MULTIKEYS FOR THE SCALABLE MULTIMEDIA SERVICE

Robert Kutka, Andreas Hutter,Klaus Illgner, Jürgen Pandel, and Marcel Wagner

Corporate Technology, Information and Communications
Siemens AG
Otto-Hahn-Ring 6, 81739 Munich
Robert.Kutka@Siemens.com

ABSTRACT

We present a concept which enables services to be offered on different quality levels and to be billed accordingly. The technical implementation combines scalable coding with cryptographic techniques and unequal error protection. Different keys are used for the various layers (multikeys). This makes it possible to selectively decode different quality levels.
In addition to the facility for tiered billing, our method increases error protection during transmission, which is a major advantage for mobile devices.

1. SCALABLE CODING

Scalable coding methods for pictures and voice were developed in order to extract services of various qualities and display them on terminals having different capabilities [1]-[4]. They are used in the MPEG-4 standard (scalability profiles) and the JPEG 2000 standard [5], [6]. They consist of separate data streams (layers) of differing quality. We take the following types of scalability into account:
Spatial resolution scaling: this corresponds to different picture sizes of the encoded image layers.
Temporal resolution scaling: different picture frequencies.
Amplitude or SNR resolution scaling (SNR = Signal to Noise Ratio): different quantization parameters in the layers.
Content scaling for texts: the lowest layer contains only headlines, while the higher ones contain the full text and any additional images [7].
Update scaling: updates of share prices, sports reports or other important events.
Any combination of scaling techniques.

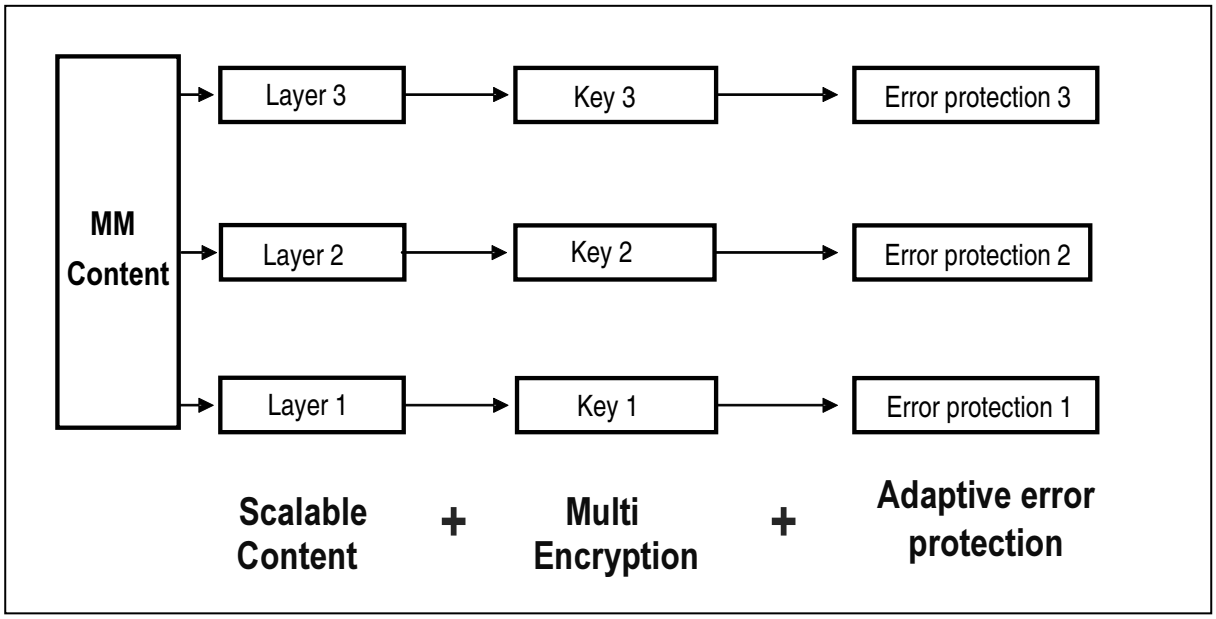

Fig. 1: Principle of scalable coding combined with multi-encryption

2. COMBINATION OF SCALABLE CODING, ENCRYPTION AND ERROR PROTECTION

We combine scalable coding with our new proposed multikey technique and unequal error protection as set out below:

Fig. 1 shows an example with 3 layers. The individual layers are compressed separately. The lower the quality level, the lower the bandwidth during transmission. We likewise apply encryption individually and separately to the layers. This makes selective decoding possible.

