A Proposal for Combination of Compression and Encryption

Lutz Vorwerk*, Thomas Engel, Christoph Meinel

Institute of Telematics, Trier, D-54292

ABSTRACT

This paper describes how to integrate encryption in algorithm which uses wavelets to compress data. Wavelets are more useful in image compression than other methods. This is because the definition about which data should be lost is more flexible. This adaptation of wavelets specific features images leads to acceptable results. The use from computer in image transfer will increase further and will therefor become necessary to transfer image data quickly. Additional protection of the image against unauthorized access will become necessary. Image compression increases the amount of time needed for transferring images. Regarding the area of telemedicine, there is demand for the protection of images. The reason for this demand is the need to prevent the relationship between patient data and image from being determined. The reference approach intends to describe combination image compression by using wavelets and to integrate encryption into the wavelet-transform and compression procedure.

Keywords: wavelets, compression, asymmetric encryption, multimedia, security, transformation, graphic file formats, audio file formats

1. INTRODUCTION

In the age of computer science, the evolution of microprocessors, the pricing of memory chips and other hardware components are reasons for the fact that the development and the use of multimedia applications is becoming a state of the art. 'Multimedia' signifies the transfer of large amounts of data represented as images, audio, animations or of a combination of the three from one place to another via internet or intranet. Algorithms were developed to reduce the amount of data that is to be transferred and processed.

In imaging, JPEG (Joint Photographic Experts Group), GIF (Graphics Interchange Format) and TIFF (Tag Image File Format) are popular. For the compression and representation of audio data, the AU (audio)-standard has been established. Algorithms for both audio and image data are are MPEG-1 (Moving Picture Experts Group) and more recent versions are used to compress movies that may contain audio-data, but the single algorithms are not useful for stand-alone images.

The need for security in transferring data from one point to another requires additional algorithms to the compression algorithms which encrypt the data. In medicine, this problem of choosing performance in encrypting images which have to be transferred produces conflict. The problem arises through the constraints of the physicians, i.e. radiologists which do not allow them to separate images from patient data. The problem to compress and encrypt sequences of images together with patient data is time consuming tasks. Within other disciplines it is desired to encrypt images, sequences of images and audio waves or movies to protect information that is integrated in such kind of data. The need to protect image and audio data against unauthorized access requires fast and smart methods to compress and encrypt the data.

The overall purpose of this proposal is to show a new algorithm that makes use of wavelet-transform in compressing image data. Wavelet-transform emerged during the last few years as a enabling technology for image compression. Its very useful in image and audio compression of filter the frequency spectrum of image and audio signals in such a way that only those frequencies remain which can be perceived by an observer or listener. Other disciplines of wavelet-transforms like the solution of linear equations, pattern cognition are not covered in this proposal.

Additionally a wavelet basis may be constructed in such a way that the compressed data (audio or image) can only be interpreted if the basis is known. The aim of this paper is to examine the construction of appropriate wavelet basis.

Some conditions have to be considered during the process of image transformation which leads originally to compressed image. The image data is decomposed in wavelet coefficients and detail coefficients needed to construct the image data.

*vorwerk@ti.fhg.de

The process from raw data to the desired compressed and encrypted format using wavelets occurs in two steps. The first step during wavelet-transform is the construction of a basis. There are some standard bases e.g. Haar, Daubechies, Mexican Hat or Coiflets. The basis considered in this case must have additional characteristics. It is possible to specify a variable that has a value range broad enough to make it impossible to determine the values of variable within feasible timing constraints.

The value of variable represents the public key of the new characteristic 'encryption' which is integrated in wavelet-transform. The combination of transformation and encryption is such a compression scheme reduces the processing time compared to the application of transformation and compression in first step and making use of additional encryption algorithm in second step. For the reconstruction of the compressed and encrypted data private key is needed. The algorithm for decomposition and reconstruction of the raw data has to correspond to the wavelet-transform, compression and the asymmetric encryption (public and private key). A solution for this problem is presented in this paper defining an appropriate process.

The algorithm to be developed has to conform to the condition for verified and adapted as the private key is included in the computation of the wavelet-transform and compression. To guarantee the decomposition the condition of orthogonality is important for reconstruction. The process of encoding is different from the process of decoding (reconstructing) the raw data because of asymmetric encryption. Considering the encryption algorithm and making use of symmetric scheme, any private key is associated with an appropriate public key. The private key is not computable from the public key. This condition is combined with the conditions of wavelet-transform.

