IET Image Processing

Research Article

IET Journals
The Institution of Engineering and Technology

Incorporating iris, fingerprint and face biometric for fraud prevention in e-passports using fuzzy vault

ISSN 1751-9659
Received on 17th January 2019
Revised 1st July 2019
Accepted on 29th July 2019
E-First on 23rd October 2019
doi: 10.1049/iet-ipr.2019.0072
www.ietdl.org

Katarzyna Bobkowska[1], Khaled Nagaty[2] ✉, Marek Przyborski[1]

[1]*Department of Geodesy, Faculty of Civil and Environmental Engineering, Gdansk University of Technology, Gdansk, Poland*
[2]*Computer Science Department, Faculty of Informatics and Computer Science, The British University in Egypt, Cairo, Egypt*
✉ *E-mail: khaled.nagaty@bue.edu.eg*

Abstract: A unified framework which provides a higher security level to e-passports is proposed. This framework integrates face, iris and fingerprint images. It involves three layers of security: the first layer maps a biometric image to another biometric image which is called biostego image. Three mapping schemes are proposed: the first scheme maps single biometric image to single biostego image, the second scheme maps dual biometric images to single biostego image, the third scheme divides the biometric image into sections and maps each section to different biostego image. A mapping function maps the intensity value of each pixel in the biometric image to pixels with same intensity in the biostego image. A representative pixel is randomly selected from the set of pixels, and its coordinates are recorded in the location map of the biometric image. In the second layer, the location map is encoded using fingerprint fuzzy vault. In the third layer, the encoded location map is hidden in the biostego image using steganography technique. The biostego image which contains the encoded location map is stored in the e-passport's memory. Keeping the mapping scheme secret and by using the fingerprints fuzzy vault to encrypt location map, the proposed approach provides higher level of protection against fraud.

1 Introduction

Borders of countries are the first line of defence against terrorists. However, terrorists' countermeasures should not disturb or confuse ordinary passengers. This is a big challenge for developing effective, fast and hacker proof system of border control. Nowadays, e-passports and e-IDs are able to store more information than they were in ordinary so-called 'paper versions'. These documents may also store biometric data such as images of faces, fingerprints or iris scans. More than 100 countries are currently using e-passports in the workplaces. These kinds of documents are assumed to be the most reliable identification methods because they are based on biometric characteristics of an individual which make the individual unique and therefore can be used for identification and authentication [1–3]. Security system, based on the method 'what we are' or 'how we behave' is more secure than using method of 'what we own' such as keys or 'what we know' such as passwords or PIN codes which are created and kept by the users. Passwords and PIN codes are susceptible for attempts of hacking using brute force to crack the password. A biometric identification system uses the individual's body as passwords or PIN codes. The most earlier biometrics used for person identification are fingerprints and handwritings but recently advanced biometrics such as iris, face, voice-print and palm prints are used for identity recognition and verification. Special devices are used to read the biometric features stored in the e-passport's chip and match them against features stored in biometric identity database. However, fingerprints and iris require cooperation from the traveller to provide his biometric data to the inspection terminal. Common biometrics has different challenges that can affect their performance in identifying individuals:

- Dirt, wetness and wearing of the skin affect the performance of fingerprints as biometric.
- Presence of glasses adversely affects using retina as biometric.
- Low light and movement when scanning an individual's iris reduce the effectiveness of this biometric.
- Scarring, skin changes due to age [4] and jewellery can cause problems with hand geometry biometric.
- Changes in age, scars, glasses, hairstyle and lighting affect using face as biometric [5].
- Variations in writing from day to day can change a person's handwriting and affect using this biometric [6].

In the following sections, the details of biometric mapping schemes are described. A biometric mapping function as a means to secure data stored in e-passports is proposed. The authors are aware of the limitation of the least significant bit (LSB) method used; however the main assumption of presented work is to keep things as simple as possible as the proposed schemes are independent of the stenography technique used. Therefore, using methods that are better than LSB and testing their efficiency is possible.

2 Related work

In 1998, a first generation of e-passports appeared where a fingerprint image was embedded into the chip of Malaysian passports. In 2003, a second generation of e-passports appeared which contained extracted fingerprints information only. When passing through international airports the automated gate reads the fingerprint's information from the chip and matches it with the fingerprint acquired by scanner [7]. Pattinson in [8] outlined the privacy problems of e-passports that may be readable by anyone and argued for basic access control (BAC). He pointed out the importance for a direct link between optically scanned card data and the secret key embedded in an e-passport. Jacobs in [9] discussed the need for BAC and investigated the issues surrounding a national database of biometric identifiers. In [10], the EU added an extra protection mechanism which was known as extended access control (EAC). The EAC includes a Diffie–Hellman key agreement and a reader which must first authenticate itself to the e-passport chip. In [11], the authors described a new biometric passport with wireless contact possibility. No information is released without the approval of e-passport holders. In the proposed approach, the fingerprints fuzzy vault scheme protects the privacy of the information where an e-passport holder has to physically submit his/her fingerprint to enable access to the e-passport chip. In the e-passport presented in [11], the owner's face is stored in the passport chip with some local features, such as

© The Institution of Engineering and Technology 2019

position of the eyes, nose and so on, and if fingerprints are used they are stored as compressed images. Mohamed Abid in [12] proposed an authentication technique for e-passports that was based on iris biometric and elliptic curve cryptography. A cryptographic key regeneration scheme that is based on iris biometric was used to obtain a stable input from the biometric data in order to generate the security parameters of the elliptic curve. In 2011, Herve Chabann in [13] employed the elliptic curve cryptography to protect e-passports. All the above approaches protect e-passports by either using biometric data with cryptography or cryptography alone, namely the elliptic curve cryptography. Although steganography can provide an extra level of protection for e-passports, it is not employed in the above approaches. In [14], Bhagya Wimalasiri *et al.* proposed a novel multi-stage authentication scheme that incorporates verification of data stored inside the radio frequency identification (RFID) tag, watermarking, facial and signature authentication for e-passports. In the proposed framework, biometrics, steganography and cryptography are all integrated to add extra level of security to the e-passports. Many concerns are raised regarding individuals' interaction with biometrics scanners, for example about hygiene with touching fingerprint devices or health risks for more recent biometrics methods such as iris or retina scanning. Complaints are raised against hand geometry systems as users claim that they dry their hands. Concerns are raised against retinal systems regarding the risk that retinal scanning devices would damage their vision with extended use over time. For those limitations and above-mentioned challenges, no single biometric modality is sufficiently robust and accurate to be used independently for authorisation in real-world applications which require high security checks such as border control. Any biometric modality for authorisation will become more powerful when used in conjunction with other biometric modalities for authorisation such as face, iris or fingerprints which own unique features that can be extracted quickly during the identification process to accurately identify a person [15]. The presented paper proposes a unified framework to prevent e-fraud in e-passports. This framework integrates biometric mapping schemes: single mapping, dual mapping and distributive mapping schemes with the LSB steganography technique and fingerprints fuzzy vault. A biometric mapping scheme generates location maps by mapping biometric image to host biometric image which is called the biostego modality or biostego image. The generated location map is then encoded using the fingerprints fuzzy vault algorithm before being hidden in the biostego image using steganography technique. In this work, we use the LSB steganography algorithm because it is simple and more suitable for the proposed approach, although more sophisticated steganography methods can be used as the proposed mapping schemes are independent of the steganography techniques. Finally, the biostego image which contains the hidden encoded location map is stored in the memory chip of the e-passport. This approach fulfils three goals: confidentiality protection, storage capacity reduction and increasing overall identification performance. Confidentiality of the biometric information stored in the e-passport's memory is achieved using the fingerprints fuzzy vault. Protection of the e-passport against fraud is achieved by using the integrated three layers of security. The use of multimodal biometrics, specifically the combination of physiological biometrics such as face, iris or fingerprint images is hypothesised to improve the e-passports security. On the other hand, using more than one modality will require more space, but with the combination of intensity mapping and steganography a biometric modality can be easily hidden into a host modality, thus exploiting the same space used by this modality in the memory chip. Different biometric modalities can act as biostego modality, for example the face image can be used as a biostego modality for hiding an iris image. Different mapping schemes can be used to map biometric images to biostego modalities. Biostego modalities and mapping schemes used by e-passports should be kept secret. This means that without knowing which biometric modality is the biostego modality and which mapping scheme used the safety of the e-passports will be improved significantly. In this work, three physiological biometrics are used as a prototype namely face image, iris and fingerprint images of an individual to secure e-passports where the true face image is used as the biostego modality (biostego image). The other two biometrics namely the iris and fingerprint images will be both hidden in the biostego image (true face image). Different mapping schemes are proposed:

- single mapping scheme
- dual mapping scheme
- distributive mapping scheme.

Each mapping scheme generates a location map which contains the coordinates of the biostego image pixels whose intensity values are the same as the intensity values of the biometric image to be hidden. The location map is then encoded using the fingerprints fuzzy vault technique which uses the minutiae extracted from the input fingerprint image. The file which contains the vault data V.txt is stored unencrypted (plain) in the memory chip. The encoded location map is then hidden in the biostego image using the LSB method. Finally, the biostego image which contains the encoded location map is stored in the e-passport memory chip. Hiding data and encoding information are extremely important in today's high technology [16]. In this paper, the methods and algorithms that are implemented and used in various issues are:

- image mapping
- LSB value, which is commonly used to hide information [17–19]
- Fingerprint fuzzy vault – the method that is often used in cryptography to secure data [20–23].

