Multidimensional Enhanced Hadamard Error Correcting Code In Comparison with Reed-Solomon Code in Video-Watermarking Applications.

JAKOB WASSERMANN[1], ANDRZEJ DZIECH[2]
[1] Dept. of Electronics and Telecommunications
University of Applied Sciences Technikum Wien,
Hoechstaedrplatz 5,1200 Wien
AUSTRIA
jakob.wassermann@technikum-wien.at
[2] Dept. of Telecommunication
AGH University of Science and Technology
Czarnowiejska 78, 30-001 Kraków
POLAND
adzie@tlen.pl

Abstract. Watermarking technology.play a central role in the digital right management for multimedia data. Especially a video watermarking is a real challenge, because of very high compression ratio (about 1:200). Normally the watermarks can barely survive such massive attacks, despite very sophisticated embedding strategies. It can only work with a sufficient error correcting code method. In this paper, the authors introduce a new developed Enhanced Multidimensional Hadamard Error Correcting Code (EMHC), which is based on well known Hadamard Code, and compare his performance with Reed-Solomon Code regarding its ability to preserve watermarks in the embedded video. The main idea of this new developed multidimensional Enhanced Hadamard Error Correcting Code is to map the 2D basis images into a collection of one-dimensional rows and to apply a 1D Hadamard decoding procedure on them. After this, the image is reassembled, and the 2D decoding procedure can be applied more efficiently. With this approach, it is possible to overcome the theoretical limit of error correcting capability of $(d-1)/2$ bits, where d is a minimum Hamming distance. Even better results could be achieved by expanding the 2D to 3D EMHC. A full description is given of encoding and decoding procedure of such Hadamard Cubes and their implementation into video watermarking procedure.To prove the efficiency and practicability of this new Enhanced Hadamard Code, the method was applied to a video Watermarking Coding Scheme. The Video Watermarking Embedding procedure decomposes the initial video through Multi-Level Interframe Wavelet Transform. The low pass filtered part of the video stream is used for embedding the watermarks, which are protected respectively by Enhanced Hadamard or Reed-Solomon Correcting Code. The experimental results show that EHC performs much better than RS Code and seems to be very robust against strong MPEG compression.

Key-Words: - Hadamard Error Correcting Code, ECC, Hadamard Transform, , Watermarking, DWT, MPEG

1 Introduction

Many applications in telecommunication technologies are using Hadamard Error Correcting Code. Plotkin [1] was the first who discovered in 1960 error correcting capabilities of Hadamard matrices. Bose, Shrikhande[2] and Peterson [3] also have made important contributions. Levenshstein [4] was the first who introduced an algorithm for constructing a Hadamard Error Correcting Code. The most famous application of Hadamard Error Correcting Code was the NASA space mission in 1969 of Mariner and Voyager spacecrafts. Thanks to the powerful error correcting capability of this code it was possible to decode properly high-

quality pictures of Mars, Jupiter, Saturn, and Uranus [5]. A good overview of Hadamard Error correcting code is presented in [6] and [7].
In this paper we introduced a new type of multidimensional Hadamard Code, we called it Enhanced Multidimensional Hadamard Error Correcting Code (EMHC). It can overcome the limit of error correcting capability of d/2-1 bits where d is the minimum Hamming distance. The application of this Code in Video Watermarking gives also a strong proof of its effectiveness. The reason for selecting Video Watermarking lies in strong compression ratio, normally factors greater than 1:200, which is applied to the video sequences. For example, an uncompressed HDTV video stream has a data rate of 1.2Gbit/s and for distribution reason, it must be compressed to 6Mbit/s. For embedded watermarks, it is a big challenge to survive such strong compression ratio. Error correcting code plays a decisive role in surviving of the embedded Watermarks.
This paper has followed the structure: In Chapter 2 contains the introduction into classical Hadamard Error Correcting Code. Chapter 3 describes the new Enhanced Multidimensional Hadamard Code and its error correcting capabilities.
In Chapter 4, the authors explain the Video Watermarking Scheme and the Chapter 5 presents the results and discussion.

2 Hadamard Error Correcting Code

The Hadamard code of *n*-bit is a linear code, which can be generated by rows of a n*n Silvester-Hadamard Matrix H_n. It can encode $k=log_2(n)$. The Hamming distance between the words is constant and is *n/2,* The code can be denoted as $(2^k,k,2^{k-1})$ and it can correct $\left\lfloor \frac{n}{4}-1 \right\rfloor$ errors. The Code Rate is $R=\frac{k}{2^k}$. In the case of *n*=8 we obtain the following matrix:

$$H_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix} \quad (1)$$

The code words are the rows of this Matrix H_8. To get the corresponding Code Book we have to map the -1 entries to 0 (-1➔0). In Table 1 the Code Book of the linear Code (8,3,4) is depicted. The Hamming distance of this code is d=4.