Finally, to conclude the subject, it remains to said that the usage of wavelets leads to good compression ratio for image data. Compared to other processes like JPEG [8] compressing, it generated good quality of lossy compressed images and reduces the amount of data even in lossless compression. The integration of asymmetric encryption into the process of wavelet-transform and compression saves the encryption of the compression.

2 WAVELETS

The focus of this paper lies on the compression of two-dimensional images. There are many approaches to compress images which uses the Fourier-transform or the discrete cosinus transform, like JPEG [7]. Wavelets are more suitable for image compression than these approaches, because wavelets can be adapted to particular features of images and therefore be able to good image quality despite the loss of data. A wavelet is a function which passes above and below the x-axis. The area enclosed by this function is zero. The function can be scaled on the x-axis and shall be orthogonal [6].

To explain the term orthonormal it is necessary to know what a function is orthonormal is orthogonal and normalized. If a function is orthogonal it fulfills the following condition:

Two functions f and g are called orthogonal if the inner product of f and g with weight w is zero. The inner product is defined as follows:

$$< f \mid g >= 0 \qquad (1)$$

with

$$< f \mid g >:= \int_1^0 f(x)g(x)w(x)dx\,. \qquad (2)$$

A function is normalized if the inner product of this function with itself is one:

$$< f \mid f >= 1 \qquad (3)$$

Using the wavelet-transform it is possible to transf orm digital image data into frequencies. According to the used wavelet, particular frequencies below a specified barrier are left out. Afterwards the rest of the image data will be compr essed. The featured adaptation leads to high compression. The compression is easy an image by constructing wavelets which enables this if the wavelet and the barrier is chosen appropriatel y. As example, we chose the perception of frequencie s by human eyes. The human eye is only able to percep t frequencies in a small area of possible frequencies. The frequen cy of infra red light lies outside this area. This kind of light can be perceived by human eyes. In the used digital image s, these frequencies can be found in invisible data as needed for transformation procedures that make this data visible. For digital image s integrated in internet web pages, the frequenc ies can be reduced to the one which can be perceived by huma n eyes. For digital two-dimensional radiological image s the approach is the same.

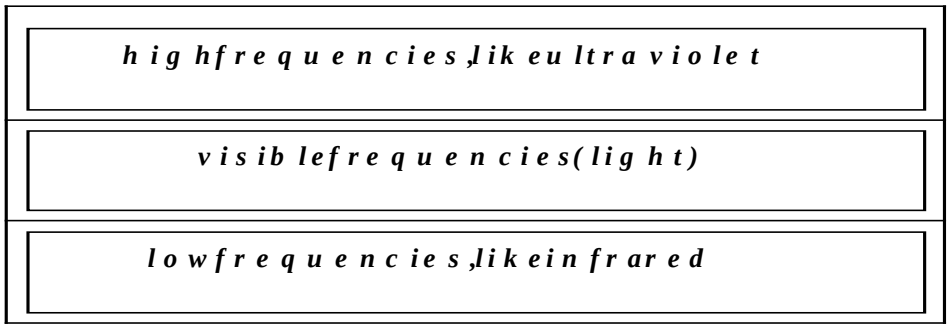

Figure 1: Frequencies perceived by human eyes

There are many kinds of wavelets developed to emphasize spe cial features of the objects which have to be examine d. Some wavelets are widely used. Two examples are depicted in figure 2. The first example is the Haar-wavelet, which is the simplest wavelet and is used in many tutorials to intro duce the usage and construction of wavelets [9,10,11,12]. It is non-continuos.