The combination and modification of these three independent schemes are important parts of the work of the authors. This allowed for a completely new encoding method for electronic identity documents. The subject is quite popular because of the rigorous need for protection of personal data or biometric data. The following approaches are used to develop methods of data encoding and decoding: watermarks [24], orthogonal code and joint transform correlation [25], DCT [26], slanted-SVD [27], chaos embedded genetic algorithm [28]. These are just examples of popular methods, tools and algorithms used to hide biometric data; they indicate importance, complexity and enormous progress of research in this issue. The motivation of this work is to protect e-passports against fraud by adding extra layers of security using image mapping, steganography and bio-cryptographic techniques. Verification/identification algorithms which are based on the combination between cryptography and steganography provide only two levels of security, while in our proposed schemes three levels of security are provided which make them harder for intruders and impostors to break in. In common steganography algorithms only one host image is used, however in the proposed distributive steganography scheme two (biostego) images are used. The first biostego image hides a section of the biometric image to be hidden while the second host image hides the remaining section of the biometric image to be hidden. This distributed steganography adds an extra security feature to our algorithm. The e-passport presented in [14] is based on embedding a watermark in the facial image and on a printed signature for verification. The facial image with its embedded watermark is encrypted with AES key before being stored in RIFD tag. The facial image is stored on centrally stored face image database, the watermark is stored in centrally stored watermark database and the AES key is centrally stored AES key. The verification of this type of e-passports depends on matching the acquired biometric features against centrally stored reference biometric features which makes this approach susceptible to adversary biometric systems attacks. Also, a password is required to access the centrally stored AES key, and this password can be compromised or lost. In other words, the security of the e-passport in [14] depends on what you have security concept such as passwords and AES keys. The security of the proposed e-passport presented in this paper depends on the 'what you are' concept. Three biometric features are used and instead of using passwords and AES keys as in [14], a fingerprint fuzzy vault is used to secure the embedded biometric location

MOST WIEDZY Downloaded from mostwiedzy.pl

© The Institution of Engineering and Technology 2019

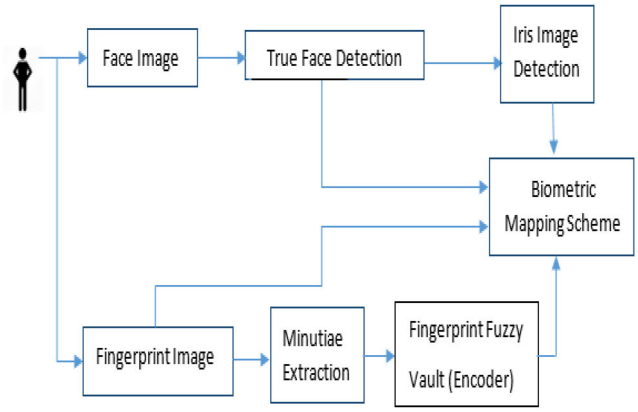

Fig. 1 *Main phases of new e-passport issuing*

maps. The e-passport in [14] has one security mode but in the proposed e-passport three security modes which correspond to three biometric mapping schemes generate the biometric location maps which improve the security level of the proposed e-passport. In [14], the verification process is done centrally which puts an overhead on the matching servers. In the proposed e-passports, the verification process is done locally on the terminal at the control gate where the biometric features acquired from the passengers are matched against the biometric features stored in the e-passport's memory chip. To access the biometric features stored in the memory chip, a passenger uses his fingerprint not a password or an AES key.

3 Proposed unified framework

The complete methodology to prevent e-fraud in e-passport is presented as a unified framework. The proposed framework is composed of four sections: section 3.1 is dedicated for new e-passport issuing, section 3.2 is dedicated for e-passport verification, section 3.3 is dedicated for intensity mapping function and section 3.4 is dedicated for biometric mapping.

3.1 New e-passport issuing

To issue a new e-passport, a coloured photo of the applicant's frontal face is acquired using a camera. A finger is selected to acquire its fingerprint image using a fingerprints live scanner. A selection of a finger must depend on a specific policy which must be kept secret. The same selected finger is used again for e-passport verification. The true face image is detected from the acquired face image then the iris image is extracted from the true face image. The acquired fingerprint image is enhanced to extract the required minutiae to generate a fuzzy vault scheme to encode the generated location maps. Location maps will be discussed later. Finally, the coloured true face image, the enhanced fingerprint image and the generated fingerprint fuzzy vault scheme are all input to the selected biometric mapping scheme. Fig. 1 shows the main phases of issuing a new e-passport.

Fig. 2 shows the implementation of the three biometric mapping schemes, where Fig. 2*a* shows the single mapping scheme, Fig. 2*b* shows the dual mapping scheme, while Fig. 2*c* shows the distributive mapping scheme.

3.2 e-Passport verification

When a passenger enters a passport control gate the camera acquires a frontal image of his/her face. Then the passenger submits the same finger used in issuing the e-passport to the fingerprint live scanner to acquire a fingerprint image. The true face image is detected and the iris image is extracted from the true face image. The minutiae are extracted from the fingerprint image to decode the location maps using the fingerprint fuzzy vault used to issue the e-passport. Fig. 3 shows the phases for e-passport verification process.

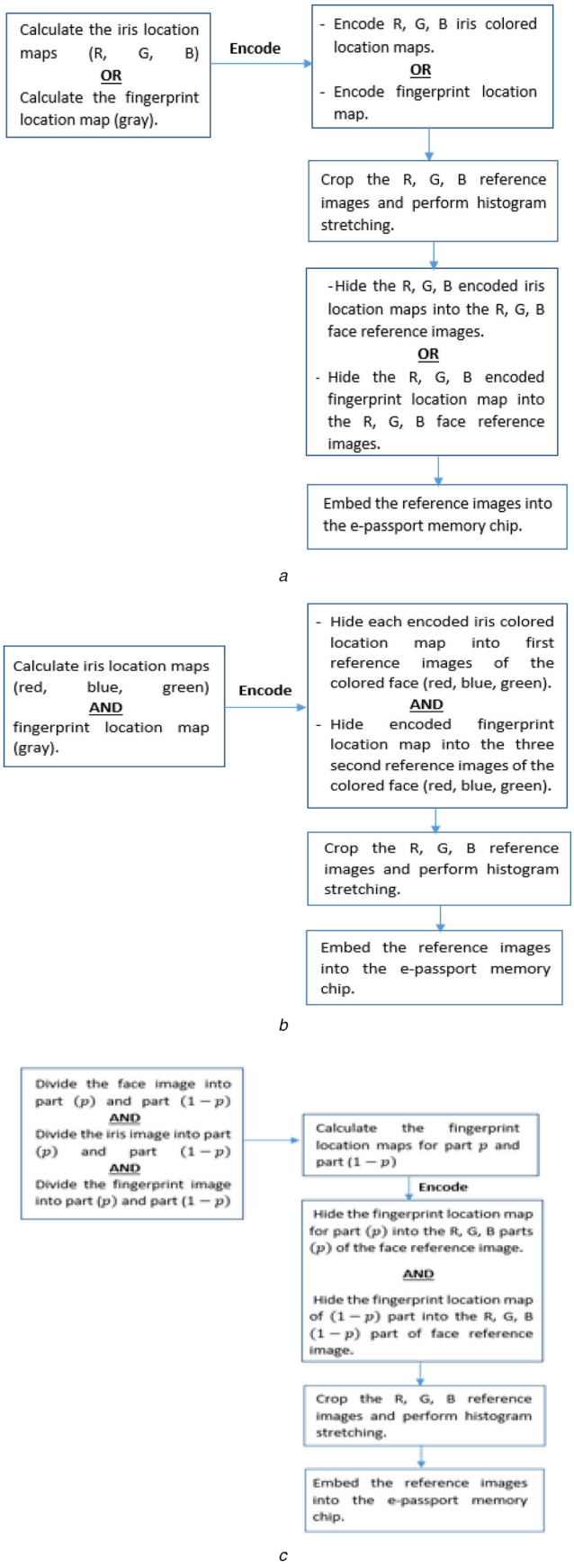

Fig. 2 *Biometric mapping schemes*
(a) Single mapping, ***(b)*** Dual mapping, ***(c)*** Distributive mapping

3.3 Intensity mapping function

In this section, an intensity mapping function is proposed to map one or more biometric image to another biometric image. The mapping function maps the pixels of one biometric image to

MOST WIEDZY Downloaded from mostwiedzy.pl

© The Institution of Engineering and Technology 2019

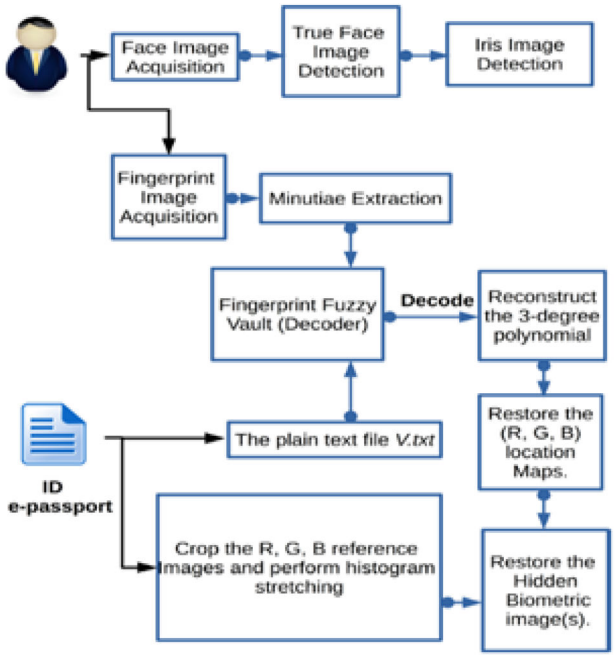

Fig. 3 *e-Passport verification*

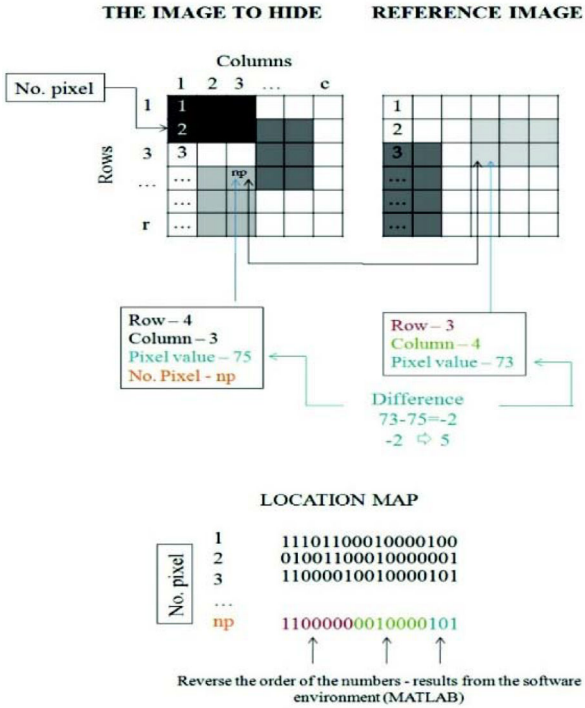

Fig. 4 *Scheme for generating location map*

another biometric image using their intensity values. The generated location map consists of the following sections: the header section which contains information about the biometric images used in the e-passport, the used mapping scheme, the size of the location map and the used biostego image(s). In the location map, there is also a section for the fingerprint image which contains the locations of the pixels in the biostego image (face image) that correspond to the pixels of the fingerprint image. The next section is dedicated for the iris image which contains the locations of the pixels in the biostego image (face image) that correspond to the pixels of the iris image. For example, in this work, we hide both the iris image, and the fingerprint image into the biostego face image. Finally, we hide a percentage P of the fingerprint image into the first biostego image, i.e. face image and hide the remaining $1-P$ of the fingerprint image in the second biostego image which is the iris image.

