Quantization-based semi-fragile public-key watermarking for secure image authentication

Mathias Schlauweg*, Dima Pröfrock, Torsten Palfner and Erika Müller

University of Rostock
Institute of Communications Engineering
Richard-Wagner-Strasse 31, 18119 Rostock, Germany

ABSTRACT

Authentication watermarking approaches can be classified into two kinds: fragile and semi-fragile. In contrast to the latter one, fragile watermarking does not tolerate modifications of any single bit of the watermarked data. Since the transmission of digital data often requires lossy compression, an authentication system should accept non-malicious modifications such as JPEG compression. Semi-fragile techniques aim to discriminate malicious manipulations from admissible manipulations. In our approach, we extract image content dependent information, which is hashed afterwards and encrypted using secure methods known from the classical cryptography. The image data is partitioned into non-overlapping 4x4 pixel blocks in the spatial domain. The mean values of these blocks form *n*-dimensional vectors, which are quantized to the nearest lattice point neighbours. Based on the changed vector values, a hash is calculated and asymmetrically encrypted, resulting in a digital signature. Traditional dual subspace approaches divide the signal space into a region for signature generation and a region for signature embedding. To ensure the security of the whole image, we join the two subspaces. The vectors, where to embed the bits using quantization-based data hiding techniques, are predistorted and also used for the signature generation. Our scheme applies error correction coding to gain the robustness of the embedded signature to non-malicious distortions. A second quantization run finally embeds the signature.

Keywords: semi-fragile watermarking, image authentication, multidimensional lattice quantization, error correction

1. INTRODUCTION

The rapid evolution of multimedia technology over the past decade has brought many advantages in the creation and distribution of image content. But beneath the ability of easy copying, transmitting and editing digital images the need for image content protection increases. Digital images can be modified or forged with a wide variety of available manipulation software and hence it is rather difficult to tell if a picture is the original one or if it has been tampered with.

Image authentication techniques based on digital watermarking and cryptography aim to prevent illegitimate tampering and fraudulent use of modified images. As known from the classical cryptography, to verify the exact data integrity, a signature is generated from the source signal by the use of secure hash functions (e.g. SHA-1, MD5). Afterwards, the signature message digest is encrypted with a secret key. The recipient decrypts the signature and matches it with the hash generated from the received signal [1]. If even one bit of the signal is modified, it will no longer match the signature, so any tampering can be detected. However, this so-called fragile property is sometimes not practical when considering distribution of images. For instance, lossy compression has to be performed to reduce the amount of data or signal processing is applied to correct gamma, to de-noise or to resample an image. These manipulations change the pixel values but not the content and hence not the authenticity.

Semi-fragile authentication methods for digital images were introduced to tolerate certain kinds of processing. The aim is to allow admissible manipulations such as JPEG compression, but to reject malicious manipulations, which change the image content. As can be seen in several overview papers [2, 3, 4, 5] representing the state of the art, security services, such as image content authentication, are still marginal. The majority of publications in the field of digital watermarking mainly address data hiding [6, 7], the commonly used term for both steganography and robust digital watermarking for, e.g., copyright protection of still images.

*mathias.schlauweg@uni-rostock.de; phone +49-381-498-3580; fax +49-381-498-3595

Copyright 2005 Society of Photo-Optical Instrumentation Engineers.
This paper will be published in Proceedings of SPIE vol. 5915, Mathematics of Data/Image Coding, Compression, and Encryption VIII, with Applications, and is made available as an electronic preprint with permission of SPIE. One print or electronic copy may be made for personal use only. Systematic or multiple reproduction, distribution to multiple locations via electronic or other means, duplication of any material in this paper for a fee or for commercial purposes, or modification of the content of the paper are prohibited.

The process of secretly embedding information inside a data source without changing its visual perception, namely steganography, is one of the earliest applications of watermarking. The information embedder is primarily interested in hiding the very presence of the message itself from an observer. Robust digital watermarking, in turn, strives to add a signal as robust as possible to the data source. The main emphasis here is on robustness, whereas the embedded data should survive any signal processing operation the host signal goes through. In other words, if someone is able to remove the watermark, the perceptual quality of the host signal should be destroyed as well.

Unlike in robust schemes, the embedded watermark information for the purpose of authentication and content integrity verification is supposed to be fragile. One expects a watermark to be destroyed when the host data is maliciously attacked followed by an alarm to be raised caused by the extraction of the wrong watermark information. This description could be one kind of interpretation of an authentication process, where the watermark is a content independent logo. Another approach is to make the watermark information depending on the content as in the classical cryptography and to embed this watermark inside the host signal with highly robust data hiding techniques. The fragility to signal processing operations, that do not preserve the image content, is inherited to the content dependent signature generation stage. The essential features of data hiding techniques such as invisibility and robustness preferably against any kind of attack are desirable for the signature embedding stage of an authentication framework as well.

Since it can be assumed that the attacker has full knowledge of the overall authentication watermarking framework, the image content dependent watermark information has to be encrypted asymmetrically [1] before embedding. This is the only way to prevent the attacker's ability of replacing the right content dependent embedded watermark information by a wrong manipulated one. Roughly speaking, anybody should be able to verify the authenticity of a watermarked image, but nobody unless the originator should be able to replace it. In the case of a "trustworthy camera" [8], the private key to embed the watermark should be located inside the camera protected against reading. Not even the photograph must know this private key. However, as opposed to common data hiding schemes, the overall security of an authentication watermarking framework can not be gained by scrambling the positions where the content dependent signature is generated from or embedded to. Therefore, as already discussed by Fei et al. [4], the signature embedding positions have to be protected. Otherwise, an attacker knowing these positions could change the whole region used for embedding as long as the same watermark will be extracted leaving the generation region unmodified.

