Proceedings of the 5th WSEAS International Conference on Signal Processing, Istanbul, Turkey, May 27-29, 2006 (pp185-190)

Lossless Compression of Biometric Image Data

ROUMEN KOUNTCHEV
Radiocommunications Dept.
Technical University of Sofia
Bul. Kl. Ohridsky, 8,
Sofia 1000
BULGARIA
http://www.tu-sofia.bg

VLADIMIR TODOROV
ROUMIANA KOUNTCHEVA
T&K Engineering
Mladost 3, POB 12
Sofia 1712
BULGARIA

MARIOFANNA MILANOVA
Computer Science Dept.
University of Arkansas
at Little Rock
2801 S. University Ave.
AR, 72204, USA
http://www.ualr.edu

Abstract: In the paper is presented a new approach for solving some of the authentication problems in large computer systems, communication networks and mobile communications, using a new method for lossless compression of some kinds of biometric information (fingerprints and signature images). The image processing is based on two-level Inverse Difference Pyramid (IDP) Decomposition with 2D Walsh-Hadamard Transform, followed by Histogram-Adaptive Run-Length data coding. In the paper are presented the comparison results, obtained for large number of test images of the pointed image classes. The investigation was performed with software products, based on the new method, on the JPEG 2000 standard (lossless version) and on the FBI compression standard. The new method attains high compression ratio and this is a basis for the future method development and implementation in security systems, which require fast and reliable user authentication. In the paper is presented a specific approach for digital watermarking based on the IDP and using the biometric data as a watermark.

Key words: Inverse Pyramid Decomposition, Biometric data processing, Lossless compression, Digital watermarking

1. Introduction

Problems like user authentication in the communications networks and mobile communications are of great importance. The main objectives of the network security are to protect all kinds of computer system resources from unauthorized, illegal, unwanted access, use, modification, or theft. The basic tools widely used for countering a security threat are secure rooms, passwords, access privileges, etc. But just having a valid user code and password does not necessarily prove the real user's identity and most reliable are the techniques based on the biometric data verification [1,2]. There are only three physical characteristics of the human body, which have the uniqueness necessary to provide absolute positive identification rather than a high probability of positive identification: the fingerprint, the retina of the eyeball (retinal scan), and the iris of the eyeball (iris scan). Another popular approach is the visual comparison of an individual's signature, which has been used for many years as a method of identification and is now popular for electronic comparison in which signature dynamics such as pressure, speed, and direction of pen stroke are measured. The pointed methods have one general disadvantage – they all need plenty of data to ensure reliable authentication and this is the main factor, which contributes to the basic problems related with the implementation of biometric information use:

- the slow data transfer, resulting from the large amounts of data needed for the authentication;
- the slow decision speed due to processing technologies that create lack of productivity, waiting lines, and frustration on the part of the persons being authenticated;
- the requirement to maintain large databases containing this data.

In order to solve these problems the archived biometric data is compressed using different techniques, which as a rule are based on DCT or wavelet transforms and in general decrease the image quality to some degree [3].

The method for lossless image compression, presented here, ensures high compression ratio of the biometric data and as a result enables the faster transfer of the information, needed for the authentication. The method is applicable in both computer systems and mobile communications.

Another reliable tool for data protection is the digital watermarking. The efficient new lossless

compression permits to develop watermarking techniques with biometric data embedding.
The paper is arranged as follows: section 2 presents the new Inverse Difference Pyramid (IDP) method for image decomposition and the algorithm for lossless data compression; section 3 presents the results obtained with the new method and the comparison with other widely used methods; section 4 points the ability to hide the compressed information or to use it as a digital watermark, and section 5 (Conclusion) presents the basic method advantages and its abilities for future applications in systems which require user authentication with highest reliability.

2. Lossless image data compression with Histogram-Adaptive Run-Length Coding (HARLC)

The basic requirements for the image compression algorithms are: 1) the big compression ratio; 2) the high quality of the restored image; and 3) the low computational complexity. As it is known [3], in practice are used some specially developed methods for lossless data compression. Most of them are based on the large number of same values in the processed data and their coding, as a rule is some kind of run-length or arithmetic coding. The inefficiency of the conventional approach is mainly a result of too many symbols being involved in the coding. Another general disadvantage is that these methods are not adaptive to input data statistics. In order to achieve higher efficiency some authors [4] developed modifications, which better suit the processed data.