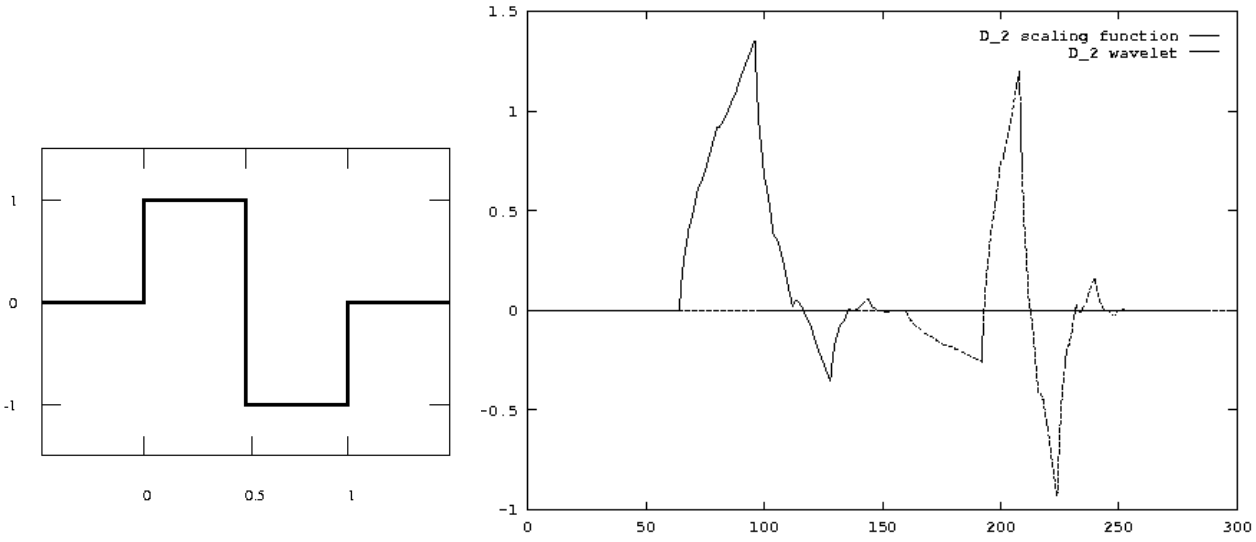

Figure 2: a) The Haar-wavelet b) The Daubechie-wavelet

Wavelet-transforms have an infinite set of wavelet bases. These are functions. Wavelets are assigned to families. The Daubechies family is an example. There are subclasses within each family, distinguished by the number of coefficients and the level of iteration. To find an appropriate wavelet family for digital image processing, another wavelet has to be defined. This mother wavelet, also called analyzing wavelet, can be adapted to our needs.

Mother wavelets for:

- discrete wavelet transform (DWT)

$$\Phi_{(a,b)}(x) = 2^{-\frac{b}{2}}\Phi(2^{-b}x - a) \quad (4)$$

- continuous wavelet transform (CWT)

$$\Phi_{a,b}(x) = \Phi\left(\frac{x-b}{a}\right) \quad (5)$$

$$\Phi_{a,b}(x) = \left(\frac{1}{\sqrt{a}}\right)\Phi\left(\frac{x-b}{a}\right) \quad (6)$$

This mother wavelet can be dilated and scaled by the two variables a and b. This way the appropriate wavelet family will be found by estimating the scaling factor a and the location of the wavelet. Re-scaling is done by powers of two. Transforming is done by integers. The mother wavelet is indicator for the mother wavelet used to construct the wavelet basis. This leads to the second specification which we want to discuss in this paper: the integration of encryption in wavelet compression. But first we have to discuss the wavelet transform.

3 WAVELET TRANSFORM

There are two kinds of wavelet transform: the continuous wavelet transform and the discrete wavelet transform. The continuous wavelet transform contains a lot of redundancy. It would be nice to have a small set of data to describe the wavelet. The computation of the wavelet transform has a linear complexity. Therefore discretisation is necessary. The discrete wavelet transform computes on discrete data like that contained in digital images. Now it is possible to reduce the wavelet function to a basis that describes the whole function.

To perform a discrete wavelet transform a filter has to be defined which describes a wavelet. To obtain this filter a scaling function has to be chosen. This scaling function with two conditions (7) forms an orthonormal basis of the space V and uses the following dilatation equation (8) as a starting point.

$$\{\phi(x-k), k \in \mathbb{Z}\} \quad (7)$$

$$\phi(t) = \sum_k c_k \phi(2t-k) \quad (8)$$

$$\int \phi(t)\,dt = 1 \quad (9)$$

This equation possesses the feature which is shown in (9). It therefore permits to define construction methods for scaling functions. Three of them should be mentioned here:

- Iterate the recursive relation starting with the box function and some values. This will give the spline family (box, hat, quadratic, cubic, etc.). One of Daubechies' wavelets, noted D_4, is obtained by this method which obtain a wavelet which is the derivative of a cubic spline filter function.
- Perform the Fourier-transform on the dilation equation.
- Work directly with the recursion. If $\phi(k)$ is known at integers, applying the recursion give the values at points of values $(i/2^j)$.