The multimodal biometric mapping function is done as follows:

For each input pixel $I(i, j)$:

i. Find the set of k-nearest neighbouring pixels $I^*(i^*, j^*)$ in the biostego image using the following equation:

$$V_{ij}^k = \{(i^*, j^*) \,||I(i,j) - I^*(i^*, j^*)| = \} \quad \text{s.t.} \quad \forall i^* \in N, \forall j^* \in N, \in [-4, 3] \tag{1}$$

where V_{ij}^k is the set of k-nearest neighbouring pixels $I^*(i^*, j^*)$ to the input pixel $I(i, j)$, N is the number of rows and columns of the biostego image, k is the number of neighbouring pixels in the set V_{ij}^k.

ii. For each set of k-nearest pixels V_{ij}^k, select a pixel to represent the pixels in this set using random number generator.

iii. Map the coordinates of the representative pixel (i^*, j^*) to N^+ using the following functions:

$$f(i^*, j^*) = i^* j^*, \quad \forall i^* j^* \in N^+ \tag{2}$$

$$L(i, j) = i^* j^* \lambda', \tag{3}$$

where L is the location map of the input image such that:

$$\begin{aligned}
\lambda' &= 0 \text{ if } \lambda = 0 \\
\lambda' &= 1 \text{ if } \lambda = 1 \\
\lambda' &= 2 \text{ if } \lambda = 2 \\
\lambda' &= 3 \text{ if } \lambda = 3 \\
\lambda' &= 4 \text{ if } \lambda = -1 \\
\lambda' &= 5 \text{ if } \lambda = -2 \\
\lambda' &= 6 \text{ if } \lambda = -3 \\
\lambda' &= 7 \text{ if } \lambda = -4.
\end{aligned}$$

Convert $(i^* j^* \lambda')_{10}$ to its binary string $(i^* j^* \lambda')_2$

Fig. 4 shows a schematic diagram for mapping a pixel at location (4,3) in the query image to location (3,4) in the reference image and generating a location map using the proposed mapping function.

3.4 Biometric mapping

Each e-passport must employ at least two biometric images in order to increase the security levels of an e-passport. Many schemes of biometric mappings can be implemented. The first scheme is to map a single biometric image to a single biostego image which is the single biometric mapping, a second scheme is to map two biometric images to one biostego image which is the multiple biometrics mapping, a third scheme is to map a section of the biometric image to one biostego image and map the remaining section to a second biostego image which is called the distributive biometric mapping.

On issuing an e-passport, the following procedure is employed:

- Select according to a certain policy which biometric image will be the biostego image,
- Select according to a certain policy which mapping scheme will be used to generate the correspondent location map,
- Use the fingerprints fuzzy vault to encode the generated location map,
- Hide the encoded location map in the biostego image using a steganogrphy technique which is the LSBs technique in this work,
- Store the biostego image which hides the encoded location map in the e-passport memory chip.

Each e-passport has its unique location map which differs from other e-passports. This is due to the combination between the employed mapping scheme and the biometric modality chosen as

MOST WIEDZY Downloaded from mostwiedzy.pl

© The Institution of Engineering and Technology 2019

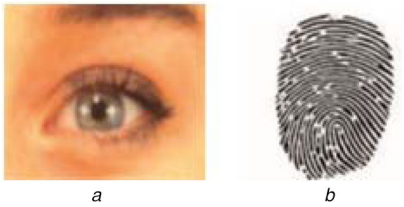

Fig. 5 *Iris and fingerprint image samples*
(a) Iris image from KDFE database [29] which is freely available, ***(b)*** Fingerprint image from https://img.bhs4.com/0e/c/0ec6b1f2738dbc167c0d863d88348c3ac12e1ca3_large.jpg, also freely available

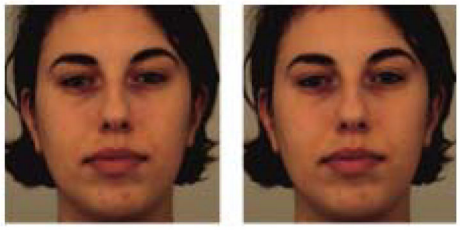

Fig. 6 *Image before and after hiding data using LSB*
(a) Image without hidden data, ***(b)*** Image in which secret data is hidden using the LSB

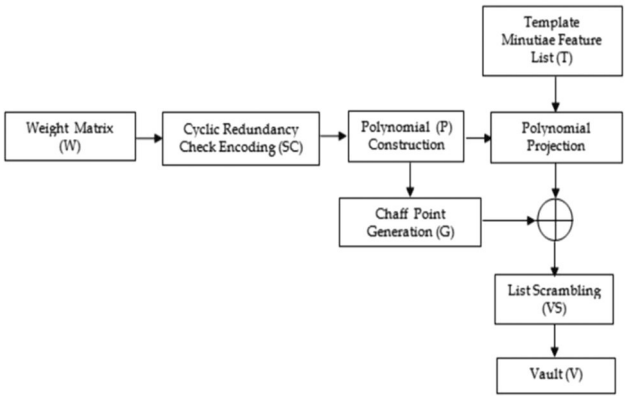

Fig. 7 *Fuzzy fingerprint vault to encode the weight matrix (**W**) (as adapted from Umult Uludag [30])*

the biostego image to hide the location map (see Appendix for proof of location map uniqueness). For coloured biometrics the location map is composed of three location maps one for each colour channel namely: red location map for the red channel, green location map for the green channel and the blue location map for the blue channel. Grey-scale biometrics such as fingerprints have only one location map. The different schemes of biometric mappings are listed below.

3.4.1 Single mapping: In this scheme of biometric mapping, a single input biometric image will be mapped to the biostego image and a location map will be generated. The location map will be encoded using the fingerprints fuzzy vault technique and then it is hidden in the biostego image using the LSB method before storing the combination in the memory chip of the e-passport. In case the biometric image to be hidden is grey scale, such as a fingerprint image and the biostego image is coloured such as a coloured face image, then the coloured biostego image can be converted to a grey scale image before mapping the biometric image to it. The alternative is not to convert the 'coloured biostego image' to grey scale image, only one channel from the RGB image channels is used to encode and decode the grey scale biometric image. The decision is dependent on whether we need colour biostego image or not. Keeping this decision confidential enhances the security level of the e-passport. In case the biometric image and the biostego image are both coloured, then the red channel of the biometric image is mapped to the red channel of the biostego image, the green channel of the biometric image is mapped to the green channel of the biostego image and the blue channel of the biometric image is mapped to the blue channel of the biostego image. Switching between mappings of colour channels can add extra level of security, i.e. mapping a colour channel of the biometric image to another colour channel of the biostego image. One alternative of colour mappings is to map the red channel of the biometric image to the blue channel of the biostego image, the green channel of the biometric image to the red channel of the biostego image and the blue channel of the biometric image to the green channel of the biostego image. There are nine colour mappings between coloured biometric image and coloured biostego image. Which colour mapping is used with an e-passport must be kept confidential. In all cases of colour mappings, three location maps are always generated. In case of the biometric image to be hidden is coloured and the biostego image is grey scale such as hiding coloured iris image into a fingerprint image, then each pixel in each colour channel is mapped to the pixels of the grey scale channel of the biostego image. Three location maps are also generated in this case.

3.4.2 Dual mapping: In this type of mapping, a dual mapping scheme is used, the coloured iris image and grey scale fingerprint image are mapped, as presented in Fig. 5 to one biostego image (coloured true face image) and retrieve them back.

3.4.3 Distributive mapping: In distributive mapping there are two biostego images, the coloured iris image and coloured true face image. A percentage P of the fingerprint image is hidden in the true face image and $1 - P$ of the fingerprint image is hidden in the iris image. As another alternative, the percentage P of the fingerprint image can be hidden into the iris image and $1 - P$ can be hidden in the true face image.

4 LSB method

The LSB is the 'youngest one' it means the least important bit [17–19]. In case of digital images, the intensity value of each pixel ranges from 0 to 255 in the RGB colour space, each R, G and B channel is expressed as binary value, the change in the value of the LSB slightly affects the interpretation of the entire image. In Fig. 6, an example of two images is presented. The first image is the input image (unchanged), the second image is the input image with its LSBs changed. The differences between the images are not visible to the naked eye.

5 Fingerprint fuzzy vault

This is a type of crypto-biometrics where cryptography and biometrics are combined to achieve high security and user's convenience in the same time [30]. Encoding is done on the basis of information that can be found in the fingerprints – the location of characteristic minutiae points. Positions of the first pixels, which contain information, are encrypted using the polynomial and then hidden in a vault of genuine and chaff points. Figs. 7 and 8 show diagrams of the method for encoding and decoding. Over the years, these assumptions are often used. An example of this approach is the publications on cryptography [2, 31, 32].