In our authentication framework, we combine generation and embedding of content dependent signature information. The content dependent watermark information is generated from all image pixel values using lattice quantization. A cryptographically secure hash function maps this information to a small amount of data, which will be encrypted and embedded. All embedding positions are pre-distorted and hashed as well. The process of pre-distortion avoids that the already generated hash value will be affected by the embedding of the signature in a second quantization run.

Firstly, we introduce different lattice quantization techniques to embed information into an image. As we will see, by using more sophisticated multidimensional quantization and error correction coding (ECC), we are able to reconstruct information bit errors as well as the hash values at these error positions in a defined range. In that way, the robustness against non-malicious distortions such as JPEG compression can be gained without raising security gaps. In section 3, we will explain and analyze our authentication framework more in detail. Experimental results will be shown in section 4 and conclusions will be given in section 5.

2. MULTIDIMENSIONAL LATTICE QUANTIZATION

In this section, we describe the use of multidimensional lattices for quantization as one possible data hiding technique. The problem of finding the optimal quantization lattice in each dimension will be considered as the classical sphere packing problem, which asks for the densest packing of equal-sized spheres in Euclidean n-dimensional space. A raised number of dimensions used for quantization results in increased robustness of the embedded information to uniformly distributed noise. Simultaneously, using more dimensions for quantization and hence more samples of the host signal yields a higher embedding-induced distortion for the same amount of information. Since data hiding is interested in a trade-off between the amount of distortion introduced to the host signal and the amount of hidden data, often lower-dimensional quantization is used. As opposed to raising the number of dimensions for quantization, error correction coding can be used before embedding the information. This kind of error protection affects the amount of hidden data as well, so we will compare both strategies the use of multidimensional quantization and error correction coding.

2.1. Quantization based data hiding

In [9], Chen and Wornell presented a class of embedding methods, called quantization index modulation (QIM), as an efficient method of digital watermarking. The information m is embedded by constructing a set of different vector quantizers $Q(\cdot)$ and by mapping the host signal samples z to the elements of these different quantizers. For example, if the set consists of two different subsets, as shown in Fig. 1 by the points marked with ×'s and ○'s, the information can be embedded in binary form, where $m \in \{0, 1\}$. If a binary bit "0" has to be embedded, z is quantized to the closest subset point ×, otherwise, if a binary bit "1" has to be embedded, the closest ○ is chosen. The amount of embedding distortion induced is determined by the sizes and shapes of the quantization cells, also called Voronoi cells comprising all points closer to its centre than to any other one. The minimum distance d_{min} between two neighbouring cell centres of the quantization set determines the robustness of the embedding. At the receiver side, after the watermarked signal is perturbed by a noisy channel, the decoder simply acts by quantizing the received signal y to the closest reconstruction point of the quantizer set obtaining the message $\hat{m}$:

$$\hat{m}(y) = \arg \min_{m} \left\| y - Q_m(y) \right\| \tag{1}$$

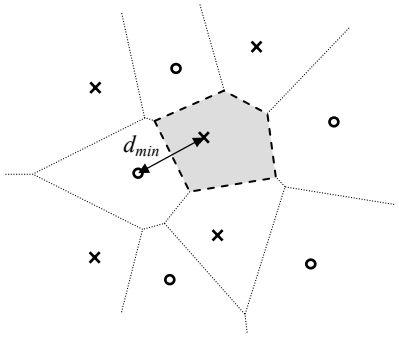

Figure 1: Voronoi cells of a QIM vector quantizer set

2.2. Dither modulation

A low-complexity realisation of the QIM method, namely dither modulation (DM), is similar to the scalar Costa scheme (SCS), proposed by Eggers and Girod [10]. It uses a set of uniform dithered scalar quantizers with step size Δ. Each quantizer subset can be expressed as $Q_m(\cdot - d_m) + d_m$, where the parameter d_m is called dither vector modulated with the embedded signal m. The host signal is divided into N length-n non-overlapping data blocks $z = \{z_i, 1 \le i \le N\}$. By embedding the information $m = \{m_i, 1 \le i \le N\}$ symbol-wise into these blocks an embedding rate of $1/n$ is achieved.

The Voronoi cells or, in other words, the cell centres of any given quantizer subset in the ensemble of dithered quantizers are shifted versions of the cells of any other subset in the ensemble. Since every ensemble consists of regularly spaced points of countable infinite number in real n-dimensional Euclidean space $\mathbb{R}^n$, these points can be considered as a lattice.

2.3. Lattice structures and sphere packings

A lattice, denoted as Λ, is the set of all integral combinations of linearly independent basic vectors v, in $\mathbb{R}^n$, [11]. Including the origin, its points have a fixed minimum distance d_{min}. With relation to quantization-based data hiding, lattices can be partitioned into subsets Λ', which are itself lattices, corresponding to the different quantizers of the quantizer ensemble. Some lattice structures produce better so-called spherical codes than others for the same n-dimensional space. The aim is to maximally separate neighbouring lattice points from each other so that the quantized signal is maximally robust to the additive Gaussian noise of the channel. On the other hand, the distortion introduced by mapping a host signal sample to the nearest lattice point should be as small as possible.

In the past, a certain amount of research has been investigated on topics in both lattices and sphere packings. The so-called "kissing number problem" considers the question of how many white spheres can maximally touch a black sphere of the same size in n-dimensional space at the same time [12]. Related to coding theory, we are looking for the maximal number of length-n codewords for a code with minimum distance d_{min}. The densest packing in Euclidean $\mathbb{R}^1$ is trivial. But, as can be seen in Fig. 2 and Fig. 3, even for the 2-dimensional case there are different possible packings, e.g., the square lattice, denoted by D_2, or the hexagonal lattice, denoted by A_2. Whereas in the case of squarely packing balls in the plane four other balls "kiss" the centred one, in the hexagonal case six balls just perfectly surround the ball in the middle.