The method for still image compression, presented here, solves these problems to a high degree. The image processing comprises two basic steps: Inverse Difference Pyramid (IDP) decomposition [5], followed by lossless coding of the obtained data. The IDP decomposition is performed as follows: the original image [B] with size m×n pixels is divided in K square sub-images with size 8x8 pixels and after that each sub-image is processed with two-dimensional (2D) orthogonal transform:

$$\hat{s}_0(u,v)=\begin{cases}\sum_{i=0}^{7}\sum_{j=0}^{7}B(i,j) & \text{for } u=v=0;\\ \sum_{i=0}^{7}\sum_{j=0}^{7}B(i,j)(-1)^{\lfloor j/4\rfloor} & \text{for } u=0, v=1;\\ \sum_{i=0}^{7}\sum_{j=0}^{7}B(i,j)(-1)^{\lfloor i/4\rfloor} & \text{for } u=1, v=0;\\ \sum_{i=0}^{7}\sum_{j=0}^{7}B(i,j)(-1)^{\lfloor i/4\rfloor+\lfloor j/4\rfloor} & \text{for } u=v=1;\\ 0 \quad - & \text{for } u,v=2,3,..,7,\end{cases} \qquad (1)$$

where B(i,j) is a pixel of the sub-image and $s_0(u,v)$ is a transform coefficient (here, the example is for a grayscale image and the used 2D transform is Walsh-Hadamard transform, WHT). To obtain the lowest "zero" IDP level are used only 4 coefficients, corresponding with the lowest spatial frequencies. The values of these transform coefficients comprise the initial level of the pyramid decomposition. Then the image is restored with inverse WHT, using the values of the participating transform coefficients only, and is calculated the difference between the original and the restored image. The obtained difference image is divided in sub-images with size 4x4 pixels and similar operations are performed again. In order to build the second (higher) pyramid level are used all transform coefficients, so that to ensure the unchanged quality of the restored image. These operations are performed in accordance with the relations:

$$[E(i,j)]=[B(i,j)]-[\hat{B}(i,j)]=\begin{bmatrix}[E_1] & [E_2]\\ [E_3] & [E_4]\end{bmatrix} \qquad (2)$$

$$[\hat{B}(i,j)]=(1/64)[H(8)][\hat{s}_0(u,v)][H(8)] \qquad (3)$$

$$[s_1^k(u,v)]=[H(4)][E_k(i,j)][H(4)] \quad \text{for } k=1,2,3,4 \qquad (4)$$

where: $[\hat{B}(i,j)]$ is the sub-image approximation;

[H(N)] is a Walsh-Hadamard matrix of size N×N;

$s_1(u,v)$ is a transform coefficient.

The calculated IDP coefficients' values are arranged as one-dimensional sequences in accordance with their spatial frequency. Each sequence contains the values of coefficients, corresponding with same spatial frequency from all sub-images in one IDP level.

Then the obtained data is processed with Histogram-Adaptive Run-Length Coding (HARLC). This part of the processing is based on one of the specific features of the image data processed with IDP and 2D Walsh-Hadamard transform, that in result of the IDP decomposition the values of most of the coefficients (in particular – in the higher pyramid level) are "zero". The basic steps of the algorithm for lossless coding are as follows:

- The processing starts with the calculation of the histogram $h(\Delta S)$ of the coefficients values in the data sequence $\{\Delta S\}$;
- The histogram is analyzed and are defined the parts, where $h(\Delta S)=0$.
- The sequences of same values (most frequently equal to zero) in the sequences $\{\Delta S\}$ are presented with some of the not-used histogram values in accordance with the following rules:

- Sequences of zeros, with length smaller or equal than that of the longest sequence of not used values

Proceedings of the 5th WSEAS International Conference on Signal Processing, Istanbul, Turkey, May 27-29, 2006 (pp185-190)

in the histogram, is replaced by a number, equal to the sum of the start value of the sequence of not used values and the length of the compressed sequence;

- Sequences of zeros in the transformed data, longer than the sequence of not used values in the histogram, but shorter than 2^{mn}, are represented with 2m words. The first of these words contains the start value of the longest sequence of not used values, the next (m-1) words contain zeros, and the remaining words – the length of the coded sequence;
- Sequences of same values, different from zero, are represented in similar way, adding one more word, containing this value.
- Very long sequences (if there are any) are represented with additional word containing the sequence length;

- At the end of the processing the code words are coded with modified Huffman code.