6 Experimental results

The following section shows how the above described data is used in the process of encoding and decoding.

6.1 Data encoding

In this stage, the multi-modal biometrics used in the e-passport are pre-processed before being used in biometrics mapping. For the e-passport photo the true face image is detected. The iris image is used as it is. There is no need to find the iris in the image, because the iris is focused to fill the entire image. Fig. 9*a* shows a standard e-passport photo and Fig. 9*b* shows the detected true face which is

MOST WIEDZY Downloaded from mostwiedzy.pl

© The Institution of Engineering and Technology 2019

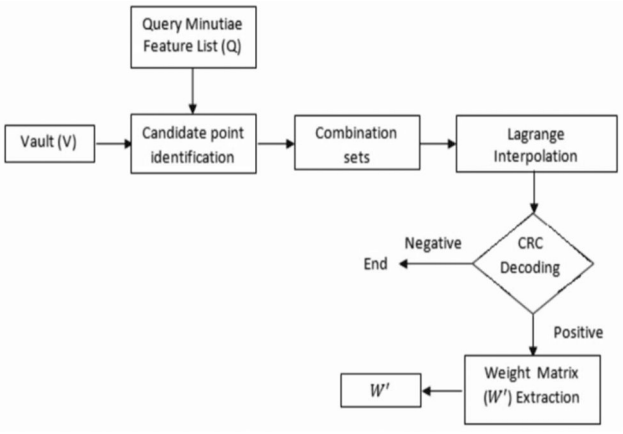

Fig. 8 *Fuzzy fingerprint to decode the weight matrix (**W**) (as adapted from Umult Uludag [30])*

Fig. 9 *E-passport photo*
(a) Adapted from the KDFE database [29] (which is freely available), ***(b)*** Detected true face used as a biostego image

used by the biometric steganography. The workflow of the preprocessing stage is presented in Fig. 10.

The input data are three images all of them used in the analysis:

(i) A colour passport face image, Fig. 9 – input size: 83 × 111 pixels,
(ii) A colour image of the iris, Fig. 5*a* – input size: 95 × 80 pixels,
(iii) A grey image of fingerprint, Fig. 5*b* – input size: 100 × 100 pixels.

The analyses carried out are prepared based on arbitrarily assumed size of the analysed images. Preliminary preparations of images for further process of data encoding for the e-passport are:

(i) Detection of 'true face' is conducted using Viola-Jones algorithm for object detection [33],
(ii) Digital image processing – changes in image size for the analysed data – size of true face image is 432 × 432 pixels.

Adopted changes of the image size are decided by the later image encoding using the method of LSB. The hidden image must be smaller than the image to which the mapping should be done. Therefore, the mapping is performed only on a part of the biostego image. This part of the image is named as a reference image. The reference image is located in the bottom right corner of the biostego image. It is a crop image – the lower right part of the image of the scaled true face image (see Fig. 10). The size of the reference image is 80 × 95 pixels. The reference image has been decomposed into three RGB channels, and then the histogram has been stretched and the new values assigned to the pixels. This method of preprocessing is applied not only in single mapping but also in dual mapping and distributive mapping. Histogram stretching of the reference image is necessary due to the fact that there may be a situation where there is no pixel the value of its colour is equal to the searched value. Modifying the histogram of reference image guarantees the values of pixels' illumination are

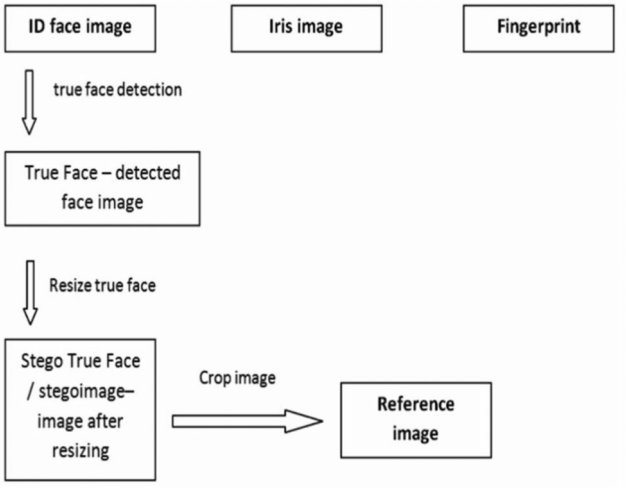

Fig. 10 *Image preprocessing workflow*

not changed and the mapping process can be done, independent of the selected method. The number of bits in the binary value for each ($i^* j^* \lambda'$) is clearly defined. The resulting location map L is converted to the form of vectors ***WM*** which consist of the number of elements equal to the number of columns × number of rows of the map L. The resulted vectors are completely hidden in the biostego image, where the number of pixels must be at least equal to the number of vector elements ***WM*** + 100 (the value 100 is based on the assumptions associated with fingerprints fuzzy vault). Hiding is performed using the LSB method. The last bit of the pixel for each colour channel (R, G or B) is converted to a bit map locations L. While hiding the location map in the biostego image using LSB, the first pixel in which the information is hidden has been chosen randomly. For each colour, the first pixel of the image is defined separately (e.g. *a* – index of first pixel for red colour, *b* – index of the first pixel for the green colour, *c* – index of the first pixel for blue colour). The values range between 1 and 100. The essence of the coding is hiding the location map in a manner that it is not directly possible to locate pixels which contain information. With the fingerprint fuzzy vault technique, a V.txt file is generated, which contains additional coded information from the fingerprint and more precisely the coordinates of characteristic points of a fingerprint which are fingerprint minutiae for data encoding. In this work, a third-degree polynomial $p(u)$ is used to implement the fingerprint fuzzy vault in contrast to the polynomial used in article [30], where the encoding is based on a polynomial of the eighth degree. A 3-degree polynomial is used because the true face image that acts as a biostego image is coloured and there is no need to encode more than 3 values for location maps of red, green and blue. Therefore, a 3-degree polynomial is sufficient for testing the proposed mapping schemes. Furthermore, the computational complexity of encoding using 3-degree polynomial is much less than 8-degree polynomial. On the other hand, an 8-degree polynomial can be used if needed. The encoding and decoding processes are not practically different from the algorithm proposed in article [30], but instead of the transition to a set of nine coefficients c_i, $i = 1, 2, \ldots, 8$, four coefficients a, b, c and *d* are used. Equation (4) shows the polynomial used in this work, together with a description of coefficients

$$p(u) = au^3 + bu^2 + cu + d \tag{4}$$

where *a* is the index of the first pixel with information in the red colour, *b* is the index of the first pixel with information in the green colour, *c* is the index of the first pixel with information in the blue colour, d is the random number.

The values of *u* arise as a result of coding coordinates *x* and *y* minutiae. To extract minutiae coordinates the algorithm of Athi Narayanan [34] is used. Minutiae coordinates in the form of eight bits binary digits have been accumulated to the form of $(u)_2 = [x|y]$ – 16 bits digit. Each binary value of *u* is transformed

MOST WIEDZY Downloaded from mostwiedzy.pl

© The Institution of Engineering and Technology 2019

to a decimal form $(u)_{10}$ which is used to create a set of vault points, in line with the authors of article [30].

In the case of encoding using different mapping schemes, the following activities are performed:

(i) *Dual mapping*: Hiding the location map of a coloured iris image using the method of LSB is carried out as in the case of single mapping, but the location map of the fingerprint image is hidden in pixels of the three colour channels of the biostego face image. The following diagram shows the scheme for hiding the location map of the fingerprint image (Fig. 11).

(ii) *Distributive mapping*: In this case, the fingerprint image is divided into two parts: for P percent (for all 100 rows, and from 1 to P column) of the fingerprint image the location map is hidden in the whole iris image while the remaining $100 - P$ percent (for all 100 rows, and the $P + 1$ 100 columns) is hidden in the true face image, specifically, the reference image. As a result, two location maps are generated. One corresponds to the first part – $L1$ imprints, the second map corresponds to the second part of fingerprint – $L2$. Both arrays are merged together to generate the final location map which is hidden in the intensity values of the red colour pixels of the true face image. In this case, the polynomial coefficients a and b are important for encoding using fingerprints fuzzy vault while c and d are not, where a is the index of the first pixel containing bits of location maps, b is the percentage of columns, for which the location map is made on the basis of the iris image.

The file containing the vault data V.txt is stored unencrypted (plain) in the memory chip.

6.2 Data decoding

In the decoding process, the input data is the text file V.txt (plain) containing the vault data restored from the memory chip and the fingerprint image of the traveller acquired by the scanner. Decoding of the image components, or hidden images, can be made after fingerprint verification. It is important that the coordinates of the fingerprint image during decoding are exactly the same as the fingerprint image coordinates used during encoding. In the context of this paper, the issue of the correct orientation of the fingerprint image is not addressed as the encoding and decoding processes are performed on the same fingerprint images. The first step in decoding is choosing values of u with $z = p(u)$, from among the complete set of vault points according to the procedure described in [30]. Depending on the degree of the polynomial, an indication of the appropriate number of points to enable interpolation is necessary. Interpolation allows to determine the coefficients of the polynomial (in the case previously quoted polynomials $p(u)$ the coefficients a, b, c, d). After the polynomial coefficients, in other words the decoded data, are determined it is able to extract from the decoded image the hidden location map L. During the decoding of biostego image it is necessary to crop the reference image and perform histogram stretching same as during the encoding process. This allowed the erudition of hidden pixel.

The diagram for the decoding process is shown in Fig. 12. Depending on the mapping scheme, it is necessary to take into account the size of the location map and reference it to the individual data.

6.3 Discussion

In this section, the results of the verification process using the described schemes are presented. Twenty testing sets are used in the experiments. Each dataset consists of three images, and each image has the following dimensions:

(i) extracted image of the face – 54 × 54 pixels,
(ii) fingerprint image – 100 × 100 pixels,
(iii) iris image – 95 × 80 pixels.

