IMAGE CONTENT SOFTWARE ANALYSIS

HAMBALÍK Alexander – MARÁK Pavol, SK

Abstract

This contribution provides an overview of present methods for processing and verifying authenticity of digital images. It also discusses a topic of fingerprint image processing. Their appropriate application allows to reveal modified image parts before being released to public. Moreover, they help us perform an automated comprehensive analysis of fingerprint image properties that is still a challenging task in the field of forensic science.

Key words: image content analysis, authentication, fingerprint image properties.

SOFTVÉROVÁ ANALÝZA OBSAHU OBRAZOV

Resumé

Príspevok uvádza prehľad v súčasnosti používaných metód na spracovanie a obsahovú analýzu overovania pravosti (autenticity) obrazov a spracovania daktyloskopických vzorov. Ich vhodná aplikácia v praxi uľahčí ešte pred vydaním odhaliť v dokumentoch určených na zverejnenie (napr. v článkoch, záverečných prácach, súdnych dokumentoch zmenené obrazy. Okrem toho dovolia realizovať aj automatizovanú, v daktyloskopii doteraz úplne absentujúcu hromadnú a podrobnú obsahovú analýzu daktyloskopických stôp.

Kľúčové slová: analýza obsahu obrazov, autentifikácia, vlastnosti odtlačku prsta.

Introduction

A photography technology brought a possibility to capture a world around us. In comparison to drawn pictures, a digital image recording is fast and depicts a true form of real objects with existing technology limitations and drawbacks. In post-processing, we sometimes need to edit, create magnified details, use cropped image parts and eliminate unwanted defects. Existing approaches can be misused to intentional image content modifications. Analogous photography is rarely used in present but they have not disappeared totally with arrival of digital recording and processing devices. On the contrary, they expanded in a considerable extent. Image editing using scanners, computers and photo editing software offer literally unlimited possibilities. A positive image is created directly while using these technologies with no need for a negative image. Therefore, additional changes are hard to detect. If they are used as evidence in written documents (scientific papers, dissertations, master and bachelor theses, etc.) or in investigation procedures, it is not an easy task to reveal an indiscernible falsification optically, by a naked eye or using magnifying glass. Digital equipment helps us a lot in this direction. Falsification and detection methods are being still developed. They are based upon assorted principles. It is easier to detect modifications in records made and added automatically by the device. These can be altered easily. There are more sophisticated approaches based on searching image details. Monochromatic image processing and feature extraction can be viewed as their special case. In this paper, we briefly review these technologies based on our acquired experience. Listed examples reflect the ongoing research in this area. They are outcomes of algorithms developed and tested by us (we also tested algorithms developed by other authors). They serve primarily for a detection of forged images in a batch mode. This is suitable for publishers or fingerprint analysis for scientific purposes.

1 An overview of most widely used image details processing techniques

From the moment of selection of an object being shot and triggering the image recording to storing the image in memory, a rather complex process involving a number steps is executed. Each processing stage is irreplaceable and usually adds some distinctive features to the resulting record. Some of these features are related to specific technical solution of image processing. These traits are typical for a specific manufacturer or his product family produced at given time and reflect a technical progress of the particular time. Other traits characterize particular element that has been used in the processing and adds unique features to the record in similar manner as human leaves his or her fingerprints on real world things. There are no two lens that would be completely identical in all their properties even if made the same way. Similarly, one cannot find two exactly the same images recorded by the semiconductor chips of the same series. Therefore there is a wide range of distinctive features in digital images suitable for the detection of image modification without the knowledge of the original digital record. However, it is difficult to extract and examine all these features reliably. Virtually these features cannot be modified additionally and their analysis requires complex methods and software tools.

Besides them, the record is enriched by metadata, for example a time of record, aperture size, shutter speed, image serial number, etc. It is similar in case of computer-generated images or various diagnostic equipment. Unfortunately, data automatically added by a device can be additionally modified with relative ease leaving no traces of intentional manipulation. Digital records can be well separated and processed. Mostly, their informative value is considered less valuable than in case of unalterable characteristics.