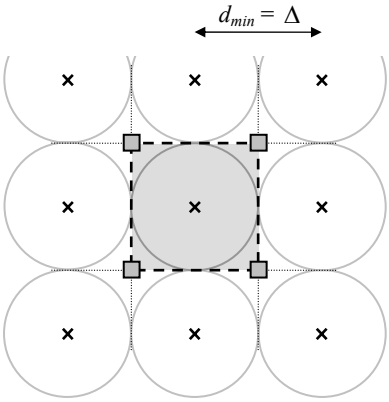

Figure 2: Square lattice D_2

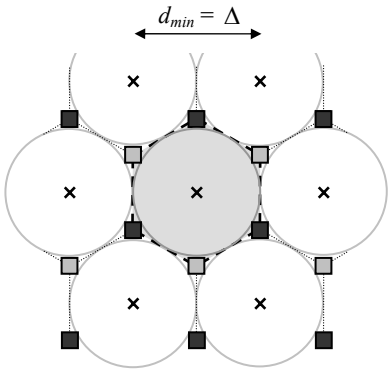

Figure 3: Hexagonal lattice A_2

By comparing these both planar packings, the space between neighbouring balls is smaller for the hexagonal structure. We say that its density δ, defined as the quotient of the volume of the unit sphere divided by the volume of the fundamental Voronoi region, is higher. Hence, $\delta = 1$ is the upper bound for any kind of sphere packing and so it is desirable that the Voronoi region $\mathcal{V}$ associated with a particular lattice point has nearly spherical form. Among others, in [13], the authors try to give an answer to this question. They consider the problem of existence of lattices in Euclidean space which are simultaneously good for sphere packing, sphere covering, channel coding and quantization. In the case of the packing problem, as mentioned above, a lattice should be structured such that the greatest possible number of non-intersecting spheres of the same given radius $d_{min}/2$ can be packed together. Roughly speaking, primarily the volume of a Voronoi region $Vol(\mathcal{V})$ is to be minimized. The sphere covering problem, instead, seeks to minimize the size collection of the arranged spheres, which means that the Voronoi region should have nearly spherical form. An optimization according to the latter criterion results in lower quantization-induced distortions. In the 2-dimensional space, the hexagonal lattice is optimal in terms of sphere packing as well as sphere covering. But, as we will see when considering $\mathbb{R}^3$, a denser sphere packing not always stands for lower mean-squared error (MSE) distortions per dimension, defined as:

$$\overline{D}_e = \frac{1}{n} \cdot \frac{1}{Vol(\mathcal{V})} \int_{\mathcal{V}} \left\| z - Q(z) \right\|^2 dz \tag{2}$$

The lattice points in both Fig. 2 and Fig. 3 marked with ×'s represent one quantizer subset, which can only be used for quantizing the host signal but not for embedding information. To do so, more than one quantizer set is needed of course. Since the small squared areas at the gaps between the balls namely "deep holes" are the points furthest away from the ×'s, these positions are ideal for placing other quantizer subsets. If all deep holes of a given lattice are fully used, the conjunction of the quantizer subsets is denoted as dual lattice structure. A given lattice is self-dual if it is identical to its dual. In Fig. 3, there are two different shadings for the small squared areas, meaning that this lattice structure is optimally suited for an ensemble of three different quantizer subsets and hence for using a ternary symbol alphabet for the hexagonal lattice. Although the embedding capacity can be increased by a factor of $(3/2)^n$ due to the 3-ary scheme, the minimum distance between different lattice points is $\sqrt{3/2}$ times lower, compared to the square lattice.

Considering the 3-dimensional Euclidean space $\mathbb{R}^3$, we need to distinguish between three different lattice packings: the "simple cubic", the "body-centred cubic (bcc)" and the "face-centred cubic (fcc)". In Fig. 4, the oblique projections are summarized for these three types of lattice packings. The density δ per dimension is equal for both the planar square lattice and the simple cubic lattice, which is denoted by $\mathbb{Z}^3$. As opposed to the fcc lattice D_3, which is the unique densest lattice sphere packing for three dimensions, the Voronoi region of the bcc lattice D_3^* is better suited for quantization in sphere covering sense. Its Voronoi region, a truncated octahedron, is most "close" to spherical form, as can be seen in Fig. 5. In [14], Barnes and Sloane proofed that the bcc lattice has the smallest MSE distortion of any lattice quantizer in three dimensions, if the input to the quantizer can be assumed to have a uniform distribution.

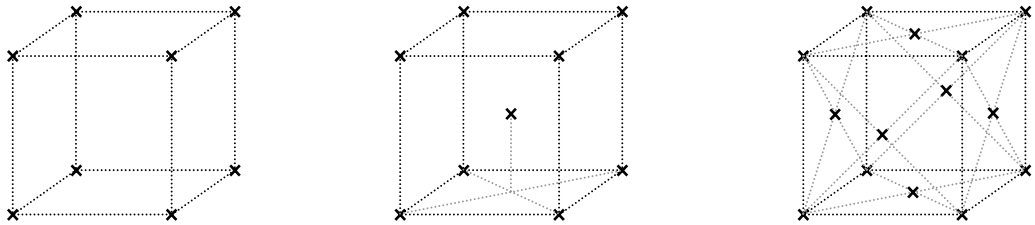

Figure 4: Simple cubic $\mathbb{Z}^3$ (left); body-centred cubic D_3^* (middle); face-centred cubic D_3 (right)