The coefficients a_k are chosen from the interval (1,0).

$$\langle \phi(t), \phi(2t-k) \rangle \qquad (10)$$

Now we are able to develop filter data from wavelets defined by the dilation equation. The next section describes how we can do wavelet transform and the inverse wavelet transform.

4 WAVELET COEFFICIENTS

To perform a discrete wavelet transform it has to be guaranteed that the transformed data can be reconstructed. Therefore some conditions for the high pass filter g_k and the low pass filter h_k will be given. The method using these filters is called Quadrature Mirror Filters (QMFs) and make it possible to perform the wavelet transform in linear time. The bandwidth of signal is split in half.

Filter conditions [3]:

$$\sum_k h_k = \sqrt{2} \qquad (11)$$

$$g_j = (-1)^j h_{1-j} \qquad (12)$$

$$\sum_k (-1)^k g_k = 0 \qquad (13)$$

$$\sum_k h_k h_{k+2m} = \delta_{0m} \text{ for all } m \qquad (14)$$

Data given to the high pass filter transformed to wavelet coefficients. The same data given to the low pass filter will be transformed to scaling coefficients. The data for the filter can be computed by using equations two of the filter conditions.

To perform the inverse wavelet transform additional features are necessary. They are given by the following equations. The inverse operations will be written as g^{-1} and h^{-1} and will be related as follows:

$$g \qquad g_n = h^{-1}_{-n} \qquad (15)$$

$$h \qquad h_n = g^{-1}_{-n} \qquad (16)$$

5 THE WAVELET COMPRESSION

After coefficients are computed, we perform discrete wavelet transform on image data and reconstruct the image data via inverse wavelet transform. Figure 2 gives an example how to do the transform and figure 4 illustrates the inverse wavelet transform. The figures illustrate the hierarchical nature of the multi-

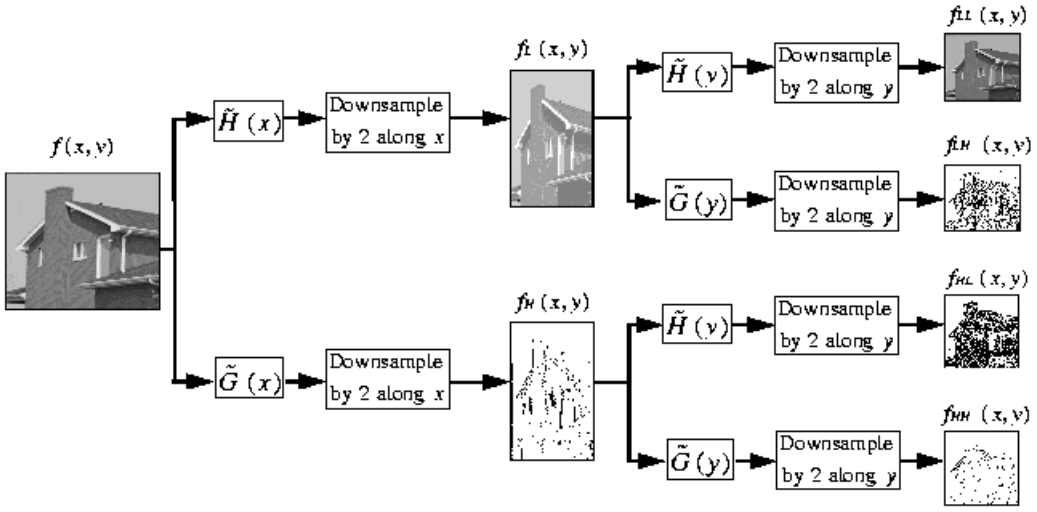

Figure 2. Forward wavelet transform

resolution method. It reminds one of the pyramidal approach often used in image processing. Here the filter functions in figure 3 represented as matrix $\tilde{G}$ and in figure 3 represented as matrix $\tilde{H}$ are used to decompose the image represented as two-dimensional function f(x,y). First the wavelet transform is applied the x-values and afterwards to the y-values. The inverse filters H^{-1} in figure 4 represented as matrix H and in figure 4 represented as matrix G.