For reliable detection of intentional or unintentional modifications of a record we need to carry out a procedurally complex, time consuming, detailed image content analysis. By following a correct procedure, image content may expose much information about possible modifications. Shape discrepancies (object dimension proportions, irregularities in color ambience, inappropriate orientation from perspective viewpoint, unusual shadow placements or lens distortions, etc.) can help us discover unwanted image modifications. Shape discrepancies (object dimension proportions, irregularities in color ambience, inappropriate orientation from perspective viewpoint, unusual shadow placements or lens distortions, etc.) can help us discover unwanted image modifications.

Most common methods of creation of digital image forgery:

- object removal in the picture
- adding new object
- object modification
- metadata modifications (editing of saved data created by the device but not visible in the image)

There are many various forms of image content protection (active or passive). These are difficult to use in case of individually recorded images. Author can change their content prior to application of protection, thus subsequent use of protection is ineffective. Devices creating digital photos normally do not possess this kind of protection. Image content check for possible additional changes is still the only real option.

For analysis purposes we mostly implement principles that employ e.g.:

- Characteristic lens imperfections – various focusing of the light ray depending on color, called chromatic aberration, image distortion etc.
- Characteristic sensor imperfections – native resolution, sensitivity (expressed by ISO number) depending on color (light ray frequency).

- Characteristic sensor noise – depends on the amount of falling light, color, temperature and type of sensor semiconductor.
- Properties of saving or compression algorithms (file formats – lossy and lossless conversions)
- Perspective analysis
- Illumination direction analysis
- Object analysis (dimensions, object orientation, their linkage to ambient objects, etc.).
- Bitmap content analysis (abrupt color gradient changes in neighboring image areas, etc.).
- Analysis methods based on SVM (Support Vector Machine).

At our institute, we try to find appropriate and easy-to-deploy methods for detection of additional changes in digital images. Besides design of our own methods we evaluated various techniques proposed by other authors. From the obtained experience it might be easily inferred that the majority of them can be used with limitations. Most likely, just one method is not capable of detection of all possible image modifications. A final decision on the significance of discovered modifications is made by a specialist based on software analysis results. We have not yet discovered an algorithm for fully automated image content assessment.

Images in printed form are hardest to analyze because we need to digitize them once more (e.g. using scanners). Upon storing, original metadata are not renewed. In this case, a method of analysis based on these metadata cannot be used. Even methods based on analysis of properties of object contour color transitions are not reliable. During scanning these properties are changed with the added noise (paper, coloring and scanner properties). A solution to this problem is presented by object detection methods. They analyze object attributes like light conditions, inclusion to perspective, dimension disproportions, etc.

We have investigated these methods recently. In one of them, SIFT [1,2] algorithm was used. This is used in cases when image forgery was achieved by image part copying. There is another method called SURF. Unfortunately, we have not tested it yet. A server application accessible through a web interface detects key points in image and based on them it is able to find all similar parts (a multiple copying). In a reasonable timeframe, it is able to detect relatively small changes even in case when a copied part was geometrically transformed (zoomed in, zoomed out, stretched, rotated, compressed, etc.).

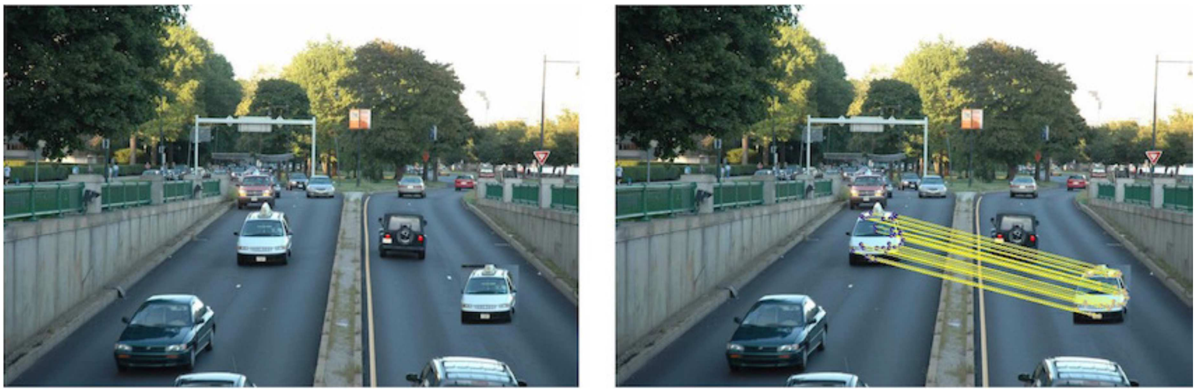

Fig. 1 - Copied image part (on the left) detected by our software (on the right)