Images of the face have been randomly chosen from the freely available data in the Karolinkska Directed Emotional Faces

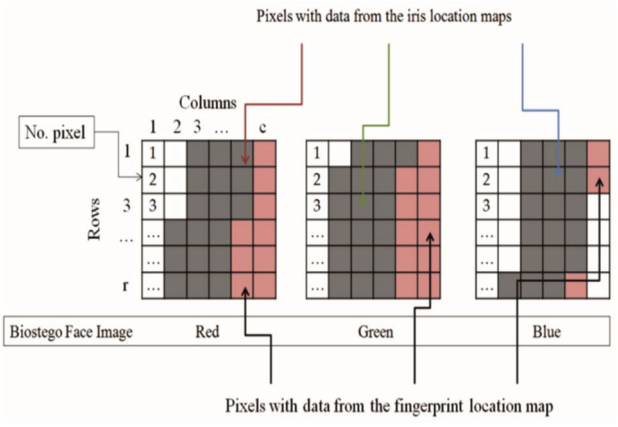

Fig. 11 *Scheme for hiding the location map of the fingerprint for dual mapping method*

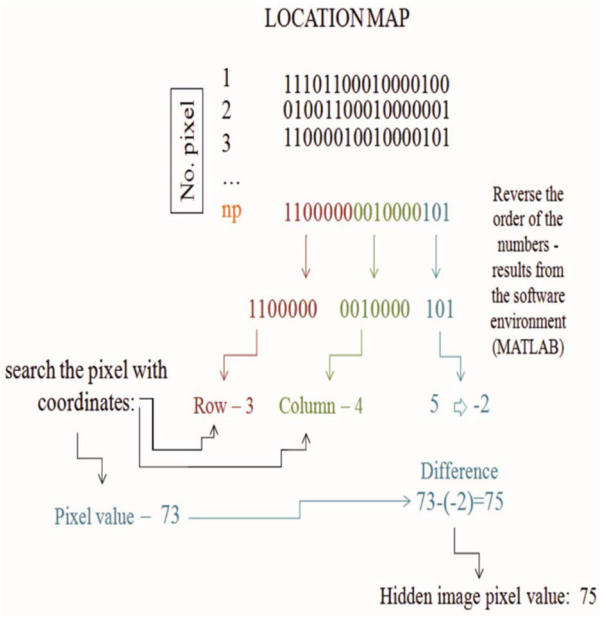

Fig. 12 *Scheme of decoding location map*

(KDFE) database [29]. In the presented work, only one fingerprint has been used (see Fig. 5), due to restrictions against free access to data bases with such fragile information. Iris images were extracted from the chosen face images according to the algorithm described in [35]. The detailed description of commonly used algorithms for iris recognition was presented in [36]. To show the analysis results, input images (those that have been hidden) were compared against output images (those that have been decoded). Similarity of the images is described by three coefficients listed below:

- Index SSIM (structural similarity):

$$\mathrm{SSIM}(x, y) = [l(x, y)]^{\alpha}[c(x, y)]^{\beta}[s(x, y)]^{\gamma} \tag{5}$$

where

$$l(x, y) = \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \tag{6}$$

$$c(x, y) = \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \tag{7}$$

$$s(x, y) = \frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3} \tag{8}$$

MOST WIEDZY Downloaded from mostwiedzy.pl

© The Institution of Engineering and Technology 2019

where μ_x is the mean for image x; μ_y is the mean for image y; σ_x is the standard deviation for image x; σ_y is the standard deviation for image y; σ_{xy} is the cross-covariance for images x and y.

If $\alpha = \beta = \gamma = 1$, and $C_3 = C_2/2$ default selection of C_3 the index simplifies to

$$\mathrm{SSIM}(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (9)$$

- PSNR (peak signal-to-noise ratio):

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\mathrm{peakval}^2}{\mathrm{MSE}}\right) \quad (10)$$

where peakval is either specified by the user or taken from the range of the image datatype, MSE is the mean square error.

- Correlation coefficient r:

$$r = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{\sum_m \sum_n (A_{mn} - \bar{A})^2 \sum_m \sum_n (B_{mn} - \bar{B})^2}} \quad (11)$$

where $\bar{A} = \mathrm{mean2}(A)$ and $\bar{B} = \mathrm{mean2}(B)$.

The coding and decoding of the analysed datasets are carried out three times for single mapping, dual mapping and distributive mapping schemes. For single mapping scheme, the results for the SSIM, PSNR and 2D correlation coefficients of the 20 sets are the same. Table 1 shows the results of one set. The standard deviation for each dataset using the single mapping scheme has been calculated. Table 2 shows the standard deviations of one set.

For dual mapping and distributive mapping schemes the results in Table 3 are the arithmetic means of the acquired values. Due to the fact that the coding algorithm operates randomly, different values of the SSIM index, PSNR and 2D correlation coefficients can be calculated for the same data. The standard deviation for each dataset is calculated and presented in Table 4.

In case of single mapping, the hidden and decoded images are identical due to the fact that the face image (in which the data was hidden) is too large ($432 \times 432 = 186624$ pixels) that after hiding 129,200 bits of iris location map (iris images – 95×80 pixels, and each pixel is represented by 17 bits), the last image columns have pixels with unchanged values. Thanks to the unchanged reference image pixels.

Unfortunately, in case of dual mapping scheme, the LSBs of the reference image pixels are changed. These result from additional hiding of the location map of fingerprints. In contrast, the obtained values of SSIM, PSNR and the correlation coefficients, allow concluding that the loss within decoded images is within the accepted limits. As an example, a value of about 40 dB is a typical PSNR value for compressing images with 8 bits colour depth [31]. Of course, there is a possibility in case of dual mapping the output images are identical, as the input images. On the other hand, it would require increasing the size of the biometric stego image into which the location maps generated are hidden using LSB method.

For distributive mapping the decoded fingerprint image is not the same with respect to the original image, however the differences are still negligible. This is because of changes in the brightness of 170,000 of the 186,624 pixel face image in the field of red, which are associated with the change of the pixel values of reference image. As in the case of dual mapping, increasing the size of the face image is affected by the lack of changes in the pixel values of the reference image. Another solution in this situation is that the use of reference image in terms of red, while hiding location maps of fingerprint image in green or blue colour.

All the analysis is done on images of a predetermined size. Standardising the size of the biometric images that need to be encoded and stored in e-document is recommended in order to apply this method. However, the limitation of the proposed e-passports lies in the size of the reference image of the biostego image used for the mapping and embedding of the location map. In single mapping scheme the reference image must be as large as the input biometric image. In case of dual mapping scheme, the size of the reference image must be as large as the size of the dual input images. This can put a limit on the number of input images to be mapped and embedded into a face image. In distributive mapping, the reference image of each biostego image must be as large as the part p of the input image to be mapped to and embedded into it.

Table 1 Similarities analysis of encoded and decoded images for one set

	Single mapping		
	Iris R	Iris G	Iris B
SSIM	1	1	1
PSNR	∞	∞	∞
2D Corr. Coef.	1	1	1

Table 2 Standard deviations of similarity analysis measures presented in Table 1

	Single mapping		
	Iris R	Iris G	Iris B
SSIM	1	1	1
PSNR	∞	∞	∞
2D Corr. Coef.	1	1	1

Based on the statistical analysis of SSIM and PSNR there is no big difference between the original biometric image and reconstructed biometric image. So, we expect that the accuracy of the biometric classifier using the original image will not be significantly different from the accuracy using the reconstructed biometric image.

Figs. 13–15 show the histograms of the 20 sets for PSNR, SSIM and 2D-correlation coefficients for the dual mapping scheme, respectively. Figs. 16–18 show the histograms of the standard deviations for the three metrics PSNR, SSIM and 2D-correlation coefficients for the 20 sets using dual mapping scheme, respectively.

From the above histograms it appears that there are no significant differences between the PSNR, SSIM and 2D correlation coefficients for iris images in the 20 sets. This interpretation was validated by the standard deviation coefficients which show the amount of variation or dispersion of the SSIM index and 2D coefficients of the 20 sets. It is well known that SSIM is an image quality metric that assesses the visual impact of three characteristics of an image: luminance, contrast and structure. The typical SSIM index is a decimal value in the range $[-1$ to $+1]$ where +1 indicates two identical images and therefore indicates perfect structural similarity. A value of 0 indicates no structural similarity. The histogram figures for SSIM indices of the three colour channels of iris image in Fig. 14 are close to +1 for dual mapping scheme which imply that the reconstructed iris images are still preserving the characteristics of the original image. The histogram figures for PSNR metrics of the iris images of the 20 sets show some slight differences as it appears from the histograms of standard deviations for the PSNR metrics. Typical values of PSNR in lossy image compression and video compression are between 30 and 50 dB, provided the bit depth is 8 bits, where higher is better [37, 38]. It appears from the histogram figures of PSNR that the PSNR for the reconstructed iris images in the 20 sets are within the range [44–49 dB] for the red and green channels of the 20 iris images, and within the range [41–49 dB] for the blue channel which means that the PSNR for the reconstructed images are within the typical range of PSNR. However, the histograms of PSNR, SSIM and 2D correlation coefficients for the fingerprint images show some differences between the 20 sets in the dual mapping scheme. It appears from Tables 1 and 2 that in case of single mapping scheme, the histograms for the PSNR and SSIM indices show that the reconstructed iris images of red, blue and green channels are exactly the same as the original images which imply that the false acceptance rate (FAR) and false recognition rate (FRR) for the reconstructed images and original images are the same. Therefore, if FAR = 0 and FRR = 0 using original images then the FAR = 0 and FRR = 0 using reconstructed

