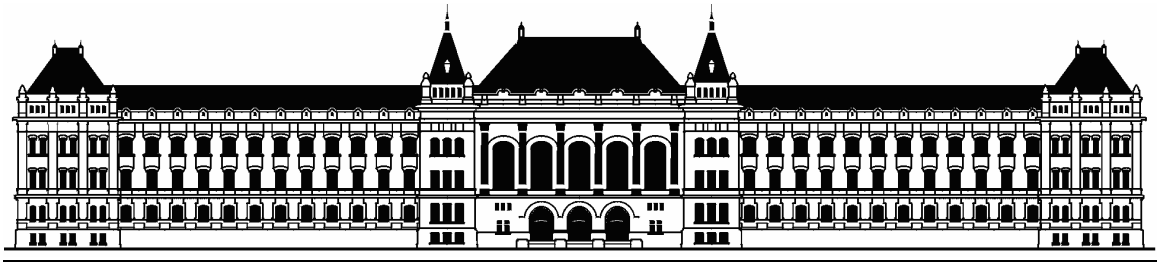

Budapest University of Technology and Economics
Department of Control Engineering and Information Technology

STEGANOGRAPHIC CONTENT AUTHENTICATION METHODS

Main results of the PhD. Thesis

Lenti József

Advisor:
Dr. Loványi István PhD.
Department of Control Engineering and Information Technology

Budapest 2005

1 Introduction

In this day and age we use mainly digital documents. The threat that digital, audio and video materials will be copied and distributed illegally is more and more realistic. When digital formats were not widely used, it was still possible to copy multimedia materials, but the quality of the copy was always worse than the original. The copying of digital documents and multimedia materials can be made without decreasing the quality and there is no need for expensive equipment in the process. The distribution of digital media is also easier than analog – today many documents are available on computer networks where the origin of those documents is not always controllable.

Digital files can be transmitted in the original and in various compressed formats. The compressed formats can provide the same quality and applicability as the original uncompressed format. The authentication control and the integrity of multimedia materials have an increasing importance in different areas. Content authentication can be used for many purposes, for example in legal processes, in medical applications, in electronic commerce – where it is needed for whatever reason that the authenticity of the received digital media is verified. The applied methods can be different according to the requirements of the applications. During the verification process in general three main parameters are checked: data integrity, data source and data authenticity.

In many cases – for example in case of medical applications – it is needed that the integrity of the image should be verified, the modification of the original image should be detected. One possible way to be able to detect modifications is when cryptographic methods are used, information is attached to the original data and the integrity verification is based on that information. Another possible and more reliable solution is when the information which is needed for integrity verification is embedded in the original data or media file.

Integrity verification in case of multimedia data is different from generic message authentication. Generic message authentication techniques are usually based on complete authentication. Multimedia data is stored and processed in various formats – like JPEG, MPEG, FLAC, generally in standard compressed formats. The original and the AVI compressed version of a copyrighted DVD movie can be considered as the same – even if there are differences in quality between them.

Generally speaking the authentication of multimedia information can be done using cryptographic and steganographic methods. In cryptography usually message authentication techniques are used for this purpose. Content authentication is different from general message authentication. Generic message authentication techniques are usually based on complete authentication. . The most common technique for message authentication is the digital signature-based authentication. In this case the modification of the original message is not allowed at all; even if a single bit is modified it will not be considered authentic. Digital signature is an encrypted version of the message digest which is extracted from the signed data, it is handled generally as a separate data file which is attached to the original data.

Watermark embedding represents a scheme where the hidden information is embedded into multimedia data, where the original multimedia data is called cover media or original media. Watermarking technology can be applied for any kind of multimedia data like videos, still images, audio files etc. In the authentication of multimedia documents the purpose is not to authenticate the document bit by bit, but to authenticate the multimedia content. In content authentication the acceptable modifications – which might be caused because of lossy compression – should be distinguished from malicious manipulations, where for example the visual meaning of the data is altered.

The classic robust watermarking solutions are designed to tolerate and survive any kind of modifications and for that reason they tolerate also content modifications. For content authentication semi-fragile watermarking techniques are used. For content authentication watermarking solutions are preferred, since in this case the authentication can be based on the embedded information.