We created a working software solution that is being currently tested. We used MICC-F220 image database as a testing sample. It consists of 220 images in dimensions ranging from 720x480 to 800x600 pixels. On average, there is 1,2 % share of copied image parts in the original image, out of which 110 are original images and 110 are changed in copy-move way. It also consisted of images whose copied and pasted parts where geometrically transformed (skewed, rotated or with changed dimensions).

We measured a detection success rate by TPR coefficients (True Positive Rate) and FPR (False Positive Rate). TPR coefficients represent a ratio of correctly identified forged images to total number of forged images in database. FPR coefficient expresses a ratio of number of unaltered images falsely identified as altered to total number of unaltered images. We divided examined image to smaller parts (clusters). If the software finds at least 3 key points in one cluster with corresponding counterparts in different cluster, then the examined image is evaluated as forged. Software cannot determine the importance of the image modification in terms of analysis objectives. The final decision is always made by an expert according to the obtained results.

After fine tuning (with 0,6 threshold value), our software [3] achieved a level of TPR=100 %, thus correctly marking all altered images, but FPR=14,58 % at the same time. It means it classified 16 unaltered images out of original database as altered. After closer examination, we found that the software was confused by very similar, often symmetric details like window frames, wall decorations, advertisement banners, etc.

At the threshold of 0,5 we achieved TPR=95,45 % (105 out of 110 images) along with FPR=7,72 % (8 out of 110 images). During testing, the threshold value was set to 0,4 – 0,6 range. The lower the value was set, the more altered images were not detected by the software. On the other hand, less original images were flagged as altered.

The average computation time was 108 seconds. This time is acceptable even in a batch mode. We used a common PC for testing purposes. In case of powerful server computers, this time may be considerably lower.

Except shape similarity, we also examined light conditions used to reveal additional changes. Image analysis based on object illumination can be carried out in different ways. In our case we chose a solution in which we examine effect of direct or reflected illumination on the object. More specifically, we analyzed an amount of light reflected by the subsurface part of object exposed to light source. Mathematical description employs Shafer's light reflection model.

The current version of application suffers problems with correct highlighting of illuminated surfaces. Therefore, updates in the present algorithms are inevitable.

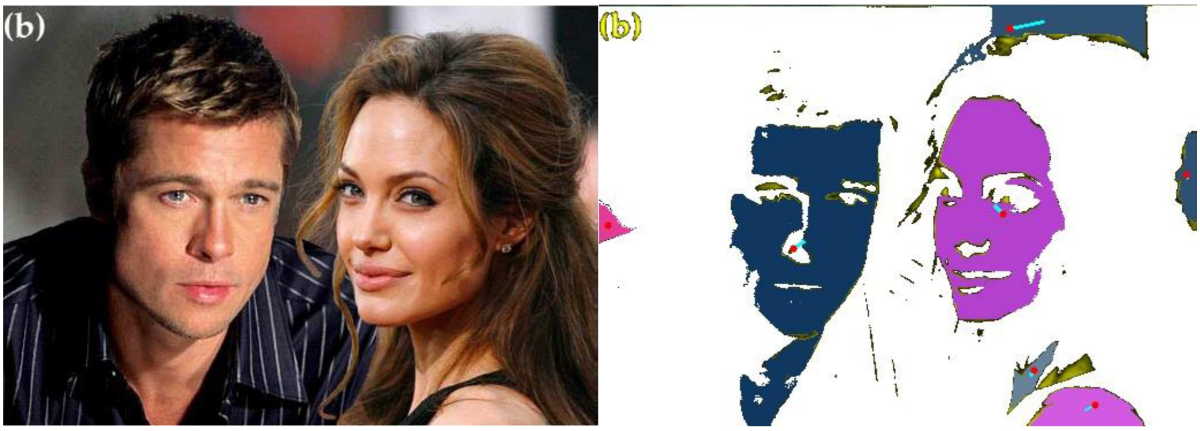

Fig. 2 – Forged image (on the left) and its light conditions indicated by our software (on the right)