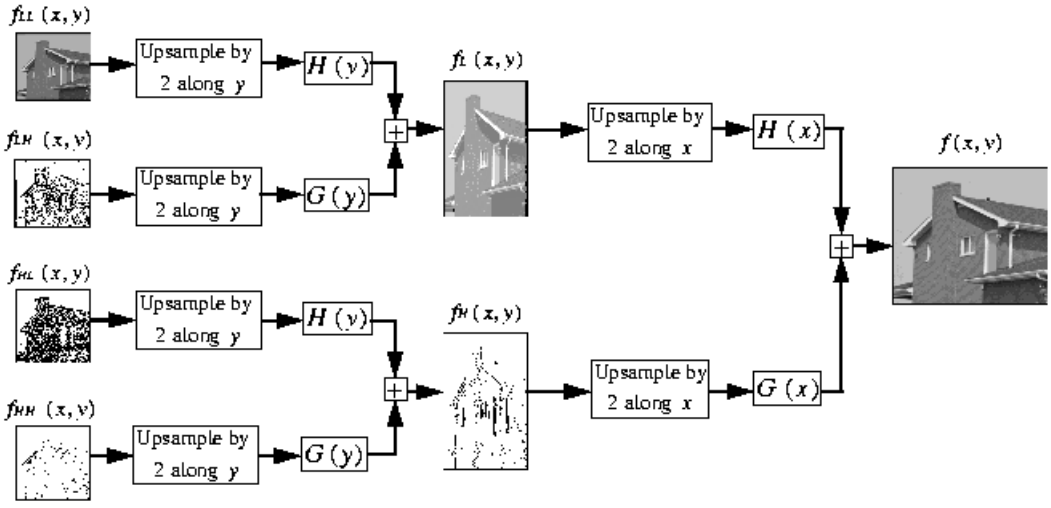

Figure 4. Inverse wavelet transform

The conventional way to proceed is shown in figure 5. After the wavelet transform process called quantization prepare the wavelet coefficients for compression. The quantization process transforms the wavelet coefficients into values which are easier to handle for defining an error tolerance to perform lossy compression with acceptable image quality after decompression. For quantization, two approaches were proposed [4]. The first approach is to divide the real axis in a number of non-overlapping intervals and relate the coefficients to the intervals. The relationships are stored in a table. This approach is called scaling quantization. The other approach is the vector quantization and replaces a group of coefficient s with one symbol. A good pre-condition is required that the wavele t is orthogonal and the wavelet basis is orthonormal. These requirements allow a quick find solution for the compres sion problem.

After quantizing, the transformed data is ready for compressio n. For compression there are two approaches [4]. The first is called fixed length coding. It replaces each symbol obtaine d from quantize with the same number of

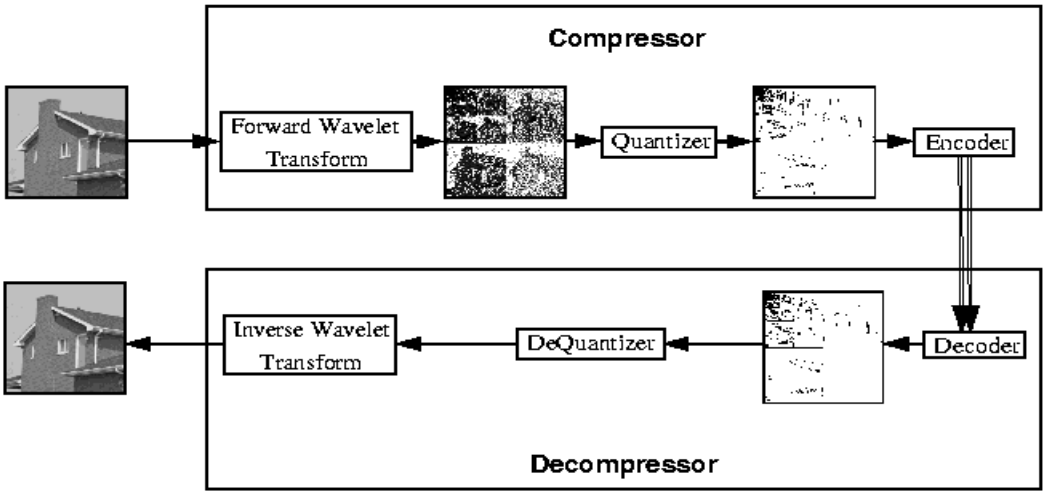

Figure 5: Wavelet compression and decompression of digital mages

bits. This requires a good quantizer. The second approach i s the variable length coding. Here, longer code words ar e assigned to less frequent used symbols and shorter code wor ds are assigned to more frequently used symbols. Examples f or coding algorithms using this approach are Huffman and arith metic coding. A third approach which is tailored to wavele t is Shapiro's tree encoding. It exploits the self-similarity between the differen t wavelet bands.