Message	**Code Words**							
0 0 0	1	1	1	1	1	1	1	1
0 0 1	1	0	1	0	1	0	1	0
0 1 0	1	1	0	0	1	1	0	0
0 1 1	1	0	0	1	1	0	0	1
1 0 0	1	1	1	1	0	0	0	0
1 0 1	1	0	1	0	0	1	0	1
1 1 0	1	1	0	0	0	0	1	1
1 1 1	1	0	0	1	0	1	1	0

Table 1. Code Book of Hadamard Code (8,3,4)

The decoding procedure is based on Hadamard Spectrum. The spectral component with the highest value determines the decoding message. The received code word is used to calculate the Hadamard spectrum vector. It is calculated by multiplying the received and converted (0 is mapped to -1) code vector c by the Hadamard Matrix H8.

$$s = c \cdot H_8 \quad (2)$$

Supposed we received the code word:

$$c = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

After conversion (mapping 0 to -1) we receive

$$c = \begin{bmatrix} 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \end{bmatrix}$$

According to the Eq.(2), the decoded Hadamard Spectrum vector is:

$$s = \begin{bmatrix} 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \end{bmatrix} * H_8$$

$$s = \begin{bmatrix} 0 & 0 & 8 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

The third component of the vector s has the highest value in the spectrum; all others are zeroes, s(3)=8, s(i)=0 for i=1,..8 and i≠3. It implicates that the code word at the position i=3 was received. The codebook at that position gives us the ultimate information of the message, which is (010).
In the case of one error, the value of the third component of the spectrum vector s still remains the highest one. For example a corrupted codeword

$$c = \begin{bmatrix} -1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \end{bmatrix}$$

has the Hadamard spectrum vector:

$$s = \begin{bmatrix} -1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \end{bmatrix} * H_8$$
$$s = \begin{bmatrix} -2 & -2 & 6 & -2 & -2 & -2 & -2 & -2 \end{bmatrix}$$

The third component is still the highest one, so the message can be decoded. In the case of two errors, it is already impossible to decode the message unambiguously.

Another type of Hadamard Code, so called punctured Hadamard Code can be created if additionally to the Hadamard Matrix Hn the negated Hadamard Matrix –Hn is used to generate the Code Book. In this case, the code is denoted as (2k,k+1,2k-1), where : 2^k - the length of the codewords, k+1- the length of message words and 2^{k-1} - the minimum Hamming distance. Code Rate can be increased slightly too $R = \frac{k+1}{2^k}$

For this purpose a new matrix C_{2n} with

$$C_{2n} = \begin{pmatrix} H_n \\ -H_n \end{pmatrix}$$

Is created. The rows of C2n are the Hadamard codewords. In the case of n=8, we can discuss the differences between this two versions. In contrast to Hadamard Code (8,3,4) the Hadamard Code (8,4,4), it can correct not only one error but also seven and eight errors.

In case of eight errors, our code-word

$$c = \begin{bmatrix} -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \end{bmatrix}$$

is completely corrupted. In this case, the absolute value of the third component of the Hadamard spectrum is the highest one, and it has a negative sign. A negative sign means that the decoded code word must be inverted.

$$s = \begin{bmatrix} -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \end{bmatrix} * H_8$$
$$s = \begin{bmatrix} 0 & 0 & -8 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

In the case of seven errors, we have exactly the same situation as with one error, however, with one small difference: the third component has a negative sign, what means the decoded word must be inverted. The following figure shows the error correcting capability of an (8,4,4) Hadamard code.

Fig. 1. Error Correcting Capability of 8 Bit Hadamard Code

The (8,4,4) Hadamard code can correct 1,7 and 8-bit errors regardless where they occur within the code words. Generally, we can say that n bit Hadamard code can correct totally $\left\lfloor \frac{n}{2} - 1 \right\rfloor$ types of errors.

Further, in our paper, we will consider only a regular Hadamard Code (not the punctured one), which is denoted as $(2^k,k,2^{k-1})$ where the total number of correcting errors is $\left\lfloor \frac{n}{4} - 1 \right\rfloor$.

2.2 Two-Dimensional Hadamard Error Correcting Code

The 2D Hadamard Error Correcting Code uses so-called basis images instead of Hadamard vectors. The basis images functions are orthogonal to each other, and they can be generated from the Hadamard matrix by multiplication of columns and rows. Generally, we can write

$$A_{ml} = H_n(:,l) * H_n(m,:) \tag{3}$$

In case of 4x4 Hadamard matrix

$$H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

We can calculate the complete set of 16 such basis images.