2 Preliminaries and objectives

The watermark information which is used for integrity verification or content authentication of still images is usually dependent of the content of the image [4]. In steganography there are many proposals for integrity verification in the case of medical images [12, 14]. In the case of medical applications, not only the security of the integrity verification is required. It is also important that during the embedding process the modifications to the original media file should be minimized and the

embedding process should be reversible, the embedded data must be erasable. It means that following to the detection of the embedded information the original media content can be reconstructed [2, 3, 10, 11, 13]. The goal of my research was to build up watermark information for image integrity verification, where it is has connection to the image content and to the information which is attached to the image.

It is important to define the level of the modification when the embedded information is not damaged due to the manipulation of the cover media. In case of copyright protection, watermarks are designed to survive any kind of modifications: legitimate and illegitimate distortions, attacks of the content and other manipulations. In this case the embedded information is not related to the content; it is independent from the image properties [5,7]. When the purpose of watermarking is content authentication, it is it important to define what kinds of image manipulations are acceptable, when the modified image content can be considered identical to the original. If this distinction is not defined, the content authentication would be equivalent to message authentication [9,18]. So far, as in content authentication, images could be handled identical only when there is absolutely no difference between them; it would mean that if even a single image is modified the image content wouldn't be authentic. In some cases it might be a requirement, but in most applications the modification of the image content is acceptable to a certain extent [16]. Today in steganography, content authentication is an intensively researched area [1, 15, 17].

My goal was to develop an algorithm which can be used for content authentication where the acceptable modification is the lossy JPEG compression. My research objective was to develop a solution where content authentication is possible on lossy JPEG compressed images and it is possible to find the image blocks where the image content was modified compared to the original image.

Watermark embedding solutions fulfill different requirements according to the specific application area. In watermark embedding robust, fragile and semi-fragile techniques are distinguished. Semi-fragile embedding techniques are robust against selected manipulations (the embedded information will not be damaged after these manipulations) but they are not robust against other modifications. In general semi-fragile watermarks are robust against specified modifications but fragile in any other cases. In this case, not ownership information is embedded, since the purpose of the

embedding is authentication and integrity verification, where it is possible to define acceptable modifications.

My goal was to create a semi-fragile watermark embedding algorithm. For lossy JPEG compression – with a given quality factor – it can guarantee that the embedded watermark will be kept intact, and the embedded information is erasable.

3 Novel scientific results

1. thesis: I developed a new algorithm for integrity verification and ownership identification, where the embedded information has a fixed length [L6]

The main novelty of the algorithm is that the embedded information is related not only to image content but also to attached information which are closely related to the image. In the case of former solutions based on the information which is used for integrity verification, the ownership of the image was not controllable [1, 2, 10], based on the proposed algorithm both goals can be achieved. The watermark information – which is the output of the proposed method – can be used in robust, fragile and semi-fragile embedding processes. The generated watermark information is based on image properties and has the following properties:

- It can be used as a unique identifier or the image in image databases. Since the watermark information is embedded in the image based on the watermarked image it is possible to determine those database records which are related to the image. In case of medical databases where the images are not stored in the database and handled separately it is a significant property according to the current regulations and recommendations in the field of medical informatics systems.
- Based on that information the image integrity verification is possible.
- It provides a connection between the image and other image related information.
- It is short, fixed length information; where its length is independent from the image size it is dependent on the parameters of the generation process. The size of the embedded information should be minimized in watermarking in order to minimize the distortion caused by the embedding process.

- The ownership of the image can be proven based on the embedded information; the rightful owner can prove that he or she is the copyright owner of the given watermarked image.
- The generated watermark is resistant to a watermark-copy attack.