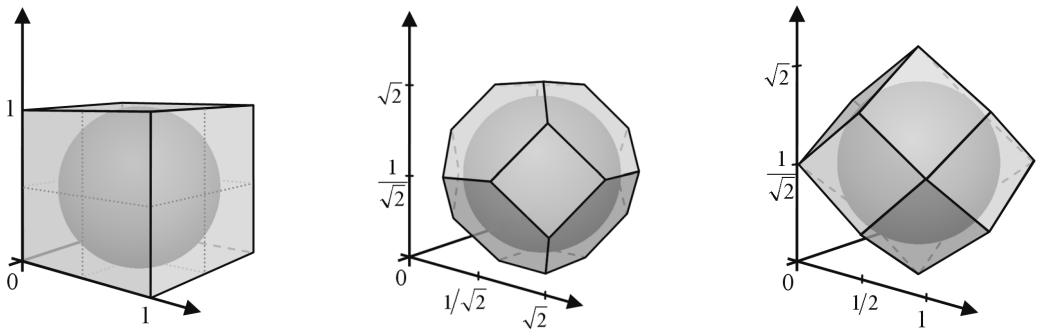

Figure 5: Voronoi regions of the simple cubic lattice (left), bcc lattice (middle), fcc lattice (right)

For the most dimensions the optimal sphere arrangement is not unique. For example, besides the fcc lattice, there is another periodic sphere packing in $\mathbb{R}^3$ with equal density, the so-called hexagonal close packing, denoted by A_3, which we can imagine as an extension of the planar hexagonal structure A_2. However, the hexagonal close packing does not fulfill the definition of a lattice, because it is not invariant with respect to any structural translations. Furthermore, its Voronoi region is even worse than the one of the fcc lattice in sphere covering sense.

Placing a second quantizer subset into the deep holes of the simple cubic lattice yields the structure of the body-centred cubic and vice versa. On the hand, the dual of the face-centred cubic lattice is the so-called diamond packing, which can be seen as the interpenetration to two fcc lattices, displaced along the body diagonal of the cubic cell by one quarter the length of the diagonal. Both distinct reciprocal pairs of structures in the 3-dimensional space are not self-dual. Furthermore, the diamond packing D_3^+, also known as tetrahedral packing, does not fulfill the definition of a lattice as well.

The optimal kissing configuration of spheres in $\mathbb{R}^4$ is not that easy to demonstrate as the configurations in the dimensions before, because human beings understandably have difficulties when imagining 4-dimensional objects. However, as explained in [15], the so-called D_4 lattice is known to yield the best sphere packing in $\mathbb{R}^4$. It consists of all the permutations of the points (v_1, v_2, v_3, v_4) having integer coordinates whose sum is even. The mathematical definition is:

$$D_4 = \left\{ (v_1, v_2, v_3, v_4) \in \mathbb{Z}^4 \mid v_1 + \ldots + v_4 = k;\ k : even \right\} \tag{3}$$

For example, all permutations of the points $(\pm 1, \pm 1, 0, 0)$ yield the 24 centres for the kissing configuration of equal-sized unit spheres in addition to the sphere at the origin (0, 0, 0, 0). The minimum distance between these lattice points is given by $d_{min} = \sqrt{2}$.

To embed binary information the D_4 lattice plus another one shifted by the dither vector $d_m = (1/2, 1/2, 1/2, 1/2)$ in coordinates can be used. The resulting lattice is the so-called D_4^* or 4-dimensional hyper-diamond lattice. The next-to-nearest neighbour vertex figure of the hyper-diamond lattice is the D_4 lattice nearest neighbour vertex figure, the famous "24 cell", which means that both lattice structures are self-dual. The facets of this 4-dimensional polytope are 24 regular octahedra. Since the Voronoi regions of both lattices D_4 and D_4^* have the same form and a volume $Vol(\mathcal{V}) = 8 \cdot d_{min}$, the good properties of the D_4 lattice are equal for both structures.

Another possible lattice structure in $\mathbb{R}^4$ can be seen as the extension of the dual pair of simple cubic and body-centred cubic known from three dimensions. The simple hypercubic lattice $\mathbb{Z}^4$ plus another one shifted by the corresponding dither vector $d_m = (1/2, 1/2, 1/2, 1/2)$ results in the lattice structure A_4^*, which we call body-centred hypercubic. It is known to have the best sphere covering probabilities in 4 dimensions [11].

The volume calculations of both unit spheres and Voronoi regions for the dimensions one to three are trivial. For a 4-dimensional unit sphere $\mathbb{S}_4$ the volume is given by $Vol(\mathbb{S}_4) = \pi^2/2$. Hence, the densities δ and the MSE distortions per dimension $\overline{D}_e$ (Eqn. 2) due to quantization for the lattices described above can be calculated and summarized as follows:

Dimension	Description of the lattice	Name	Density δ	Distortion $\overline{D}_e$
$\mathbb{R}^1$	simple integer	$\mathbb{Z}^1 = A_1^*$	1	$\simeq 0.0833$
$\mathbb{R}^2$	hexagonal	$A_2 = A_2^*$	$\simeq 0.9069$	$\simeq 0.0802$
	simple square	$D_2 = D_2^*$	$\simeq 0.7854$	$\simeq 0.0833$
$\mathbb{R}^3$	face-centred cubic	D_3	$\simeq 0.7405$	$\simeq 0.0788$
	body-centred cubic	D_3^*	$\simeq 0.6802$	$\simeq 0.0785$
	simple cubic	$\mathbb{Z}^3$	$\simeq 0.5236$	$\simeq 0.0833$
$\mathbb{R}^4$	hyper-diamond	$D_4 = D_4^*$	$\simeq 0.6169$	$\simeq 0.0766$
	body-centred hypercubic	A_4^*	$\simeq 0.4414$	$\simeq 0.0776$
	simple hypercubic	$\mathbb{Z}^4$	$\simeq 0.3084$	$\simeq 0.0833$

Table 1: Sphere packing densities and MSE distortions of the considered lattices, where the asterisk denotes the dual lattice structure meaning that all deep holes are fully used

When considering the D_4 lattice as opposed to both the simple hypercubic and the body-centred hypercubic lattice quantization, a performance gain can be seen. The D_4 lattice has a higher density and lower mean squared-error distortions than other lattices in four dimensions. In the next section, we will prove the expected gain by experimental results.

