matching", *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, 85–92 (2009).

[17] J. Hämmerle-Uhl, K. Raab, A. Uhl, "Experimental study on the impact of robust watermarking on iris recognition accuracy", *The ACM Symposium on Applied Computing*, New York, 1479–1484 (2010).

[18] L. Debiasi, A. Uhl, Z. Sun, "Generation of iris sensor PRNU fingerprints from uncorrelated data", *International Workshop on Biometrics and Forensics (IWBF)*, 1–6 (2014).

[19] J. Daugman, C. Downing, "Effect of severe image compression on iris recognition performance", *IEEE Transactions on Information Forensics and Security* 3 (1) 52–61 (2008).

[20] S. Jenisch, S. Lukesch, A. Uhl, "Comparison of compression algorithms' impact on iris recognition accuracy II: revisiting JPEG", *Proceedings of SPIE, Security, Forensics, Steganography, and Watermarking of Multimedia Contents*, 68190M– 68190M–9 (2008).

[21] C. Rathgeb, A. Uhl, P. Wild, "Evaluating the impact of iris image compression on segmentation and recognition accuracy", Tech. Rep. 2012-05, Dept. of Computer Sciences, University of Salzburg, Salzburg, Austria, http://www.cosy.sbg.ac.at/research/tr.html (2012).

[22] P. Grother, E. Tabassi, G. W. Quinn, W. Salamon, "IREX I: Performance of iris recognition algorithms on standard images", NIST Interagency Tech. Rep. 7629, Information Access Division, National Institute of Standards and Technology, http://www.nist.gov/itl/iad/ig/irexi.cfm (2009).

[23] J. Daugman, "High confidence visual recognition of persons by a test of statistical independence", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 15 (11), 1148–1161 (1993).

[24] J. Daugman, "New methods in iris recognition", *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 37 (5), 1167–1175 (2007).

[25] FotoNation UK Limited (formerly: SmartSensors Limited), Monro Iris Recognition Library and INterface (MIRLIN SDK), http://www.fotonation.com/Technologies/Biometrics/ Iris_Recognition.aspx (accessed on Aug. 25, 2015).

[26] D. M. Monro, S. Rakshit, D. Zhang, "DCT-based iris recognition", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29 (04), 586–595 (2007).

[27] D. M. Monro, S. Rakshit, D. Zhang, "Correction to: DCT-based iris recognition", *IEEE Transactions on Pattern Analysis and Machine Intelligence* 29 (09) 2, (2007).

[28] SmartSensors Limited, BATH University Iris Database (1600 classes), http://www.smartsensors.co.uk/irisweb (accessed on Aug. 25, 2015).

[29] ISO/IEC 29794-6, "Information technology – Biometric sample quality – Part 6: Iris image data". Final Draft International Standard (FDIS) (2014).

[30] G. W. Quinn, P. Grother, E. Tabassi, "Standard iris storage formats", *Handbook of Iris Recognition*, Springer London, 55–66 (2013).

[31] A. J. Menezes, S. A. Vanstone, P. C. V. Oorschot, *Handbook of Applied Cryptography*, 1st Edition, CRC Press, Inc., Boca Raton (1996).

[32] S. Hetzl, P. Mutzel, "A graph-theoretic approach to steganography", *Proceedings of the 9th IFIP TC-6 TC-11 international conference on Communications and Multimedia Security (CMS),* Springer-Verlag, Berlin, Heidelberg, 119–128 (2005).

[33] T. Adamski, W. Nowakowski, "The average time complexity of probabilistic algorithms for finding generators in finite cyclic groups", *Bull. Pol. Ac.: Tech.* 63 (4) 989–996 (2015).