2. thesis: I developed a new algorithm which generates a feature vector which can be used for image content and integrity verification. [L9]

I developed an algorithm where the integrity verification can be done also for the compressed version of the image. There are other algorithms where the integrity verification can be made for the compressed images [13, 15, 18], the proposed algorithm can detect those image blocks which are modified comparing to the original image. It means that it makes it possible to distinguish between malicious image content modification and lossy compression and therefore the integrity if the image can be verified in the case of a lossy compressed image. The algorithm has two processes: feature vector generation and feature vector-based integrity verification.
The acceptable modification is the lossy JPEG compression. It means that based on the feature code which is calculated from the original image the integrity of the JPEG compressed image can be also verified.
The novelty of the algorithm is that not only the integrity of the complete image is verified but also the integrity of the content details, which means that the modified image regions can be determined. In the verification process those image blocks are selected where the content is modified compared to the original image.

3. thesis: I developed a new erasable, semi-fragile watermark embedding algorithm, which is semi-fragile for lossy JPEG compression with a selectable quality factor. [L7, L8]

I developed a steganographic watermark embedding algorithm for digital images which is erasable, semi-fragile. If the embedded information is used for content authentication or for integrity verification where the acceptable modification is the lossy JPEG compression, it is required to use such an embedding algorithm which is semi-fragile for the accepted modification type.

The algorithm is semi-fragile for lossy JPEG compression which means that if the image is compressed with a given quality factor, it is guaranteed that the embedded information will be kept intact, and the embedded information is erasable.

The proposed algorithm can be used to embed such watermark information that is used for content authentication and where the semi-fragile property for JPEG compression is a requirement. The novelty of the proposed solution is that the JPEG quality factor is a parameter of the embedding process; it means that the embedded information will be intact during JPEG compression if the applied quality factor during the compression process is not lower than that. Therefore the image modification caused by the embedding process can be minimized according to the required resistance level. If the quality factor in the compression process is higher than the quality parameter in the embedding process, the watermark can be detected and will not be modified during the compression.

The embedded information is erasable, after watermark detection the embedded information can be removed and the original un-watermarked image can be reconstructed. The proposed algorithm modifies the cover image to a minimal extent which is required according to the given quality factor, the modification occurred during the embedding is less than in other general embedding methods [1,6,9].

4 Application of the novel scientific results

IKTA 144/2000 was a common project of the Department of Control Engineering and Information Technology, Bull Hungary Ltd. and Vasútegészségügyi Ltd. The goal of this project was to develop a portable patient record structure which contained also medical images which could be used in the communication between medical information systems. The first thesis is related to this project.

In the Balaton research project there is a cooperation between the ENST Bretagne and the Budapest University of Technology and Economics. In the cooperation the main research focus was on telediagnosis on medical imaging and on image compression. Since among medical systems there are educational applications not only content but also owner authentication is required for the applied images. The second and the third thesis is related to this work and also to IKTA4 138/2001 project.

5 References

[1] N. F. Johnson, Z. Duric, and S. Jajodia. Information Hiding: Steganograph and Watermarking - Attacks and Countermeasures. Kluwer Academic Press, Dordrecht, the Netherlands, 2001.

[2] X. Kong and R. Feng. Watermarking medical signals for telemedicine. IEEE Trans on. information Technology in Biomedicine, 5(3):195–201, Sept. 2001.

[3] H. Tachibana, H. Harauchi, T. Ikeda, Y. Iwata, A. Takemura, and T. Umeda. Practical use of new watermarking and vpn techniques for medical image communication and archive. RSNA 2002 Archive Site: http://archive.rsna.org/index.cfm

[4] A.Wakatani. Digital watermarking for ROI medical images by using compressed signature image. In Annual Hawaii Int. Conf. on System Sciences, pages 2043– 2048, Hawaii, USA, Jan. 2002.

[5] Ingemar Cox, Matthew Miller, Jeffrey Bloom, Digital watermarking. Morgan Kaufmann Publishers, 2001

[6] J. Friedrich, M. Goljan and M. Du, "Invertible Authentication", "Proceedings of SPIE, Security and Watermarking of Multimedia Contents", 2001

[7] Jozsef Lenti, Istvan Lovanyi. "Image integrity verification in medical information systems", "Proceeding of MIE2003, The New Navigators: from Professionals to Patients, Medical Image Information Systems", pp 286-291

[8] Bruce Schneier. Applied cryptography Second Edition. John Whiley and Sons Inc. 1996

[9] M. M. Yeung and F.Mintzer, An invisible watermarking technique for image verification, in Proc. IEEE International Conference on Image Processing, vol. 2, pp. 680–683, Santa Barbara, California, USA, October 1997.