3. PROPOSED AUTHENTICATION FRAMEWORK

After the above introduction concerning sphere packings and lattice structures, in this section, we propose our authentication framework using multidimensional dither modulation and error correction coding. We will compare the considered lattices and discuss which is best suited for our approach under robustness and distortion constraints.

Although our semi-fragile watermarking scheme works in spatial domain, other domains could be used as well. The scheme is blind, which means that no further watermark information except the public key and the embedding strength parameter Δ have to be submitted besides the watermarked image. No metadata, which could get lost due to format transformations, is necessary. The framework is structured modularly so that single components such as the hash function or the used encryption can be replaced without influencing the overall functionality.

As already mentioned, we inherit the task of semi-fragility to the image content dependent signature generation stage. Features, robust to allowed small image manipulations but fragile to malicious tampering, are extracted from the image and hashed using a cryptographic hash function. Afterwards, the encrypted signature is robustly embedded into the image data using multidimensional dither modulation, as one possible well known data hiding technique. At the verification side, the same signature generation will be applied extracting the same content dependent features as long as the content has not been maliciously manipulated. The inverse data hiding scheme will be used to extract the embedded signature, which will be decrypted and compared with the hashed features, as shown in Fig. 6. Our scheme allows embedding additional information together with the asymmetrically encrypted feature hash value. This could be used to, e.g., identify both hash and encryption methods. The suggested concept of embedding unsecured additional information assumes that an attacker has no profit from changing. As we will explain more in detail in section 3.2, error correction coding (ECC) can be used to gain the robustness of the embedded information or, in other words, to reconstruct bit errors due to channel distortion.

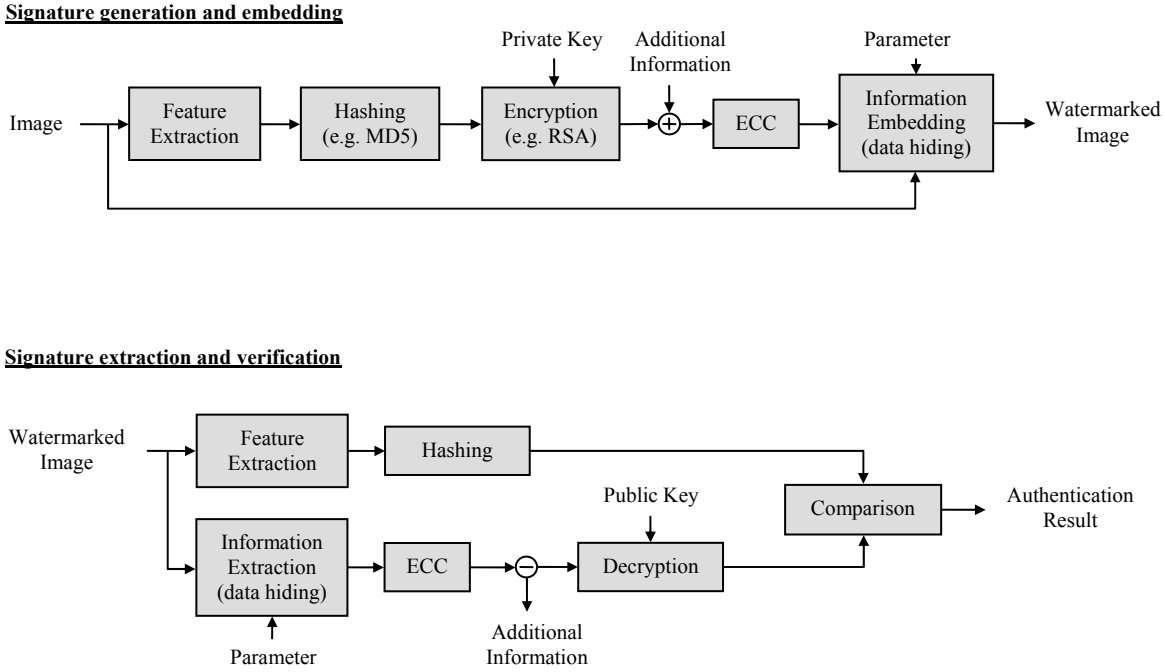

Figure 6: Authentication process (signature generation and embedding) & signature verification process.

3.1. Quantization-based feature extraction and embedding

There are many different ways to extract content dependent features from an image [2, 3, 4, 5]. For example, some approaches involve image positions of edges, contours or zero-crossings in the spatial domain whose existence is proved during the verification process. Other methods are based on single coefficients or on relationships between pairs of coefficients in the transform domain (e.g., DCT, DWT or DFT). The technique described here uses the mean values of non-overlapping pixel blocks directly. All approaches have in common that the gathered features will be quantized to allow some small amount of pre-defined distortion and hence to be semi-fragile.