2 Fingerprint image processing and analysis

Biometric recognition has become a strong part of security mechanisms and more or less it starts to replace traditional authentication methods. Firstly, it provides user convenience and expected higher security based on the premise of uniqueness of biometric trait that is used for a recognition in an automated manner. Fingerprints are well known anatomical traits with a long history. Besides this, fingerprints possess many characteristic information, are easy to capture and can be found on items of everyday use making them a valuable trace in criminal investigation. Their popularity has grown so much that their manual processing was replaced by automated computer systems. Many specialized algorithms have evolved to solve a difficult task of representing, processing and analyzing fingerprint patterns that are considered to be unique. In this section we would like to briefly review current existing approaches to fingerprint image processing, namely image enhancement and feature extraction. These two areas form a part of sequential scheme of general fingerprint processing as can be seen in Fig. 3.

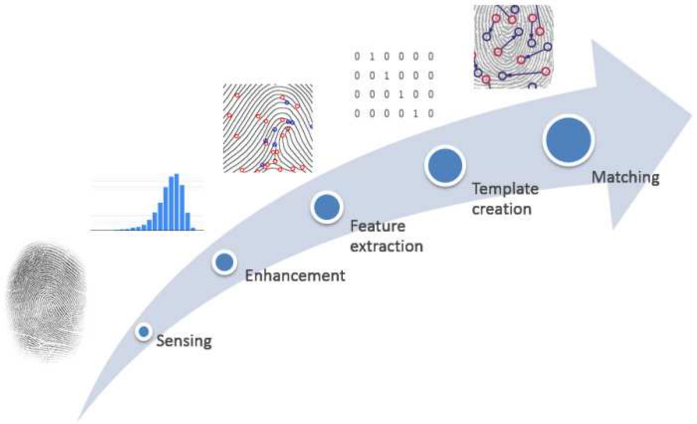

Fig. 3 - Automated fingerprint processing stages

Biometric recognition has become a strong part of security mechanisms and more or less it starts to replace traditional authentication methods. Firstly, it provides user convenience and We have recently started a couple of research activities at the Institute of Computer Science and Mathematics concerning development of software solutions for demonstration of performance of various fingerprint enhancement methods as the fingerprint quality is generally a crucial problem in the field of automated fingerprint recognition and indicates a reliability of particular technology. What is more important to state, is our efforts in the area of fingerprint feature extraction algorithm development. We published several papers dedicated to novel methods of fingerprint feature extraction that focus on automated detection of rare features present in the patterns made by friction ridges. We try hard to interconnect students of bachelor and master studies to develop new and established methods of both enhancement and feature extraction in their final theses. By doing so, our intention is to build a complex expert software system for fingerprint analysis that could be eventually used on a professional level in forensic area. The Institute of Forensic Science in Bratislava is our long-term research partner and collaboration with such a highly trained experts give us a lot of experience and help us navigate in our research in a way that is respected worldwide.

In this paper we primarily focus on the most important results of our research. In the first part we discuss our implementation of enhancement techniques where contextual filtering is the most prominent one. After, we describe techniques of minutiae extraction based on traditional pixel-wise methods and on the other hand, there are machine learning approaches with neural networks. This overview is presentation of results obtained by authors themselves and students they have supervised.

Fingerprint enhancement methods

Before going deeper in the topic we consider it important to define levels of fingerprint features. In general there are 3 levels of fingerprint features. Level-1 features are visible ridge flow patterns that are used for rough classification purposes only. Overall ridge flow normally fall within one of the categories: arc, loop and whorl. Level-2 features are local ridge characteristics sometimes called minutiae. In Fig. 4 we can see classification scheme of minutiae provided by the Institute of Forensic Science in Bratislava, Slovakia. They are associated with their relative frequency they occur in Slovak population represented by 1 000 sample fingerprint images.