Owing to interference at the air interface, error protection is necessary for mobile devices. We employ unequal error protection, with the lowest layers being given the greatest protection [8], [9]. It is vital to perform encryption between compression and error protection so that the key is then also protected.

The service provider can provide customers with decoding keys using a tiered scale of charges. The basic layer can be offered unencrypted and free of charge as a demo preview.

2.1. Encoding unit

A multilayer coder conforming to the MPEG-4 standard is used for encoding. As already mentioned, the various layers can be split into different MPEG-4 elementary streams (ES). The MPEG-4 standard offers the additional option of using an IPMP interface (IPMP = Intellectual Property Management and Protection), which permits independent encryption of the ES. An identification code for the encryption mechanism used can be transported in the configuration information for the MPEG-4 presentation for every ES, enabling unique assignment and decryption of the specific ES for which a key is provided. Fig. 2 illustrates this principle:

For the encoded data transported in the individual elementary streams, the procedure is then as follows: the bit stream generated by the coder is subdivided into segments of different importance. Only the important data is forwarded to the encryption unit! The data after the picture start codes and the block headers is suitable for this.

In addition, the data stream is subdivided into encryption units, at which it is possible to recommence decoding if an error occurs.

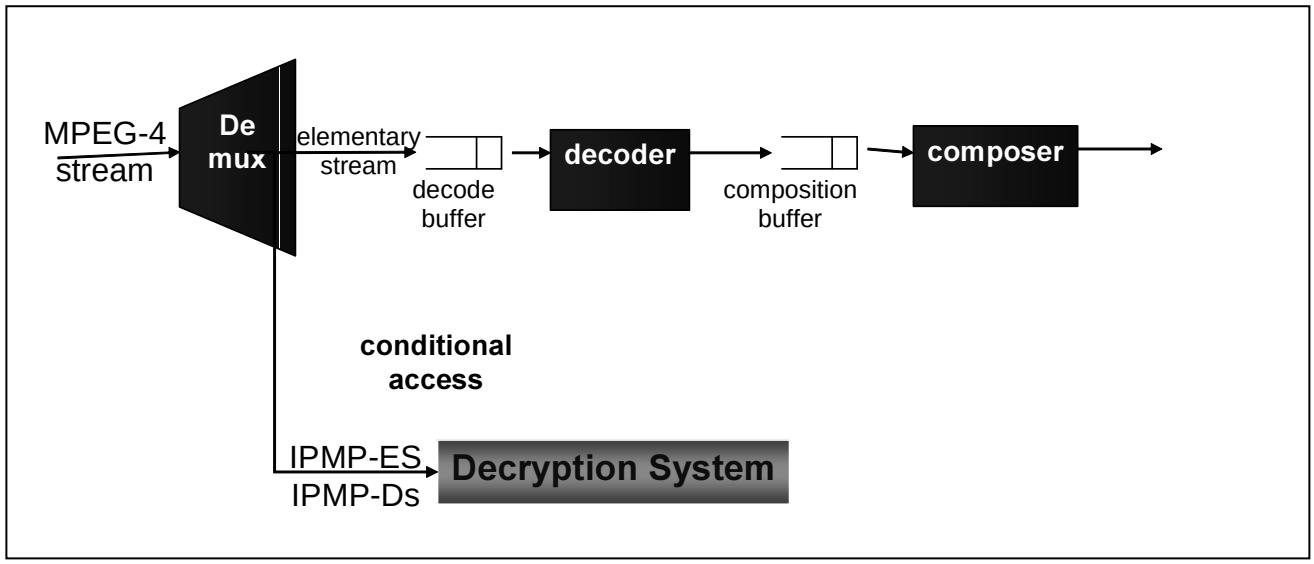

Fig. 2: Splitting of the MPEG-4 stream into elementary stream and IPMP (Intellectual Property Management and Protection)