In our watermarking approach, the image is partitioned into $L \times L$ pixel blocks (e.g., 4×4 pixels) in the spatial domain. The mean values of these blocks form n-dimensional vectors $z = \{ z_i, 1 \leq i \leq M \}$, which are quantized using n-dimensional lattice quantization. The size ($L \times L$) of the pixel areas represented by every single mean value determines the robustness of the watermarked image due to distortions such as JPEG compression. The larger the block size, the higher is the robustness. But on the other hand, larger block sizes result in a higher vulnerability to the following malicious

manipulation. An attacker, who maintains the protected quantized mean value for the corresponding $L \times L$ pixel block, could change any pixel of this block. He would be able to insert edges or textures into the image changing the content. Hence, the verification of the authenticity for a watermarked image does only hold up the original image resolution divided by the factor L.

As can be seen in Fig. 7, two subsequent quantization runs are applied during the authentication process. In the first loop, the mean value vector is quantized to the nearest lattice point neighbour using the step size Δ. All quantized values are hashed and encrypted using RSA (e.g., with 1024 bit). Afterwards, the bit string can be passed through any kind of ECC, e.g., block-based BCH-Coding [16] to lower the probability of single bit errors due to channel distortions. In the second loop, the resulting length-N signature is embedded symbol-wise into $N \leq M$ samples of the pre-distorted sample vectors.

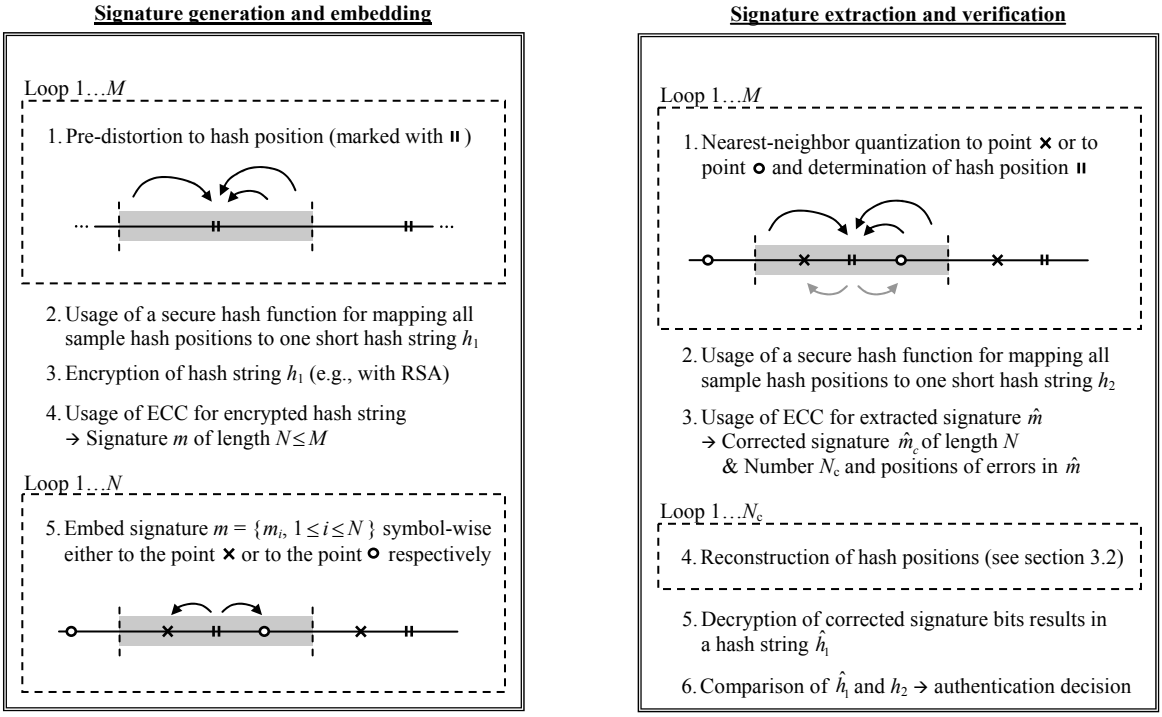

Figure 7: Authentication watermark embedding and verification steps exemplary for simple integer quantization.

At the verification side, both the feature extraction (quantization of block mean values) and the determination of the embedded signature bits take place simultaneously. By nearest neighbour quantization of every single sample vector to either a point marked with × or to a point marked with o, each representing one quantizer subset, the signature bits are extracted. Each region, which we also call hash position here, consists of one × as well as one o.

In Fig. 7, we demonstrated the steps only for simple integer quantization, but higher-dimensional lattice quantization can be used in the same way. For example, in the case of the D_4^* lattice, the 4-dimensional sample vectors are pre-distorted to the root lattice D_4. To embed binary information the pre-distorted vector is either shifted by the vector $(1/4, 1/4, 1/4, 1/4)$ or by the vector $(-1/4, -1/4, -1/4, -1/4)$ respectively.

3.2. Reconstruction of signature and hash during verification using ECC

To be able to compare the lattice structures A_1^*, D_2^*, D_3^*, A_4^* and D_4^* concerning information induced embedding distortions, we use the same minimum distance (dither vector) between the points of their different quantizer subsets. As opposed to the former ones, the distance between the lattice points of the same subset is $\sqrt{2}$ times higher in the case of

the D_4^* lattice. This can be used considering error correction coding. When we imagine a binary "1" to be embedded into a sample vector (see Fig. 8) and due to channel noise the vector would be distorted more than $d_{min}/2$, a verification error would occur (see Fig. 9). A signature bit "0" instead of the bit "1" would be detected and a wrong hash position would be determined. But if we are able to reconstruct the embedded signature bit using ECC, then also the hash position can be reconstructed as long as the distortion was not stronger than d_{min}. Fig. 10 shows the basic principle, which can be used for higher-dimensional quantization as well. The quantization cell may be thought of as a shifted overlapped version of the original cell. Hence, the range of accepted channel distortion is raised without security loss.