MOST WIEDZY Downloaded from mostwiedzy.pl

© The Institution of Engineering and Technology 2019

Table 3 Similarities analysis of encoded and decoded images

		Mapping method				
		Dual mapping				Dist. mapping
		Iris R	Iris G	Iris B	Fingerprint	Fingerprint
Set 1	SSIM	0.9943	0.9907	0.9946	0.9360	0.9986
	PSNR	46 dB	44 dB	43 dB	26 dB	54 dB
	2D Corr. Coef.	0.9998	0.9997	0.9998	0.9833	0.9999
Set 2	SSIM	0.9981	0.9980	0.9985	0.8258	1.0000
	PSNR	48 dB	49 dB	49 dB	17 dB	55 dB
	2D Corr. Coef.	0.9999	0.9999	0.9999	0.9544	1.0000
Set 3	SSIM	0.9949	0.9967	0.9966	0.9460	0.9989
	PSNR	46 dB	44 dB	44 dB	25 dB	54 dB
	2D Corr. Coef.	0.9999	0.9996	0.9998	0.9783	1.0000
Set 4	SSIM	0.9983	0.9977	0.9976	0.9460	1.0000
	PSNR	48 dB	48 dB	45 dB	19 dB	56 dB
	2D Corr. Coef.	0.9999	0.9997	0.9995	0.9847	0.9998
Set 5	SSIM	0.9963	0.9987	0.9966	0.8660	1.0000
	PSNR	44 dB	49 dB	48 dB	21 dB	56 dB
	2D Corr. Coef.	0.9999	0.9999	0.9997	0.9633	0.9999
Set 6	SSIM	0.9993	0.9987	0.9946	0.8345	1.0000
	PSNR	44 dB	46 dB	44 dB	22 dB	53 dB
	2D Corr. Coef.	0.9996	0.9993	0.9998	0.9754	0.9999
Set 7	SSIM	0.9953	0.9917	0.9916	0.8885	0.9978
	PSNR	45 dB	45 dB	41 dB	26 dB	52 dB
	2D Corr. Coef.	0.9998	0.9899	0.9994	0.9886	0.9997
Set 8	SSIM	0.9936	0.9910	0.9944	0.9221	0.9986
	PSNR	44 dB	45 dB	42 dB	27 dB	54 dB
	2D Corr. Coef.	0.9995	0.9993	0.9993	0.9901	0.9999
Set 9	SSIM	0.9928	0.9927	0.9916	0.9102	0.9997
	PSNR	46 dB	46 dB	48 dB	23 dB	55 dB
	2D Corr. Coef.	0.9998	0.9991	0.9997	0.9897	0.9996
Set 10	SSIM	0.9933	0.9908	0.9986	0.8834	0.9999
	PSNR	46 dB	45 dB	44 dB	23 dB	54 dB
	2D Corr. Coef.	0.9989	0.9989	0.9993	0.9923	0.9999
Set 11	SSIM	0.9944	0.9918	0.9946	0.8756	0.9996
	PSNR	45 dB	44 dB	43 dB	29 dB	55 dB
	2D Corr. Coef.	0.9993	0.9998	0.9998	0.9941	1.0000
Set 12	SSIM	0.9977	0.9928	0.9947	0.8989	1.0000
	PSNR	44 dB	44 dB	43 dB	17 dB	54 dB
	2D Corr. Coef.	0.9999	0.9995	0.9994	0.9788	0.9999
Set 13	SSIM	0.9921	0.9905	0.9951	0.8991	1.0000
	PSNR	44 dB	44 dB	49 dB	17 dB	54 dB
	2D Corr. Coef.	0.9992	0.9991	0.9991	0.9882	0.9999
Set 14	SSIM	0.9932	0.9933	0.9955	0.9344	1.0000
	PSNR	48 dB	47 dB	48 dB	17 dB	54 dB
	2D Corr. Coef.	0.9988	0.9990	0.9996	0.9898	1.0000
Set 15	SSIM	0.9979	0.9909	0.9996	0.8674	0.9997
	PSNR	49 dB	46 dB	48 dB	23 dB	53 dB
	2D Corr. Coef.	0.9995	0.9991	0.9999	0.9834	0.9998
Set 16	SSIM	0.9982	0.9912	0.9988	0.9010	0.9997
	PSNR	46 dB	47 dB	45 dB	22 dB	56 dB
	2D Corr. Coef.	0.9993	0.9989	0.9999	0.9978	0.9997
Set 17	SSIM	0.9988	0.9971	0.9982	0.9345	0.9995
	PSNR	47 dB	47 dB	47 dB	25 dB	52 dB
	2D Corr. Coef.	0.9999	0.9992	0.9992	0.9956	0.9998
Set 18	SSIM	0.9984	0.9986	0.9923	0.9336	0.9999
	PSNR	47 dB	44 dB	43 dB	25 dB	52 dB
	2D Corr. Coef.	0.9999	0.9997	0.9992	0.9987	1.0000
Set 19	SSIM	0.9999	0.9948	0.9966	0.8962	0.9999
	PSNR	45 dB	46 dB	41 dB	29 dB	53 dB
	2D Corr. Coef.	0.9989	0.9997	0.9997	0.9988	1.0000
Set 20	SSIM	0.9995	0.9988	0.9992	0.8349	0.9997
	PSNR	49 dB	47 dB	45 dB	29 dB	53 dB
	2D Corr. Coef.	0.9998	0.9997	0.9998	0.9977	0.9999

MOST WIEDZY Downloaded from mostwiedzy.pl

© The Institution of Engineering and Technology 2019

Table 4 Standard deviations of similarity analysis of the measures presented in Table 3

		Mapping method				
		Dual mapping				Dist. mapping
		Iris R	Iris G	Iris B	Fingerprint	Fingerprint
Set 1	Std. Dev. SSIM	0.012	0.0012	0.007	0.1294	0.008
	Std. Dev. PSNR	2 dB	1 dB	1 dB	1 dB	2 dB
	Std. Dev. 2D Corr. Coef.	0	0.007	0	0.0012	0.009
Set 2	Std. Dev. SSIM	0.011	0.009	0.007	0.112	0
	Std. Dev. PSNR	2 dB	1 dB	1 dB	1 dB	2 dB
	Std. Dev. 2D Corr. Coef.	0	0	0	0.015	0
Set 3	Std. Dev. SSIM	0.011	0.007	0.008	0.106	0.005
	Std. Dev. PSNR	1 dB	1 dB	1 dB	1 dB	1 dB
	Std. Dev. 2D Corr. Coef.	0.011	0.0013	0.006	0.0146	0
Set 4	Std. Dev. SSIM	0.009	0.0077	0.006	0.02	0
	Std. Dev. PSNR	2 dB	2 dB	2 dB	1 dB	2 dB
	Std. Dev. 2D Corr. Coef.	0.09	0.007	0.125	0.098	0.007
Set 5	Std. Dev. SSIM	0.012	0.008	0.007	0.113	0
	Std. Dev. PSNR	1 dB	1 dB	1 dB	1 dB	2 dB
	Std. Dev. 2D Corr. Coef.	0	0	0	0.014	0
Set 6	Std. Dev. SSIM	0.01	0.005	0.008	0.136	0
	Std. Dev. PSNR	1 dB	1 dB	1 dB	1 dB	1 dB
	Std. Dev. 2D Corr. Coef.	0	0	0	0.0154	0
Set 7	Std. Dev. SSIM	0.013	0.0017	0.006	0.1267	0
	Std. Dev. PSNR	1 dB	1 dB	1 dB	1 dB	2 dB
	Std. Dev. 2D Corr. Coef.	0	0	0	0.0126	0
Set 8	Std. Dev. SSIM	0.011	0.0011	0.005	0.008	0
	Std. Dev. PSNR	1 dB	1 dB	1 dB	1 dB	1 dB
	Std. Dev. 2D Corr. Coef.	0	0	0	0.01	0
Set 9	Std. Dev. SSIM	0.021	0.007	0.006	0.1034	0
	Std. Dev. PSNR	1 dB	1 dB	1 dB	1 dB	2 dB
	Std. Dev. 2D Corr. Coef.	0	0	0	0.005	0.007
Set 10	Std. Dev. SSIM	0.03	0.008	0.006	0.1134	0
	Std. Dev. PSNR	1 dB	1 dB	1 dB	1 dB	1 dB
	Std. Dev. 2D Corr. Coef.	0	0	0	0.013	0
Set 11	Std. Dev. SSIM	0.011	0.003	0.006	0.156	0
	Std. Dev. PSNR	1 dB	1 dB	1 dB	1 dB	2 dB
	Std. Dev. 2D Corr. Coef.	0	0	0	0.0141	0
Set 12	Std. Dev. SSIM	0.017	0.0018	0.007	0.112	0
	Std. Dev. PSNR	1 dB	1 dB	1 dB	1 dB	2 dB
	Std. Dev. 2D Corr. Coef.	0.009	0	0	0.0188	0
Set 13	Std. Dev. SSIM	0.021	0.005	0.001	0.1291	0
	Std. Dev. PSNR	1 dB	1 dB	1 dB	1 dB	2 dB
	Std. Dev. 2D Corr. Coef.	0	0	0	0.002	0
Set 14	Std. Dev. SSIM	0.032	0.003	0.005	0.014	0
	Std. Dev. PSNR	1 dB	1 dB	1 dB	1 dB	1 dB
	Std. Dev. 2D Corr. Coef.	0.008	0	0	0.018	0
Set 15	Std. Dev. SSIM	0	0	0	0.0174	0
	Std. Dev. PSNR	1 dB	1 dB	1 dB	1 dB	1 dB
	Std. Dev. 2D Corr. Coef.	0.015	0.001	0.009	0.0132	0
Set 16	Std. Dev. SSIM	0.012	0.0021	0.008	0.110	0
	Std. Dev. PSNR	1 dB	1 dB	1 dB	1 dB	2 dB
	Std. Dev. 2D Corr. Coef.	0	0	0	0.0178	0
Set 17	Std. Dev. SSIM	0.018	0.001	0.002	0.009	0
	Std. Dev. PSNR	1 dB	1 dB	1 dB	1 dB	2 dB
	Std. Dev. 2D Corr. Coef.	0.019	0.002	0.0028	0	0
Set 18	Std. Dev. SSIM	0.014	0.006	0.007	0.105	0
	Std. Dev. PSNR	1 dB	1 dB	1 dB	1 dB	1 dB
	Std. Dev. 2D Corr. Coef.	0.011	0.007	0	0.097	0
Set 19	Std. Dev. SSIM	0.019	0.003	0.006	0.1062	0
	Std. Dev. PSNR	1 dB	1 dB	1 dB	1 dB	1 dB
	Std. Dev. 2D Corr. Coef.	0	0	0	0.0113	0
Set 20	Std. Dev. SSIM	0.015	0.0015	0.002	0.1521	0
	Std. Dev. PSNR	1 dB	1 dB	1 dB	1 dB	1 dB
	Std. Dev. 2D Corr. Coef.	0	0	0	0.0177	0