The data decoding is performed in reverse order and the image restoration after the IDP decomposition is in accordance with the relation:

$$[B(i,j)]=[\hat{B}(i,j)]+[E(i,j)]=[\hat{B}(i,j)]+\begin{bmatrix}[E_1] & [E_2]\\ [E_3] & [E_4]\end{bmatrix}, \quad (5)$$

where:

$$[E_k(i,j)]=(1/16)[H(4)][s_1^k(u,v)][H(4)] \text{ for } k=1,2,3,4.$$

The processing of colour images is performed in similar way, building three IDP pyramids – one for each component, followed by the lossless data compression, described above.

The presented method offers outstanding results when applied for compression of fingerprints, signatures, texts, and other graphic images. The method was compared with JPEG 2000 (lossless) version and with the FBI free evaluation (test) software. The comparison was performed with images of fingerprints and signatures.

3. Experimental results obtained with IDP and JPEG2000

3.1. Fingerprints.

The testing was performed with more than 100 grayscale fingerprint images. In Fig. 1 are presented four of the used test images.

The comparison shows that the results obtained with IDP-HARLC are better than these obtained with JPEG2000 (lossless version). The application of the new method for fingerprint compression in the up-to-date databases will ensure significant decreasing of the required memory. In cases where the image should be transferred from one place to another a shorter time will be required to receive the information. As a result, the receiving side will be able to use the maximum data available for the user authentication and will obtain higher recognition reliability because the fingerprint image is sent with retained quality without slowing-down the system performance.

The comparison results, presented in Fig.2 show that the compression ratio obtained with the new method for lossless compression of graphic images is higher than the results obtained with JPEG2000 (lossless version) [5,6]: the mean value of the compression ratio, obtained with the new method for the presented image class (fingerprints) was 4,8 and for JPEG2000 (LS) it was 2,2.

Figure 1. Example test fingerprint images (size 288x353 pixels, 8bpp)

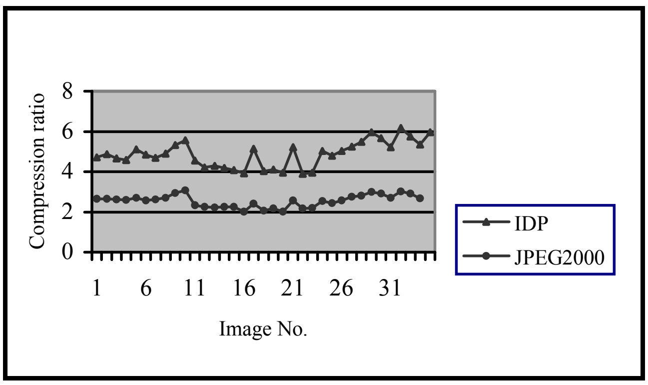

Figure 2. Results for lossless compression of fingerprint images.

Another comparison was done with the free FBI evaluation software, based on FBI standard [3,7]. The results show that the compression ratio obtained with the new method is much higher and together with this the quality of the restored images for same compression ratio is better (PSNR is higher). This comparison was performed for lossy compression only, because there was not available lossless version of the FBI compression standard on Internet.

The results, presented in Fig.3.a (lossy compression) show that for same quality the compression ratio (CR) obtained using the new method is much higher: the mean CR for the test FBI software is approximately 5, and for the new method it is higher than 8. In Fig. 3b are presented the PSNR values for same compression ratios, obtained with the two software tools: for the test FBI software the mean value for the PSNR is 28, and for the new method it is above 31.