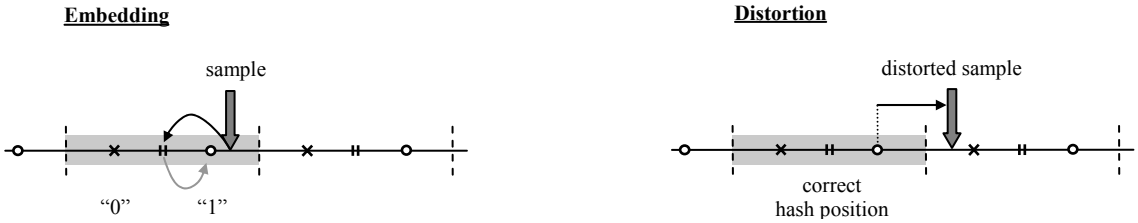

Figure 8: Distortion of a sample vector due to channel noise

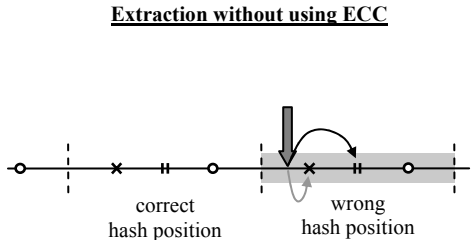

Figure 9: Occurrence of verification errors

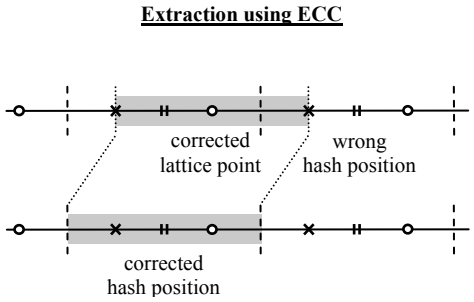

Figure 10: Hash reconstruction using ECC

4. EXPERIMENTAL RESULTS

If we use a (63, 16)-BCH code for error correction coding, the signature is approximately 4 times longer. Hence, more bits have to be embedded into the image, which means that more blocks have to be stronger distorted. Fig. 11 shows the peak-signal-to-noise-ratio (PSNR) as a function of the embedding strength parameter Δ for both embedding without ECC and embedding with ECC. As can be seen clearly, the more sophisticated D_4^* lattice yields lower embedding induced distortions than all other considered lattice structures when no ECC is used. In the case of using ECC instead, the simple integer lattice A_1^* is more advantageous.

In Fig. 12, the robustness to allowed high-quality JPEG compression is shown. By simulations on numerous standard test images of size 512 x 512 pixels, we have determined to which JPEG quality factor the watermarked image can be maximally compressed without raising an alarm. If no ECC is used, the D_4^* lattice is most robust to channel distortion such as JPEG compression. But if ECC and the proposed hash position reconstruction are used, the A_1^* quantizer ensemble is better suited for our authentication scheme. The result is not surprisingly, since block-based error correction coding is nothing else than a more sophisticated higher-dimensional lattice quantization as well.

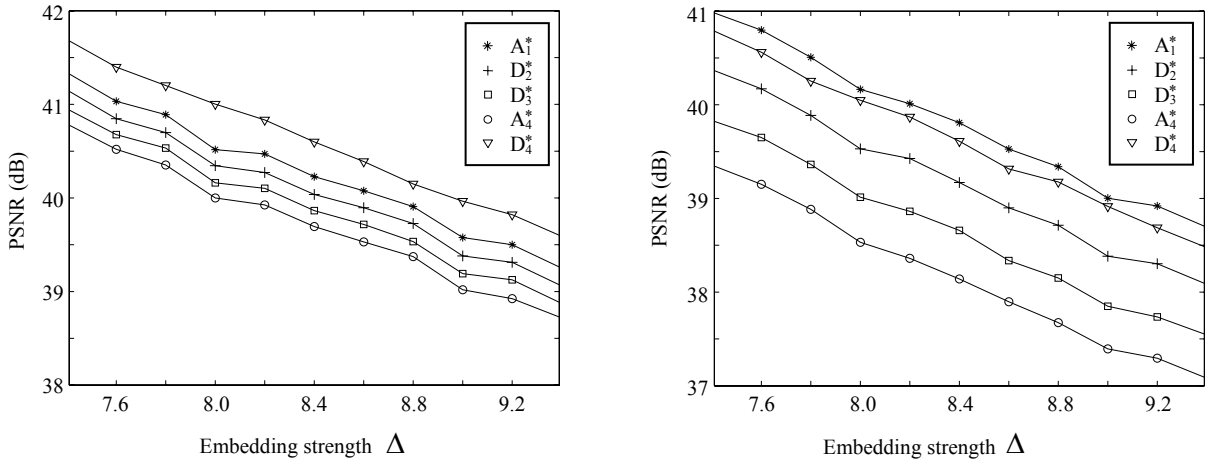

Figure 11: Embedding induced distortions without using ECC (left) and using ECC (right)