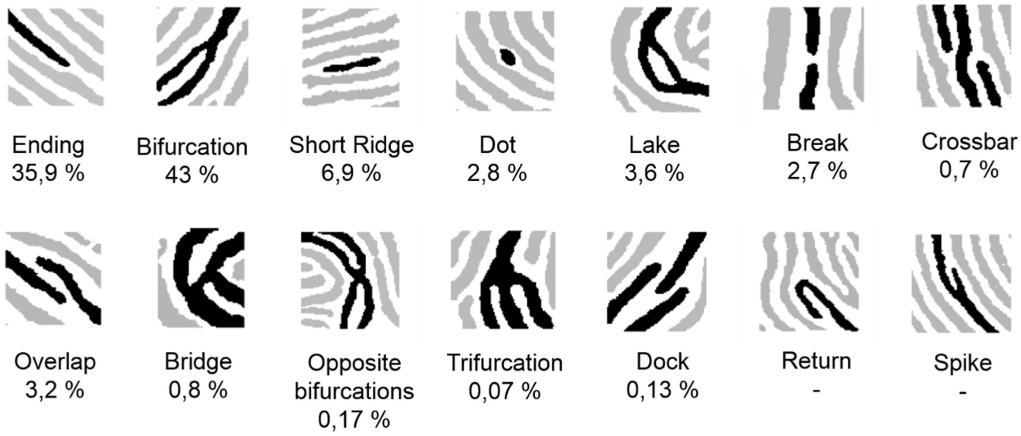

Fig. 4 - Minutiae classification

As frequency determines the significance and strength of particular minutia, it is obvious that lower frequency minutiae are more characteristic to represent a fingerprint. In our research we put the accent on implementing methods that can handle extraction of these low frequency, thereby valuable patterns. Unfortunately, this is not an easy task. Many existing algorithms focus just on detection of ending and bifurcation point, leaving the complex patterns ignored. Therefore, we have designed several techniques to analyze ridge patterns in more complex way to obtain features like short ridges, lakes, breaks and even more.

Before extraction can be performed, a well-designed enhancement process is needed to be employed. Fingerprints are patterns of varying quality, mostly making it impossible to extract features in the original form. In this section we propose a scheme of our enhancement algorithm (see Fig. 5) that has been created based on numerous experiments with many methods. The result of the enhancement is fingerprint skeleton – a most widely used compact fingerprint representation discarding all unnecessary image information and leaving just ridge pixels thinned to one-point thickness.

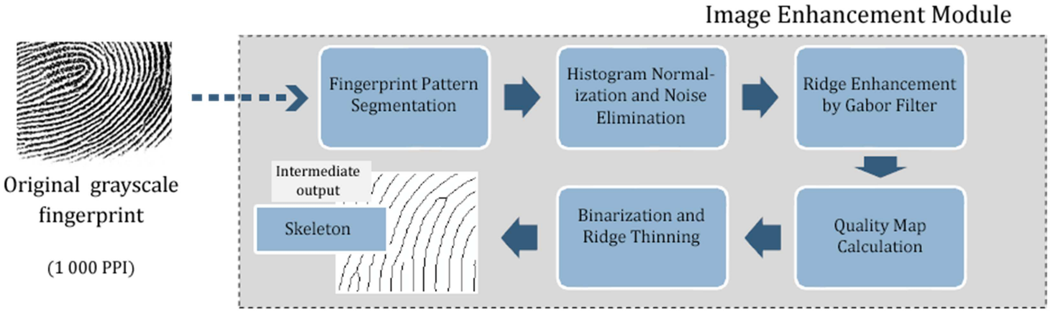
Image Enhancement Module
Original grayscale fingerprint
(1 000 PPI)
Fingerprint Pattern Segmentation
Histogram Normal-ization and Noise Elimination
Ridge Enhancement by Gabor Filter
Quality Map Calculation
Binarization and Ridge Thinning
Intermediate output
Skeleton