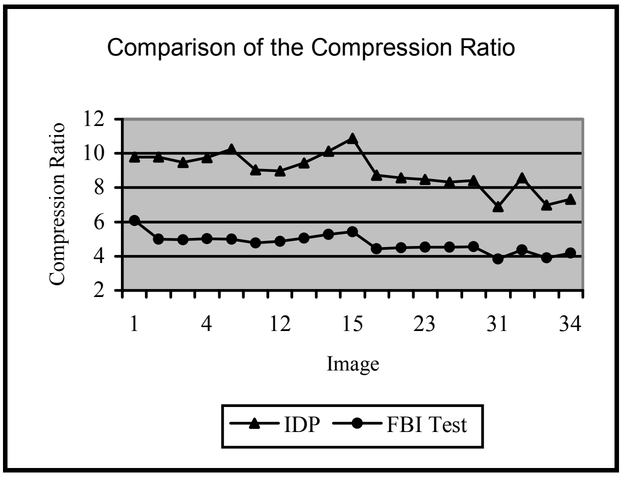

Figure 3.a. Comparison of the compression ratio for visually lossless image quality

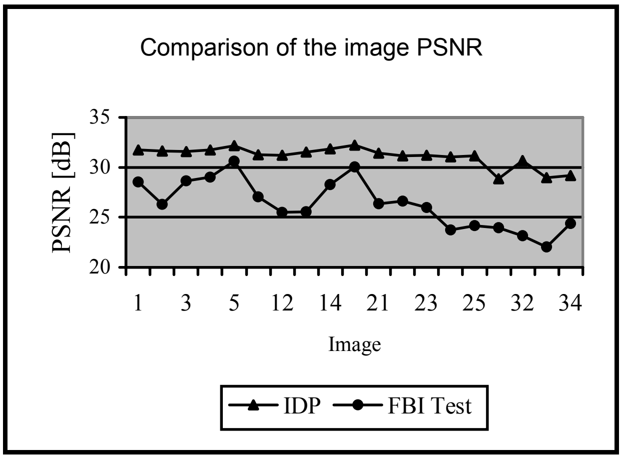

Figure 3.b. PSNR for same compression ratios
Figure 3.a,b. Comparison results for IDP and FBI standard (fingerprint images)

The experimental results show that the performance of the new method for the tested fingerprint images is better both for the CR and for the restored image quality.

3.2. Signatures

The compression of signature images is another application area for the presented method. The signatures used for the testing were scanned and the background was filtered and smoothed by removing the noises natural for scanned images. The line of the signatures was retained unchanged. Fig. 4 presents some of the used test images. The same approach is suitable for color signatures too. As a result of the high compression ratio obtained, the presented method offers another big advantage - it could be used as a basis to develop a new tool for signature authentication, presenting the signature as a sequence of TV frames, obtained in the process of signing. As a result of the high compression ratio, the size of a sequence of 40 consecutive TV frames will be equal to the size of a single signature image only. In order to retain the image quality unchanged, the compression should be performed intra-frame i.e. every TV frame will be compressed independently. For this, the video file has to be treated as a sequence of still images. The obtained compression ratio becomes higher if the TV frames are processed in groups of 8 – 12 consecutive frames, treated as one large image. The results, obtained from the processing of 1, 5, 6,.., 9 consecutive TV frames together for one of the tested signatures are presented in Table 1. The increasing of the obtained compression ratio is obvious. The presented results are for horizontal arrangement of the processed consecutive frames (i.e. they were arranged as one very wide image). Additional research was performed for vertical arrangement and arrangement in a rectangle, but the compression enhancement was not significant. The experiments showed that the processing of more than 8 consecutive TV frames together is not so efficient.

Figure 4.a

Figure 4.b

Figure 4.c

Figure 4. Test signature images

Image	L1h	L5h	L6h	L7h	L8h	L9h	Mean
HARLC	40,02	40,54	40,62	40,68	40,65	40,70	40,51
JPEG2	5,82	5.81	5.83	5.77	5.77	5.8	5,80

Table 1. Compression ratio obtained for sequence of TV frames, treated as one image

This new approach allows not only to recognize the signature, but also to analyze the movements of the hand in order to recognize whether the person is in stress or not (analyzing the tremor of the hand) and to use any other biometric and graphologists data, as pen stroke, speed, etc., which could be extracted from the video-clip information.