MOST WIEDZY Downloaded from mostwiedzy.pl

© The Institution of Engineering and Technology 2019

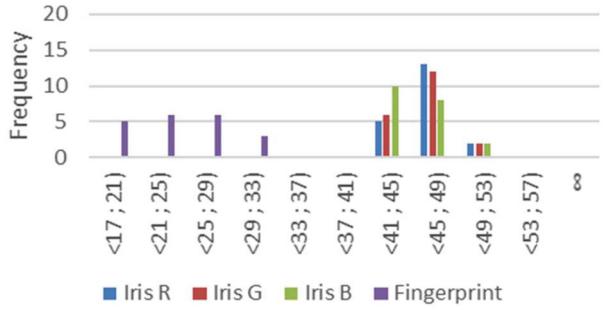

Fig. 13 *PSNR for dual mapping scheme*

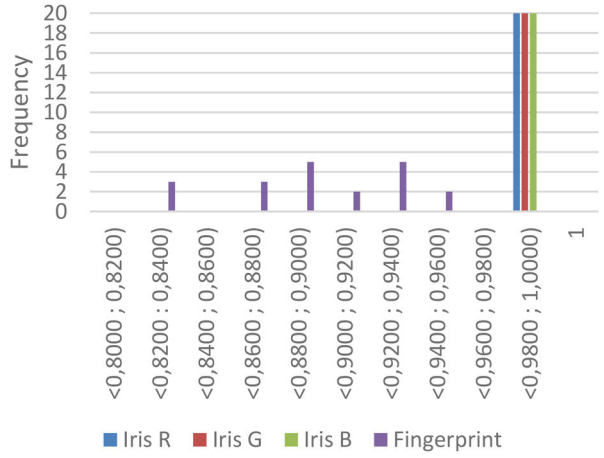

Fig. 14 *SSIM for dual mapping scheme*

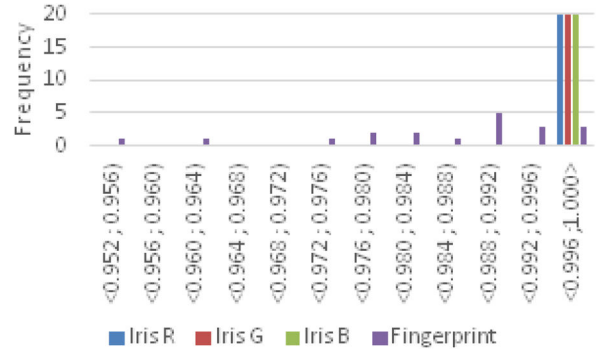

Fig. 15 *2D-correlation coefficients for dual mapping*

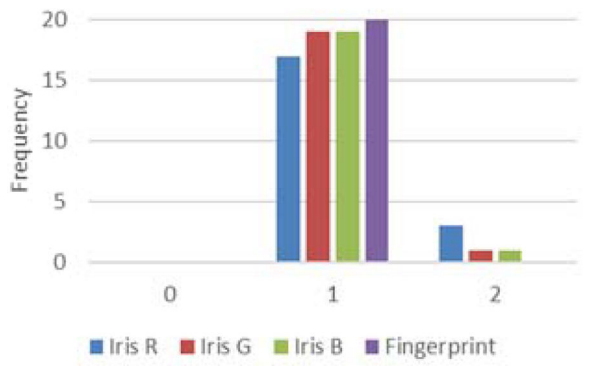

Fig. 16 *PSNR standard deviation for dual mapping scheme*

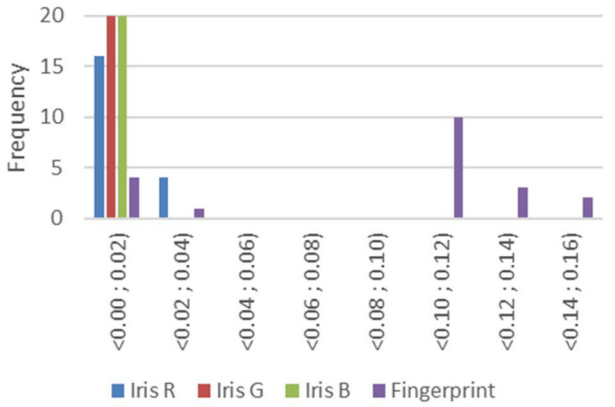

Fig. 17 *SSIM standard deviation for dual mapping scheme*

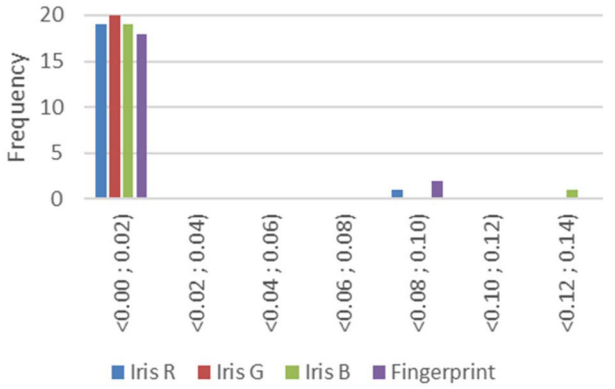

Fig. 18 *2D-correlation coefficient standard deviation for dual mapping scheme*

images which is better than [12]. It is clear from Tables 3 and 4 that the PSNR values for the 20 fingerprint images for dual mapping scheme are within the range [17 – 29 dB] which fall behind the typical range [30 – 50 dB] which imply that the FAR and FRR will be different from zero. For distributive mapping scheme, the PSNR values for the 20 fingerprint images are within the range [53 – 56 dB] which is higher than the typical range for PSNR. The PSNR values for the iris images of the three colour channels in dual mapping scheme are within the typical range [30 – 50 dB] and the SSIM indices are close to 1 which imply that the expected FAR and FRR are close to zero which is better than [12]. Accordingly, dual mapping scheme for fingerprint images is not recommended meanwhile using fingerprints with single mapping or distributive mapping schemes give better reconstructed fingerprint images. There is no constraint on using iris images with single mapping or dual mapping schemes.

7 Security analysis

In this section, we show the immunity of the suggested e-passport against possible attacks on e-passports. Skimming attack which means clandestine reading of the e-passport biometric data used for identity authentication could not happen in the proposed e-passport because its data is protected by the fingerprint fuzzy vault of the owner. The selection of a finger for an e-passport must comply with a secret selection policy. One example, a secret hash function can take the e-passport ID as input and outputs the index of the finger to be used with this e-passport. This prevents the attacker to learn about the finger chosen for an e-passport. Suppose in worst case scenario that the chosen finger selected for an e-passport is known to the attacker, for example the attacker has learned that the right index finger is used by an e-passport, this information is not enough to compromise the security of the e-passport as long as the attacker has no access to the finger of the e-passport holder. In other words, the attacker could not know which true minutiae are used by the polynomial employed by this e-passport. Moreover, using polynomials with different degrees will make it harder for the attacker to reconstruct the real polynomial. Cloning attack is occurred when an attacker read all the data contained within the e-passport's chip and perform a chip cloning attack by writing this data in a new blank chip. This kind of attack is prevented by using the fingerprint image of the e-passport's owner to generate a location map which is then encoded using the fingerprints fuzzy vault technique which uses the minutiae extracted from the same fingerprint image used to issue the e-passport. This attack will fail

MOST WIEDZY Downloaded from mostwiedzy.pl

© The Institution of Engineering and Technology 2019

in the proposed e-passport because cloning the e-passport will also clone the fingerprint location map which encoded with the minutiae of the owner fingerprint which will not match with any other fingerprint in the world due to the uniqueness property of the fingerprints. Another kind of attack occurs when an attacker tries to compromise the fingerprint location map of an e-passport to embed it into a new blank chip. This attack will also fail as the attacker needs the fingerprint's minutiae of the e-passport owner to access the location map embedded in the biostego image. Moreover, the attacker does not know which biometric is used to be the biostego image and what mapping scheme is used to generate the location map. Now imagine, the attacker altered the content of the encoded location map then the authorities can detect that the e-passport was tampered with because the retrieved biometric image which can be an iris or a fingerprint or both will contain false features which will not match with the imposter biometric features. Suppose that the attacker altered the V.txt file which contains the vault data or deleted it from the memory chip then the authorities can detect that the e-passport was tampered with because this attack will prevent decoding of the location map. Other attacks such as eavesdropping, clandestine tracking are not applicable in the proposed e-passport as RFID chips are not embedded in the e-passport.

8 Conclusion

In the framework of this paper, the authors developed a new method of coding and decoding biometric data, presented in the form of graphical files. The proposed algorithms allow processing a coded image with or without a very low loss of data value. The three presented schemes for encoding biometric data obtained from e-passports allow for no direct access to all this data. The only direct access to data in an e-passport is through the biostego image or stego-images (depending on the method of mapping) and V.txt file that contains a set of points to enable decoding of data using fingerprints fuzzy vault. The proposed schemes are so versatile that they can be used to hide other data in e-documents such as e-IDs, not necessarily e-passports. The presented schemes allow us to assume that this kind of encoding can significantly secure the e-passports or other kinds of e-documents from accessing by unauthorised people. Searching for the best method is totally explained by international situation. Increased traffic at airports, which is frustrated by the process of border controls makes such studies as set out above are fully justified. Transport and international communication depend on the efficiency of control systems of identity, in the opinion of the authors the presented schemes are a step in the right direction.

9 Acknowledgments

The work was completed under a GRAM grant, awarded in a competitive procedure by the Dean of the Faculty of Civil and Environmental Engineering, Gdansk University of Technology. The grants are funded from science funds as specified in Journal of Laws no. 96, heading 615, as amended.