Fig. 5 - Fingerprint enhancement procedure

First step of fingerprint enhancement is segmentation, in which a fingerprint pattern is separated from the background. This means we discover only useful pixels that are later processed. It is also helpful in terms of reducing time complexity of subsequent processing steps. After fingerprint is segmented, image contrast is enhanced by normalizing histogram. The result is an image with clear difference between ridges and valleys. To suppress noise or small particles we apply noise removal techniques based on common image filters. The most important step is filtering the image by contextual filters. So far, we have extensively tested two types of filters: Gabor filter and filtering in the Fourier domain. By applying convolving Gabor filter with the image we obtain a new image that is enhanced in terms of ridge orientation and local ridge shape. This way eliminate major noise artifacts and recover the clarity of the ridges by assigning similar color to ridge pixels. Gabor filtering is a rather difficult task preceded by analytic stage where one must determine local orientation and frequency in fingerprint. Local frequency is stored in an orientation map and frequency is stored in a frequency map. An example of Gabor filtering is shown in Fig. 6.

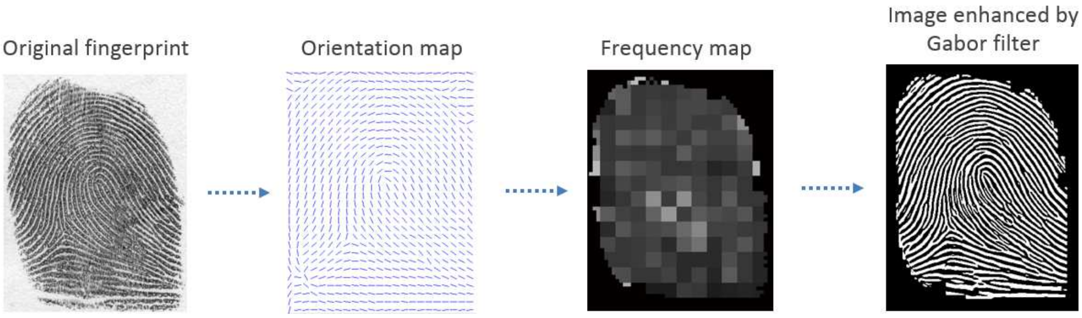

Fig. 6 - Stages of Gabor filtering

An alternative to Gabor filter is Fourier domain filtering that first decomposes image into its frequency components. Following this, a signal power spectrum is filtered by using a specific mathematical operation. According to our results, Fourier filtering is outperformed by Gabor filter as it damages fingerprint pattern in such an extent that majority of minutiae is lost. Fingerprint quality map describes local orientation coherence that reveals poor quality regions. These regions are flagged as areas of higher uncertainty in minutiae extraction stage. Binarization of fingerprint converts the image colors into two colors: black and white. Upon binarization, we create the skeleton image by applying morphological processing algorithms. In skeleton, all ridge lines are reduced to one-point curves that makes it better for computerized analysis. Skeletal form of fingerprint is the starting point for all the algorithms to be presented in the following section.

Fingerprint feature extraction methods

From among more existing approaches to fingerprint feature extraction we narrow our examination to three selected methods as they each represent fundamentally different solutions. First method to mention is minutiae extraction based on skeleton images. Traditional simple skeleton analysis involves detection of ridge bifurcations and endpoints. It scans black pixels and investigates pixel neighborhood containing 8 pixels. It is an easy task to discover a minutia point as it merely depends on how many black neighbors are connected to the pixel in question. This method is known as Crossing Number. Its capability does not allow us to detect larger or more complex patterns that occur in fingerprint. An example of minutiae extraction by Crossing Number method is depicted by Fig. 7.