The experimental results obtained with the image compression software for some of the test images are presented in Table 2. The results for the JPEG2000 compression were obtained with LuraTech Algovision, and these for IDP-HARLC – with the software, implementing the described method (TKView).

Picture	Compression Ratio, IDP	Compression Ratio JPEG2000 (LS)
Sign1	36,23	6,82
Sign2	20,53	9,90
Sign3	25,24	5,22
Sign4	35,71	6,85

Table 2. Results of the lossless compression with TKView and JPEG2000.

The results obtained with TKView, confirm the high efficiency of the method for compression of fingerprints, signatures, graphics, texts, etc.

The specific advantages of the method are:

- It ensures higher compression ratio for fingerprints and signature images than JPEG2000 (lossless version).
- It has lower computational complexity than JPEG2000. This is due to the fact that JPEG2000 is based on wavelets transform, and the IDP decomposition – on WHT [5].
- It permits the still image compression to be used in a new application area - the lossless compression of a sequence of TV frames representing signatures, which to be used for dynamic biometric features extraction, necessary for some authentication procedures.

4. Digital watermarking with biometric data

Another way to protect the contents of the transferred information is to insert a digital watermark in it. As a rule, the watermark is a relatively small data sequence, which does not increase significantly the protected contents. In result of the efficient compression, the compressed biometric data (fingerprint, signature) could be used as a digital watermark, which will make the already mentioned authentication means even more reliable. Two basic approaches are possible: to insert a resistant or a fragile digital watermark in the protected information. As a rule, the resistant watermark is used to prove the contents ownership, and the fragile one – to point at an unauthorized contents change (editing). For this, the IDP decomposition is quite suitable because of its pyramid structure (for this, the IDP decomposition should consist of 3 or more levels). The *resistant watermark* is embedded in the values of a part of the transform coefficients, selected in accordance with strictly set rules: these coefficients should be low-frequency ones, and their values should be above a pre-defined threshold. The watermark is highly resistant against the basic pirates' attacks (JPEG compression, rescaling, cropping, histogram equalization, contrast enhancement, gamma correction), because the insertion is performed in the spectrum domain of the protected signal.

The *fragile watermark* insertion is based on the specific features of the IDP decomposition. For this, the watermark data is added to the compressed image information as an additional pyramid level (additional information). This watermark could visible or invisible. In case, that the watermark should be invisible, it is not visualized and its presence becomes obvious only on authorized request. The visualized watermark proves whether the image contents are authentic. The pyramid structure permits not only to insert some kind of a digital watermark in the processed data, but to use different watermark in every pyramid level as well. In result of the efficient lossless image compression, the compressed biometric data can be used as a watermark (for example, the signature image with size 300x180 pixels after compression is approximately 1,3 KBytes).

Usually the inserted watermark is invisible (inaudible), but for certain applications a visible (audible) watermark is preferred. In cases, when such watermarks are used, they make the protected contents unusable, and the watermark removal is permitted for authorized personnel only. Example of visible watermark use is presented in Figure 5 a, b. Here the size of the watermark image is equal with that of the protected one (256x256 pixels), but usually the size of the inserted watermark is much smaller and it is inserted many times in the image contents. The compressed watermark size is negligible compared with the protected data: for example, the compressed data for the image in Fig.5.a (the squares) is 86 Bytes only (CR=762) and the compressed example text image data is 44 KBytes.

The invisible watermarks are used to prove unauthorized product use (editing, cropping, coping, etc). The method for watermark insertion could be used for data hiding as well. For example, the fingerprint image could be hidden (Figure 6 a, b) in the regular data flow in the process of usual data transfer (pictures, music) or in the conversation (for mobile communications). This application is suitable (for example) for reliable authentication needed for

Proceedings of the 5th WSEAS International Conference on Signal Processing, Istanbul, Turkey, May 27-29, 2006 (pp185-190)

bank transfers or other similar operations with high responsibility.