The inverse operations are decoding and de-quantization. Fi rst the data is decoded from the quantization table. Afte rwards the dequantized data is computed. Using the inverse wavelet tra nsform, the image data is reconstructed more or less qua lly to the original image data depending on the quality of the hos en wavelet, the chosen quantization method and the hose n coding algorithm. This conventional method is now extended by an additional element that is intended to integrate encryption in wavelet compression.

6. INTEGRATING ENCRYPTION

In wavelet compression, the kind of mother wavelet wh ich leads to a suitable wavelet basis is essential fo r in starting point for the integration of encryption. In first step we have to chose an appropriate mother wavelet. A fea ture for encryption is to hide information in such a way so reveal illegal access to the encrypted data. Keeping this in mind we have to chose another wavelet which is not a standard mother wavelet and which wavelet basis is not even used for other wavelet compressions. After doing this, we will derive a wavele t basis from the mother wavelet. This wavele t basis is to be adapted to image compression. The filter derived from t he wavelet acts as you unlock the process of decompre ssion. This approach describes the use of symmetric key. A s ymmetric key is used for both encryption and decryption. T he exchange of such a key is not secure, because the interce ption of the key make it possible to decrypt the later enc rypted

with this key. A solution is to encrypt the key with an asy
the public key is used for encryption and the other key al
key infrastructure can be defined as follows. The receiver
sends the public key to the sender. The sender, which has
encrypts the filter data with the public key and sends it
decrypts the data, gets the filter data and is able

mmetric key. An asymmetric key pair consists of keys. One
le the private key is used for decryption. The approach of
ich wants to get the encrypted messages generates the
rforms the wavelet compression and has extracted the
together with the compressed image to the receiver. Th
reconstruction of the image. Figure 6 gives an overview of

called
public
key pair and
filter
receiver
this scenario.