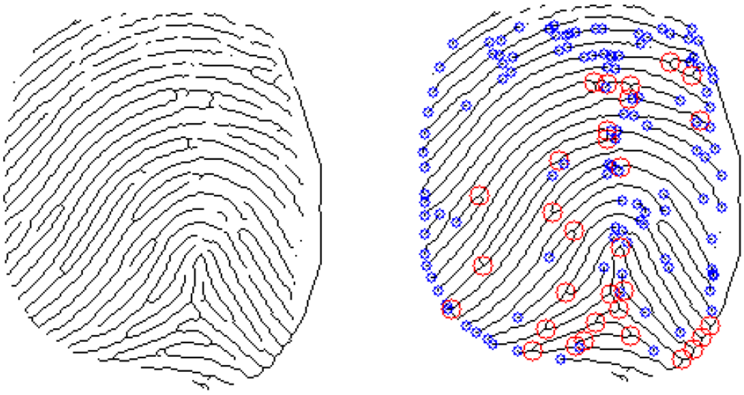

Fig. 7 - Minutiae located by Crossing Number method

To add extended capabilities of minutiae extraction we further developed skeleton image analysis by incorporating measurement of ridge length, evaluating placement of ridges and also employed an idea of complex shape recognition in the inverse skeleton image. Fig. 8 illustrates a principle of extraction of bridge and lake minutiae. The illustration shows original minutiae shape formed by the black ridges and corresponding inverse pattern. In both cases, a configuration of two bifurcations can be replaced by a configuration of two endpoints that is, in fact, easier task for any algorithm analyzing skeleton image.

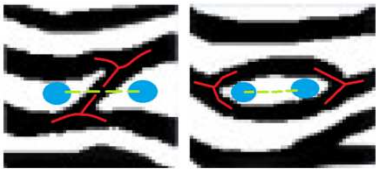

Fig. 8 - Complex minutiae and the corresponding inverse image

By employment of ridge length analysis we were able recognize patterns like isolated point and short ridge as we examined the length given as multiples of average distance between two consecutive pores along the ridge. An example of minutiae extracted using ridge length analysis is presented in Fig. 9. Picture on the left is a demonstration of ridge division into segments formed by the pores (a value of 10 pixels corresponds to resolution of 1 000 ppi). Second picture is the original skeleton. Third picture shows the resulting minutiae found by Crossing Number method (only bifurcations and endpoints). The last picture is the output of extraction process where five minutiae types were discovered.

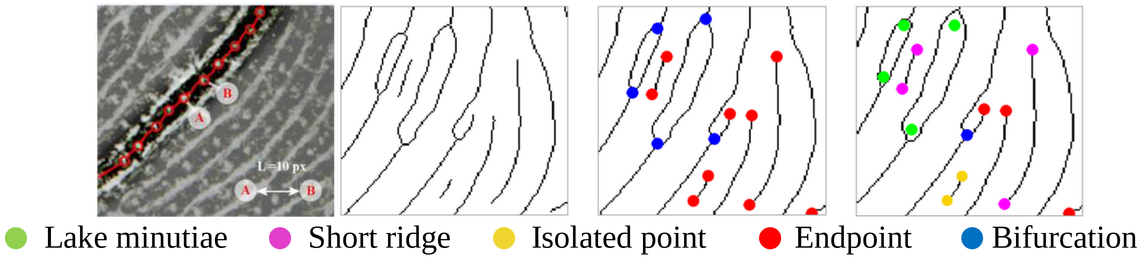

Fig. 9 – Extraction of minutiae using ridge length analysis

A completely different approach to minutiae extraction is tracking the contours of ridges in a binary fingerprint image. Here the task is to evaluate a curvature of the local ridge segment. So far, only a simple technique for ridge bifurcation and endpoint detection has been proposed. In counterclockwise tracing, ridge endpoint creates a significant left turn and ridge bifurcation creates a significant right turn.

Finally, extraction performed by neural networks has been developed. This approach takes the advantage of complex function approximation and fault tolerance that is offered by the neural networks. We constructed a neural network consisting of an input layer that takes image block pixels, one hidden layer and one output layer that serves as decision making unit. The original skeleton is divided into the blocks. Block pixels are distributed to neural network and classified into one of three classes. These classes represent complex minutiae: bridge formation, ridge break and opposite bifurcations. The critical stage was network training where we need to assemble sufficient number of training samples to make neural network learn variable patterns associated with the same class. The constructed network turned out to be a reliable minutiae classifier. The accuracy depended heavily on the quality of training data. This way we presented a promising research direction for future generation of algorithms of unique fingerprint data extraction.