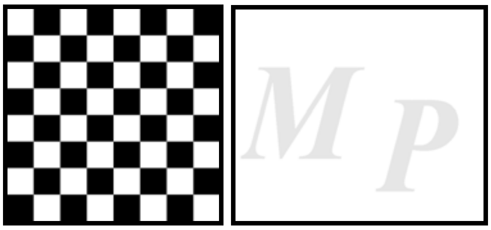

Fig. 5.a,b. Example Watermark images

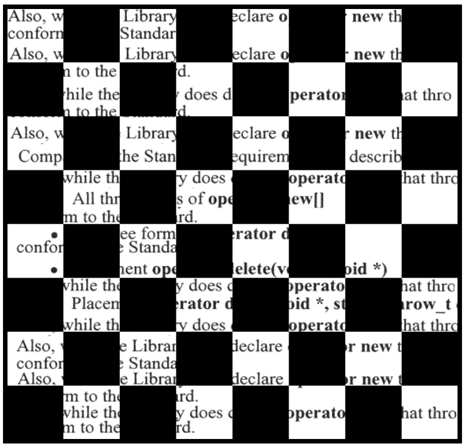

Fig. 5.b. Watermarked text image with hiding watermark: the text could not be read

Fig. 6. a. Scaled-down fingerprint image, used as watermark

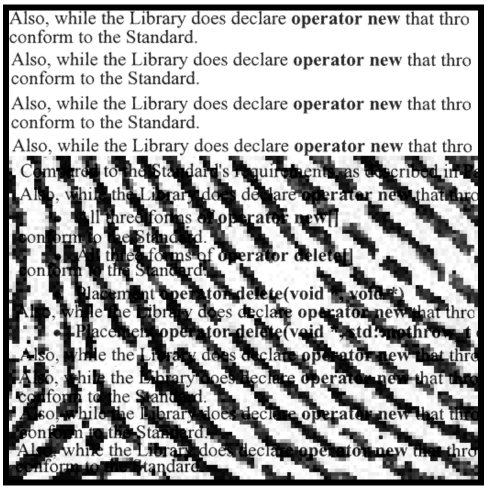

Fig. 6.b. Example for watermarked text image with visualized hidden watermark (fingerprint)

5. Conclusion

The obtained results show that the presented method is suitable for applications, which require efficient and reliable storage, archiving and transmission of some kinds of biometric information as fingerprints and signatures. The low computational complexity of the new method will permit its easy implementation for real-time tasks.

The HARLC method will be further developed in the following directions:

- Development of an algorithm, permitting to set Regions of Interest (ROI) in the processed image. In result some part of the sub-images will be processed with lossless compression, and the remaining ones – with a lossy, which will increase the method efficiency and make the compression more flexible.
- Development of an algorithm for adaptive filtering of signature images, retaining the meaning information.
- Development of intelligent software able to present the signature process as a video clip, solving the problem with the efficient intra-frame coding.

Acknowledgement: This paper was supported by the Bulgarian Ministry of Education and Science (Contract № 1304).

References

[1] J. K. Tudor. Information Security Architecture. *An Integrated Approach to Security in the Organization*. CRC Press, 2001.

[2] A. J. Menezes, P. C. Oorshot, S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1997.

[3] B.Sherlock, D.Monro. Optimized Wavelets for Fingerprint Compression, *Proc., IC on ASSP*, 1996.

[4] S. Kasaei, M. Deriche, B. Boashash. A Novel Fingerprint Image Compression Technique Using Wavelets Packets and Pyramid Lattice Vector Quantization. *IEEE Transactions on Image Processing,* Vol. 11, No. 12, Dec. 2002, pp. 1365-1378.

[5] R. Kountchev, M, Milanova, C. Ford, R. Kountcheva. Multi-layer Image Transmission with Inverse Pyramidal Decomposition. *"Computational Intelligence for Modelling and Predictions"*, S. Halgamuge, L. Wang (Eds.), Vol. 2, Chapter No 13, pp. 179–196, Springer-Verlag Berlin Heidelberg, 2005.

[6] M. Milanova, Vl. Todorov, R. Kountcheva. Lossless Data Compression for Image Decomposition with Recursive IDP Algorithm. *17-th IC on Pattern Recognition (ICPR),* Cambridge, UK, 23-26 August 2004, pp. 823-826.

[7] C. Brislawn, J. Bradley, R. Onyshczak, T. Hopper. The FBI compression standard for digitized fingerprint images, *SPIE Proceedings*, vol.2847, 1996, pp.344-355.