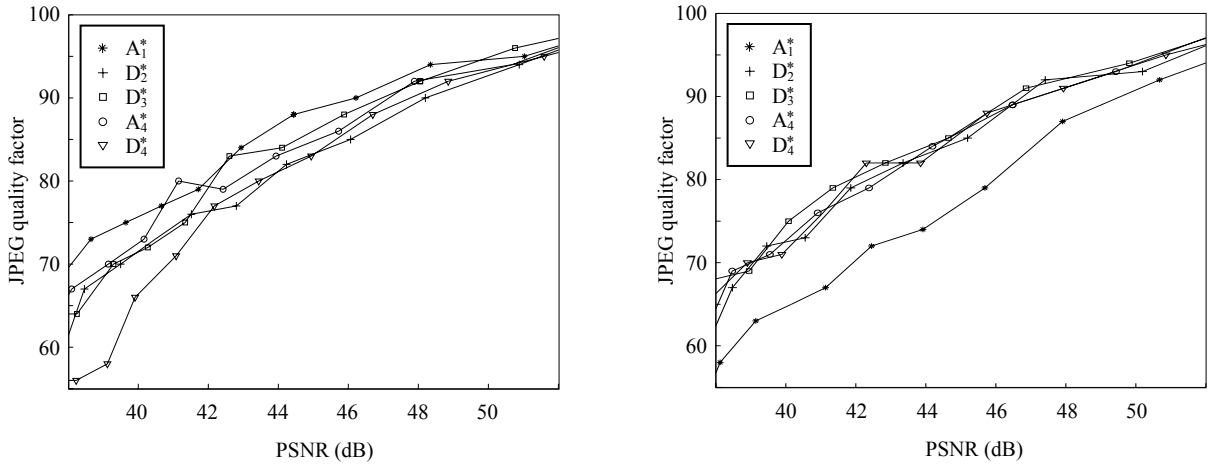

Figure 12: Robustness to allowed JPEG compression without using ECC (left) and using ECC (right)

5. CONCLUSION

In this paper, we proposed a semi-fragile authentication watermarking scheme for secure image authentication. The scheme allows some small amount of distortion to the image such as high-quality JPEG compression, but rejects larger manipulations changing the image content. We gave a detailed overview to multidimensional lattice quantization known from the field of data hiding, which can be used to generate and embed image content dependent information. In our watermarking approach, the image is partitioned into 4 x 4 pixel blocks in the spatial domain. The mean values of these blocks form *n*-dimensional vectors, which are quantized using *n*-dimensional lattice quantization. We compared different lattice quantization techniques to determine which is best suited for our scheme. Based on the changed vector values, a digital signature is generated using secure hash functions and asymmetrical encryption. To ensure the security

of the whole image, we joined the regions for signature generation and embedding. The sample vectors, where the signature bits are to be embedded, are pre-quantized and also used for signature generation. This strategy offers the possibility to reconstruct distorted sample vectors using error correction coding and hence to gain the robustness of the embedded signature. The framework was structured modularly so that single components such as the hash function or the used encryption method can be replaced without influencing the overall functionality.

REFERENCES

1. Technical Institute of Standards and Technology (NIST), "Digital signature standard (DSS)", Technical Report, FIPS PUB 186-2, 2000.
2. Ö. Ekici, B. Sankur, B. Coşkun, U. Nazi and M. Akcay, "Comparative evaluation of semifragile watermarking algorithms", Journal of Electronic Imaging, **vol. 13 (1)**, pp. 209- 216, 2004.
3. B. B. Zhu, M. D. Swanson and A. H. Tewfik, "When seeing isn't believing", IEEE Signal Processing Magazine, **vol. 21 (2)**, 2004.
4. C. Fei, D. Kundur and R. Kwong, "Analysis and Design of Secure Watermark-based Authentication Systems", IEEE Trans. Signal Processing Supplement on Secure Media, accepted for publication December 2004, to appear.
5. C. Rey and J.-L. Dugelay, "A Survey of Watermarking Algorithms for Image Authentication", EURASIP Journal of Applied Signal Processing, **vol. 6**, pp. 613-621, 2002.
6. P. Moulin and R. Koetter, "Data Hiding - Theory and Algorithms", *Lecture Notes*, Institute for Mathematical Science, Singapore, 2003.
7. H. W. Wong, "Image Watermarking and Data Hiding Techniques", *Thesis (Ph.D.)*, The Hong Kong University of Science and Technology, Hong Kong, 2003.
8. G. L. Friedman, "The trustworthy digital camera: restoring credibility to the photographic image", IEEE Trans. on consumer electronics, **vol. 39 (4)**, pp. 905-910, 1993.
9. B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding", IEEE Trans. on Inform. Theory, **vol. 47**, pp. 1423-1443, 2001.
10. J. Eggers, J. Su and B. Girod, "A Blind Watermarking Scheme Based on Structured Codebooks", *Secure Images and Image Authentication, Proc. IEE Colloquium*, pp. 4/1-4/6, London, 2000.
11. J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed., Springer-Verlag, New-York, 1999.
12. F. Pfender and G. M. Ziegler, "Kissing numbers, sphere packings, and some unexpected proofs", Notices of the American Mathematical Society, **vol. 51**, pp. 873-883, 2004.
13. U. Erez, S. Litsyn and R. Zamir, "Lattices which are Good for (Almost) Everything", *Proc. of the Information Theory Workshop*, pp. 271-274, 2003.
14. E. S. Barnes and N. J. A. Sloane, "The Optimal Lattice Quantizer in Three Dimensions", SIAM Journal on Algebraic Discrete Methods, **vol. 4**, pp. 30-41, 1983.
15. J. J. Chae, D. Mukherjee and B. S. Manjunath, "A Robust Data Hiding Technique using Multidimensional Lattices", *Proc. of the IEEE Forum on Research and Technology Advances in Image Proc.*, pp. 319-326, Santa Barbara, 1998.
16. J. Darbon, S. Sankur and H. Maitre, "Error correcting code performance for watermark protection", *Security and Watermarking of Multimedia Contents, Proc. of the SPIE*, **vol. 4314**, pp. 663-672, San Jose, 2001.