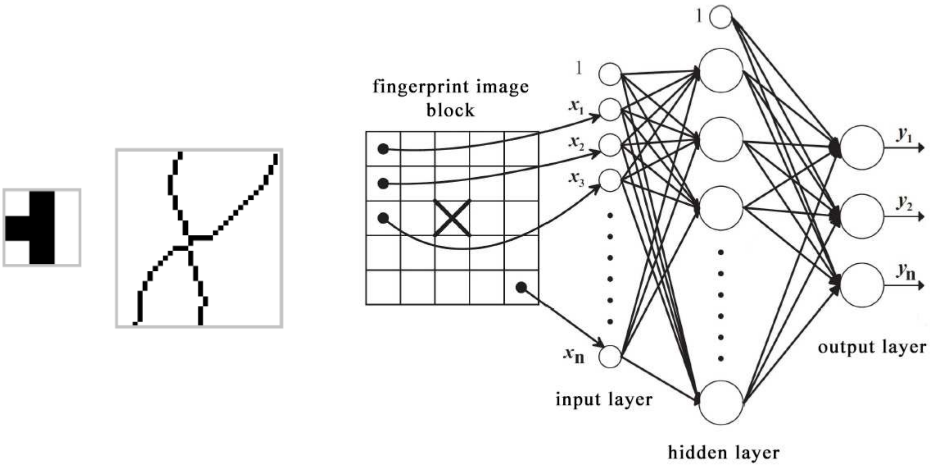

Fig. 10 - Neural network designed to recognize minutiae patterns

Conclusion

In this contribution, we provided an overview of principles and methods for digital image content analysis including a special case of automated fingerprint analysis. Most of them were tested using our own software. In some occasions, we used algorithms taken from the literature, but more often we applied our own algorithms. In case of fingerprint analysis we presented some of the unique solutions for recognition of complex minutiae that overcome existing solutions in terms of detection capabilities. Experience gained from creating and evaluating applications is the core of this paper. All the experience indicate that so different software applications like image forgery detection and fingerprint analysis have many features in common, but there are also specific characteristics. Used principles and algorithms were examined in terms of automatic analysis for purposes of scientific research or possibilities of deployment in publishing and authorization processes. We also investigated possibilities of verification of digital image appendices included in final theses and scientific papers. In contrast to text sections of documents, they are not subject to originality control.

This research was supported by:

- Ochrana osobných údajov v mobilných zariadeniach 2013-2015 Projekt: grant VEGA 1/0173/13.
- STU grant: *Pokračujúce projekty na podporu excelentných mladých výskumníkov*, project: Rozšírená softvérová extrakcia charakteristických vlastností daktyloskopických vzorov, acronym: FingerDetective2014

Literature

1. AMERÍNY, L et. al., *A SIFT-based forensic method for copy-move attack detection and transformation recovery.* IEEE Transactions on Information Forensics and Security, vol. 6, issue 3, pp. 1099-1110, 2011.
2. LOWE, D. G. *Distinctive Image Features from Scale-Invariant Keypoints,* Computer Science Department. University of British Columbia, January 5, 2004.
3. TKÁČIK, P. *Automatizovaný sieťový systém efektívneho rozpoznávania originality obrázkov.* [Master thesis – supervised by A. Hambalík], FEI STU Bratislava : Bratislava, 2015.
4. GRZNÁR, M. *Biometrické rozpoznávanie identity: odtlačky prstov a algoritmy ich predspracovania.* [Bachelor thesis – supervised by P. Marák], FEI STU Bratislava : Bratislava, 2015.
5. HOFERICA, O. *Možnosti využitia neurónových sietí v biometrických systémoch pracujúcich s odtlačkami prstov.* [Bachelor thesis – supervised by P. Marák], FEI STU Bratislava : Bratislava, 2015.
6. MALTONI, D. et al., *Handbook of Fingerprint Recognition: Second Edition.* London: Springer, 2009. 496 p. ISBN 978-1-84882-253-5.

Contact address:

Ing. Alexander Hambalík, PhD., Ing. Pavol Marák
Institute of Computer Science and Mathematics
FEI Slovak University of Technology, Ilkovičova 3
e-mail: alexander.hambalik @ stuba.sk, pavol.marak @ stuba.sk
tel.: +421 2 60298 104