10 References

[1] Bobkowska, K, Janowski, A, Przyborski, M, *et al.*: 'A new method of persons identification based on comparative analysis of 3d face models'. Proc. Int. Conf.: SGEM2016, Sofia, Bulgaria, 2016, vol. 2, pp. 767–774

[2] Bobkowska, K, Janowski, A, Przyborski, M, *et al.*: 'Analysis of high resolution clouds of points as a source of biometric data'. Proc. Int. Conf. Geodetic Congress (Geomatics), Baltic, Gdansk, 2016, pp. 15–21

[3] Jain, A.K., Ross, A, Prabhakar, S.: 'An introduction to biometric recognition', *IEEE Trans. Circuits Syst. Video Technol.*, 2004, **14**, (1), pp. 4–20, doi:10.1109/TCSVT.2003.818349

[4] Park, U, Tong, Y, Jain, A.K..: 'Age-invariant face recognition', *IEEE Trans. Pattern Anal. Mach. Intell.*, 2010, **32**, (5), pp. 947–954, doi:10.1109/tpami.2010.14

[5] White, D, Norell, K, Phillips, P.J., O'Toole, AJ: '*Human factors in forensic face identification*' (Springer International Publishing, Cham, 2017)

[6] Schomaker, L.: 'Advances in writer identification and verification'. Proc. Int. Conf on Document Analysis and Recognition (ICDAR), Parana, Brazil, 2007, pp. 1268–1273

[7] Juels, A., David Molnar, D., David Wagner, D.: 'Security and privacy issues in e-passports'. IEEE First Int. Conf. on Security and Privacy for Emerging Areas in Communications Networks, Athens, Greece, 2005

[8] Pattinson, N.: 'Securing and enhancing the privacy of the e-passport with contactless electronic chips'. Available at: pattison@axalto.com

[9] Jacobs, B.: 'Biometry in passports'. Availble at: http://www.sos.cs.ru.nl/research/society/passport/index.html

[10] BSI: 'Advanced security mechanisms for machine readable travel documents – Extended Access Control (EAC)'. Tech. Rep. TR-03110, Bonn, Germany, 2006

[11] Schouten, B., Jacobs, B.: 'Biometrics and their use in e-passports', *Image Vis. Comput.*, 2009, **27**, pp. 305–312

[12] Abid, M., Kanade, S., Petrovska-Delacretaz, D., *et al.*: 'Iris based authentication mechanism for e-passports'. 2nd Int. Workshop on Security and Communication Networks (IWSCN), Karlstad, Sweden, 2010

[13] Chabanne, H., Tibouche, M.: 'Securing e-passports with elliptic curves', *IEEE Secur. Priv.*, 2011, **9**, (2), pp. 75–78

[14] Wimalasiri, B, Jeyamohan, N: 'An e-passport system with multi-stage authentication: a casestudy of the security of Sri Lanka's e-passport', *Global J. Comput. Sci. Technol.*, 2018, **18**, pp. 14–20, ISSN:0975-4172. Available at: https://computerresearch.org/index.php/computer/article/view/1689, accessed 28 March 2019

[15] Saini, R, Narinder, R.: 'Comparison of various biometric methods', *Int. J. Eng. Sci. Technol.*, 2014, **2**, (I), pp. 24–30

[16] Pandit, A.S., Khope, S.R.: 'Review on image steganography', *Int. J. Eng. Sci.*, 2016, **6**, (5), p. 6115, doi:10.4010/2016.1480

[17] Akhtar, N, Khan, S, Johri, P.: 'An improved inverted LSB image steganography'. Proc. Int. Conf. on Issues and Challenges in Intelligent Computing Techniques (ICICT), Ghaziabad, India, 2014, pp. 749–755

[18] Kumar, A, Sharma, R.: 'A secure image steganography based on RSA algorithm and hash-LSB technique', *Proc. Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, 2013, **3**, (7), pp. 363–372

[19] Rawat, D, Bhandari, V.: 'A steganography technique for hiding image in an image using LSB method for 24 bit color image', *Int. J. Comput. Appl.*, 2013, **64**, (20), pp. 15–19

[20] Benhammadi, F, Beghdad Bey, K: 'Password hardened fuzzy vault for fingerprint authentication system', *Image Vis. Comput.*, 2014, **32**, (8), pp. 487–496, doi:10.1016/j.imavis.2014.04.014

[21] Bakhteri, R, Hani, M.K..: 'Biometric encryption using fingerprint fuzzy vault for FPGA-based embedded systems'. Proc. IEEE Region 10 Annual Int. Conf. (TENCON), Singapore, 2009

[22] Moon, D, Chung, Y, Seo, C, *et al.*: 'A practical implementation of fuzzy fingerprint vault for smart cards', *J. Intell. Manuf.*, 2014, **25**, (2), pp. 293–302, doi:10.1007/s10845-012-0656-3

[23] Nguyen, T.H., Wang, Y, Nguyen, T.N., *et al.*: 'A fingerprint fuzzy vault scheme using a fast chaff point generation algorithm'. Proc. IEEE Int. Conf. on Signal Processing, Communications and Computing (ICSPCC), KunMing, China, 2013, pp. 1–6, doi:10.1109/ICSPCC.2013.6664061

[24] Whitelam, C, Osia, N, Bourlai, T.: 'Securing multimodal biometric data through watermarking and steganography'. Proc. IEEE Int. Conf. on Technologies for Homeland Security (HST 2013), Waltham, USA, 2013, pp. 61–66

[25] Islam, M.N., Islam, M.F., Shahrabi, K.: 'Robust information security system using steganography, orthogonal code and joint transform correlation', *Optik*, 2015, **126**, (23), pp. 4026–4031, doi:10.1016/j.ijleo.2015.07.161

[26] Agrawal, N, Savvides, M.: 'Biometric data hiding: a 3 factor authentication approach to verify identity with a single image using steganography, encryption and matching'. Proc. IEEE Conf. on Computer Vision and Pattern Recognition (CVPR 2009), Miami, USA, 2009, pp. 85–92

[27] Tarif, E.B., Wibowo, S, Wasimi, S, *et al.*: 'A hybrid encryption/hiding method for secure transmission of biometric data in multimodal authentication system', *Multimedia Tools Appl.*, 2017, **77**, pp. 1–19

[28] Dogan, L.: 'A new data hiding method based on chaos embedded genetic algorithm for color image', *Artif. Intell. Rev.*, 2016, **46**, (1), pp. 129–143, doi:10.1007/s10462-016-9459-9

[29] Karolinska: 'Directed Emotional Faces (KDFE)'. Available at: http://kdfe.se

[30] Uludag, U, Pankanti, S, Jain, A.K..: 'Fuzzy vault for fingerprints'. Int. Conf. on Audio-and Video-Based Biometric Person Authentication, Heidelberg, Berlin, 2005, pp. 310–319

[31] Barni, M.: '*Document and image compression*' (CRC press, Boca Raton, 2006)

[32] Nandakumar, K, Jain, A.K., Pankanti, S.: 'Fingerprint-based fuzzy vault: implementation and performance', *IEEE Trans. Inf. Forensics Sec.*, 2007, **2**, (4), pp. 744–757, doi:10.1109/TIFS.2007.908165

[33] Viola, P, Jones, M.: 'Rapid object detection using a boosted cascade of simple features', *Comput. Vis. Pattern Recognit.*, 2001, **1**, pp. I-511–I-518. doi:10.1109/CVPR.2001.990517

[34] Narayanan, A.: 'Fingerprint minutiae extraction', 2011. Available at: https://www.mathworks.com/matlabcentral/fileexchange/31926-fingerprint-minutiaeextraction/content/Fingerprint_Minutiae_Extraction/Minutiae_Extraction.m

[35] Daugman, J.: 'How iris recognition works', *IEEE Trans. Circ. Syst. Video Technol.*, 2004, **14**, (1), pp. 21–30

[36] Vatsa, M., Singh, R., Gupta, P.: 'Comparison of iris recognition algorithms'. Int. Conf. on Intelligent Sensing and Information, Chennai, India, 2004, doi:10.1109/ICISIP.2004.1287682

[37] Welstead, S.T.: '*Fractal and wavelet image compression techniques*' (SPIE Publication, Bellingham, 1999). ISBN:978-0-8194-3503-3

[38] Hamzaoui, R., Saupe, D.: 'Fractal image compression', in Barni, M. (ed.): '*Document and image compression*', vol. **968**, (CRC Press, Boca Raton, 2006), pp. 168–169. ISBN:9780849335563, accessed 5 April 2011

MOST WIEDZY Downloaded from mostwiedzy.pl

© The Institution of Engineering and Technology 2019

11 Appendix

Uniqueness proof of the location map:

i. The probability to select a biostego image out of three biometric images = 1/3
ii. The probability to select a mapping scheme = 1/3
iii. The probability for a pixel to represent set of k-nearest neighbouring pixels $\frac{1}{|V_{ij}^k|}$
iv. For image of size $N \times N = \left(\frac{1}{|V_{ij}^k|}\right) N^2 = \frac{1}{|V_{ij}^k|^{N^2}}$, in case there is one location map for a grey scale biostego image, then the probability for two e-passports or e-IDs to have the same location map = $1/3 \times 1/3 \times \frac{1}{|V_{ij}^k|^{N^2}} = \frac{1}{9|V_{ij}^k|^{N^2}} \leq \frac{1}{|V_{ij}^k|^{N^2}} \leq 0$
v. In case there is three location maps one for each colour channel of the biostego image, then the probability for two e-passports or e-IDs to have the same location map $\frac{1}{|V_{ij}^k|^{N^2}} \leq 0$, where:

- $N \times N$ is the size of biometric image,
- $\frac{1}{|V_{ij}^k|^{3N^2}}$ is the set of k-nearest neighbouring pixels in the biostego image that have the same intensity values of the input pixel in the biometric image,
- k is the number of neighbouring pixels in the V_{ij}^k set.

MOST WIEDZY Downloaded from mostwiedzy.pl

© The Institution of Engineering and Technology 2019