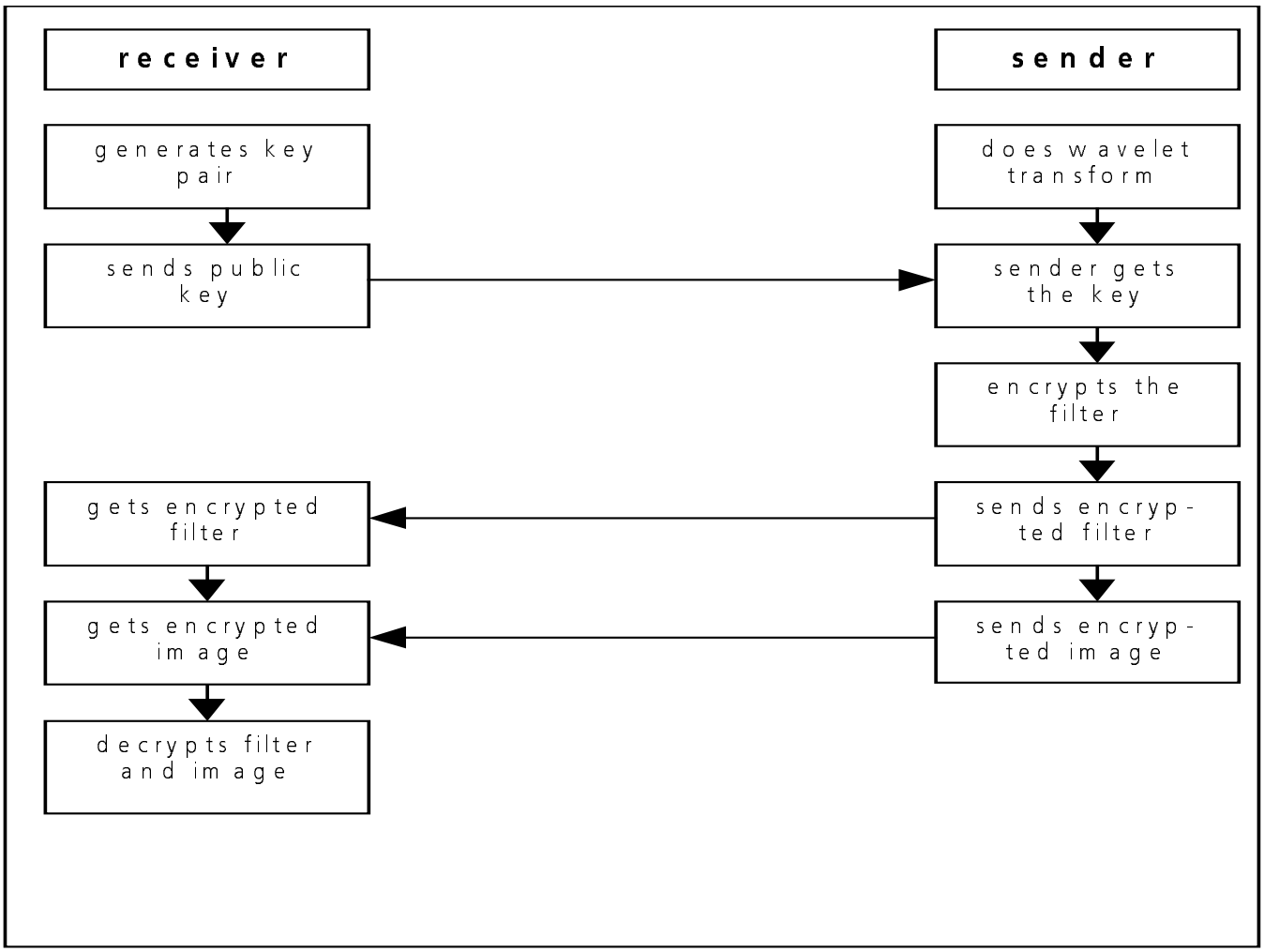

Figure 6: Scenario of secure transfer of wavelet-to

mpressed images

7 CONCLUSION

This paper described a way to integrate encryption in
leaving out the information about which filter is used to
asymmetric key which has to be exchanged by using public/pr
by constructing a new secret mother wavelet which is
wavelet is considered time consuming process. The de
and the process of construction should be automated.

approach of wavelet compression. The encryption is integr
perform the wavelet transform. The filter informati
ivate-key-pair. The security of the symmetric key is ea
dapted to image compression. The method to construc
mand to construct a new wavelet in order to integrate

ated in
on is regarded as
ched
another
encryption

REFERENCES

1. A. Graps, An Introduction to Wavelets, IEEE Computational Science and Engineering, vol. 2, no. 2, Summer 1995
2. A. Fournier, Wavelets and their applications, SIGGRAPH 1995, pp. 18-35
3. L.-M. Reissel, Multiresolution Wavelets, SIGGRAPH 1995, pp. 37-70
4. W. Sweldens, Wavelets, Signal compression and image processing, SIGGRAPH 1995, pp. 107-122
5. G. Strang, Wavelets and Dilation Equations: A brief introduction, SIAM Review, vol. 31, no. 4, December 1989, pp. 614-627
6. E. J. Stollnitz, T. D. DeRose, and D. H. Salesin, Wavelets for Computer graphics: theory and applications, Morgan Kaufmann 1996, Kap. 1-3
7. T. Milde, Videokompressionsverfahren im Vergleich, dpunkt 1995, Kap. 3.5
8. M. L. Hilton, B. D. Jawerth, and A. Sengupta, Compressing Still and Moving Images with Wavelets, Multimedia Systems, Vol. 2, No. 3, paper 1994
9. B. Vidakovic and Peter Müller, Wavelets for Kids, Duke University, 1991
10. E. J. Stollnitz, T. D. DeRose, and D. H. Salesin, Wavelets for Computer graphics: A primer, IEEE Computer Graphics and Applications, May 1995
11. A. K. Louis, P. Maaß, and A. Rieder, Wavelets, Teubner Studienbücher 1995, Kap. 3
12. L. Vorwerk, Bildkompression mit Wavelets, Seminar, C.v.O. Universität Oldenburg, 1997
13. Wavelets and Signal Processing, G. Székely, A. Eide, T. Lindblad, C. Lindsey, M. Minerskjöld, and G. Sekhniaidze, Department of Physics, Royal Injstitute of Technology, Stockholm, Sweden, 1996
14. Using Wavelet Transforms for Hurst Exponent Determination, I. Simonsen, A. Hansen, cond-mat/9707153, 1997