[10]G. Coatrieux, B. Sankur, H. Maitre, Strict Integrity Control of Biomedical Images, SPIE Conf. 4314: Security and Watermarking of Multimedia Contents III, 22-25 Jan. 2001, San Jose USA

[11]N.J.G. Brown, K.E. Britton, D.L. Plummer: Standardisation in medical image management International Journal of Medical Informatics 48, 1998, pp 227-238

[12]G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, R. Collorec. Relevance of Watermarking in Medical Imaging. 2000 IEEE EMBS Conf. On Information Technology Applications in Biomedicine, Nov. 2000, Arlington, USA. , p 250-255

[13]F. Mintzer, G.W. Braudaway, and M. M. Yeung. Effective and ineffective digital watermarks. IEEE ICIP, volume III, Santa-Barbara, Cal, October 1997, pages 9—12

[14]Lesley R. Matheson, Stephen G. Mitchell, Talal G. Shamoon, Robert E. Tarjan, Francis Zane, Robustness and security of digital watermarks, Financial Cryptography FC-98, volume 1465 of Lecture Notes in Computes Science, Springer, 1998, pages 227-240

[15]S. Bhattacharjee and M. Kutter, Compression Tolerant Image Authentication, IEEE International Conf. on Image Processing, Chicago, October 1998.

[16]M. L. Miller, I. J. Cox and J. A. Bloom, Informed Embedding Exploiting Image and Detector Information during Watermark Insertion, IEEE Intl. Conf. on Image Processing, Vol. 3, pp.1-4, September 2000.

[17]T. Uehara and R. Safavi-Naini, On (In) security of 'A Robust Image Authentication Method', Proc. IEEE Pacific Rim Conf. on Multimedia, pp. 1025-1032, Dec. 2002.

[18]M. Wu and B. Liu, "Watermarking for Image Authentication," IEEE Proc. of ICIP, Chicago, Oct 1998.

6 Publications

[L1] Lenti József, Steganographic Methods, Periodika Polytechnika, Electrical Engineering, Hungary, 2000 44/3-4, 249-258 oldal

[L2] Dr. Loványi István, Lenti József, Y2K – ezredfordulón túlmutató kihatások, Egészségügyi Menedzsment, 1999 október 1, 52-54 old.

[L3] Lenti József, Biztonság és hatékonyság, Computerworld - Számítástechnika, XVII évfolyam 39. szám,

2002 szeptember 24, 22. old

[L4] Lenti József, Staganographic methods, MicroCAD2000, Miskolc International Science Conference, 54-61 oldal, 2000 február 23-24

[L5] Lenti József, Loványi István, Nagy Ákos, Blind Signature Based Steganographic Protocol, I. Magyar Számítógépes Grafika és Geometria Konferencia, Budapest 2002 május 28-29, 133-139 oldal

[L6] Jozsef Lenti, István Loványi, Image Integrity Verification in Medical Information Systems, MIE2003, Proceedings of Medical Informatics Europe 2003, 4-7 May , 2003 Saint-Malo, France, pp. 286-291

[L7] Lenti József, Loványi István, Dezső Zoltán, Efficient Watermark Embedding in Medical Images, IEEE Conference – 2004 International Conference on Intelligent Engineering Systems, 2004 september 19-21, Cluj-Napoca, Romania, pp. 232-235

[L8] József Lenti, István Loványi, Erasable, Semi-fragile Watermark Embedding Process for Images, IEEE 9th International Conference on Intelligent Engineering Systems, 16-19 September, 2005

[L9] József Lenti, István Loványi, Feature Vector Generation for Image Integrity Verification, IEEE 9th International Conference on Intelligent Engineering Systems, 16-19 September, 2005

[L10] Z. Dezső, G. Bálint, A. Hunka, J. Lenti, I. Lovanyi Motion Capture vs. traditional medical examinations SETIT 2005 27-31 Mars 2005 Sousse – Tunisie, Actes de SETIT 2005 p. 106.