STARTCODE	PICHEADER	SLICEHEADER	MACROBLOCKHEADER	CONTENT

Fig. 3: Format of MPEG-4 stream

2.2. Encryption unit

The data is encrypted using a symmetrical encryption algorithm (advanced encryption system) [10], [11]. The session keys used for this are generated in the transmitter's encryption unit (random number generator).
Given the expected bit rates of 64-768 kbit/s, in some cases the encryption of multimedia streams is too complex. However, this complexity can be significantly reduced if only selected parts of the bit stream are encrypted as described below. In a typical video stream (e.g. H.263), the information is organized so that first the basic information, such as the start code marking the start of a picture, the picture header containing information about the picture size, etc., is coded, then finally the information describing the actual content of the picture (Fig. 3):
If the headers are not known, it is virtually impossible to reconstruct the pictures. This can be exploited for the encryption process. Since the headers together usually require less than 60 bits, a video stream can already be efficiently encrypted simply by encrypting only the 128 bits following the start code. The start code itself is not encrypted so that it is possible to identify a starting point for recommencing decoding in the event of errors. A further advantage of unencrypted start codes is that it is then unnecessary to specifically tell the decryption unit which positions in the bit stream are encrypted and which are not, since a 128-bit encryption is always performed following the start code.
Assuming that the video stream does not use slices, i.e. one picture is coded as one unit in each case, then given a picture frequency of 10 pictures/s it is only necessary to encrypt 1.2 kbit/s. Even if a picture were divided into up to ten slices, this would result in a throughput of 12 kbit/s through the encryption unit irrespective of the bit rate of the video stream. The same also applies of course to the decryption of the data at the receiving end.

2.3. Error protection unit

The multikeys method is compatible with the technique of unequal error protection (UEP). Since encrypted data would lead to the loss of the entire encrypted packet in the event of an error, we use a correspondingly higher level of error protection for these packets (Figs. 4 and 5).

Fig. 4: Effect of error protection with 9% packet loss: left without error protection, right with unequal error protection

Fig. 5: Unequal error protection applied to the picture start code (PSC) and the encrypted data

3. CONCLUSION

Our studies show that the proposed multikeys method is technically feasible. The problem of costly encryption was solved by encrypting only parts of the data stream. This considerably reduces the complexity of the method, and consequently makes its use in small mobile devices feasible. The proneness of mobile terminals to interference was reduced through special error protection for the encrypted data segments, without bloating the data stream as a consequence of redundancy.

This technique opens up application scenarios that will make m-commerce services more attractive and simpler to use. The lowest quality level, such as text and a few small-format pictures for example, should be available free of charge on every terminal. If users are in possession of a subscription key, they can display high-quality images and films on a sufficiently large display. In addition to better quality, ad-free pages could also be provided. This scenario can be extended to cover many applications: download services, street maps, movies, network games, live concert performances, privately offered MM content.

Through the scaled representation and tiered billing of multimedia data, we anticipate an increase in high-quality services and consequently a boost to the terminal market.

4. REFERENCES

[1] W. Li, "Overview of Fine Granularity Scalability in MPEG-4 Video Standard", *IEEE Trans. on Circuits and Systems for Video Technology*, Vol. 11, No. 3, pp. 301-17, March 2001.

[2] P. Amon and J. Pandel, "Evaluation of Adaptive and Reliable Video Transmission Technologies", *Int. Packetvideo Workshop 2003*, Saint-Malo, France, April 2003.

[3] F. Wu, S. Li, and Y. Zhang, "DCT-Prediction Based Progressive Fine Granular Scalable Coding", *Proc. Int. Conf on Image Processing*, pp. 556-559, Sep 2000.

[4] J.-R. Ohm, "Motion-compensated Wavelet Lifting Filters with Flexible Adaptation", *2002 Tyrrhenian Int. Workshop on Digital Communications* (IWDC 2002), Capri, Italy, Sep 2002.

[5] *ISO/IEC* JTC1/SC29/WG11 N5878, Trondheim, Norway, July 2003.

[6] *ISO/IEC* JTC1/SC29/WG11 N5877, Trondheim, Norway, July 2003.

[7] *Interactive Media*: Examples of interactive content: http://www.interactivemedia.de/home_f/index.html.

[8] G. Liebl, M. Wagner, J. Pandel, and W. Weng, "An RTP Payload Format for Erasure-Resilient Transmission of Progressive Multimedia Streams", *draft-ietf-avt-uxp-06.txt*, October 2003.

[9] A. Li, "An RTP Payload Format for Generic FEC", *draft-ietf-avt-ulp-08.txt*, October 26, 2003.

[10] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, ISBN: 0-8493-8523-7.

[11] D. Boneh and M. Franklin, "An Efficient Public Key Traitor Tracing Scheme", *CRYPTO 1999*.