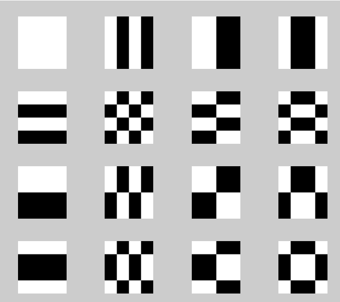


Fig. 2. Basis Images of 2D Hadamard Transform (4x4)

For instance, the pattern A_{31} is generated by Eq.(1) and has the numerical presentation

$$A_{31} = \begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \end{pmatrix}$$

It can be visualized as

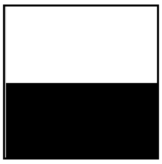


Fig. 3. Basis Image A_{31}. The "1" is interpreted as 255 (White) and "-1" as 0 (Black)

The 2D Hadamard Spectrum of such basis images, which is denoted by C, delivers a matrix where only one coefficient differs from zero. It represents a 2D spectrum of the corresponding basis image. For example, the Hadamard spectrum matrix of the pattern A_{31} is

$$C = H_4 * A_{31} * H_4^T = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad (4)$$

The component C_{31}=16 and all others are zero. This fact, identification of the basis image through its spectral coefficient, can be utilized to construct error-correcting code. The codewords are the pattern of basis images, and they can be decoded unambiguously by detecting the highest absolute coefficient value inside of 2D Hadamard Spectrum according to Eq.(4).

To apply the basic images as codewords, we have to map their two-dimensional structure into one-dimensional pulse stream which will be denoted by the codeword. In Table, 2 such 2D Hadamard codebook is depicted. In case that the basis image A_{31} is corrupted by some perturbation and looks like it depicted in Figure 4.

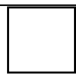
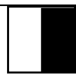
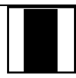
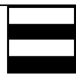
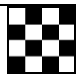
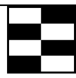
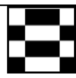
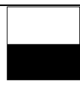
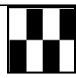
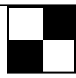
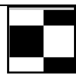
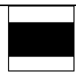
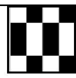
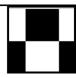
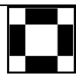
Message	Basis Image	Maximal Matrix Element	Pulse Stream (code word)
0000		C_{11}	0000000000000000
0001		C_{12}	0101010101010101
0010		C_{13}	0000000011111111
0011		C_{14}	0000111111110000
0100		C_{21}	0000111100001111
0101		C_{22}	01011010010111010
0110		C_{23}	0011110000111100
0111		C_{24}	01101001101101001
1000		C_{31}	0011001100110011
1001		C_{32}	0101010110101010
1010		C_{33}	0011001111001100
1011		C_{34}	0011110011000011
1100		C_{41}	0110011001100110
1101		C_{42}	0101101010100101
1110		C_{43}	0110011010011001
1111		C_{44}	0110100110010110

Table 2 : 2D Code Book constructed from Basic Images

It is still possible to recover the original pattern completely. To understand this, let us consider this corrupted Basic Image:

$$\tilde{A}_{31} = \begin{pmatrix} -1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & -1 \end{pmatrix} \qquad (5)$$

The Hadamard Spectrum we obtain from

$$C = H * \tilde{A}_{31} * H^{-T} = \begin{pmatrix} -2 & 2 & -2 & 2 \\ -6 & -2 & -6 & -2 \\ 10 & -2 & -6 & -2 \\ -2 & 2 & -2 & 2 \end{pmatrix}$$

the absolute value of $|C_{31}|=10$ and it still stays the highest one between the other spectral coefficients of matrix C, hence the corresponding message word could be read out from the code book depicted in Table 2. It is "1000" (see the row for coefficient C_{31}).

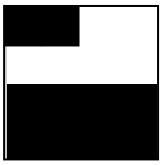


Fig. 4. Corrupted Basic Image A_{31}

The total number of errors that can be corrected is $n/4$-1 and correspond completely to the one-dimensional case. The simple enlargement from 1D to 2D doesn't bring any improvement. To overcome this limit, a new enhance Hadamard decoding procedure for 2D and 3D Hadamard Code is introduced.

2.3 Enhanced 2D Hadamard Error Correcting Code

The enhanced 2D Hadamard Code makes it possible to correct more errors as with the standard Hadamard method. With this approach is possible to overcome the theoretical limit of error correcting capability of $\left\lfloor \frac{n^2}{4} - 1 \right\rfloor$ errors.

The basic idea is to map the 2D basis images into a collection of one-dimensional rows and applying them 1D decoding procedure. After this, the image is reassembled, and the 2D decoding procedure (Eq.(4)) can be applied more efficiently.

To show the functionality of this method we consider the basis images A_{71} of 8x8 2D Hadamard Transform. In this case is n=8. This basic image (Fig.5) can be derived from Eq.(3).

$$A_{71} = H_8(:,1) \cdot H_8(7,:) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

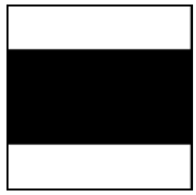


Fig. 5. Basic Image A_{71} of 2D Hadamard Transform (8x8) and its visualization. "1" is interpreted as white (255), "-1" as black (0)

This image is now corrupted by noise (Fig.6). The corresponding error matrix contains 17 errors. According to the consideration from chapter 2.1, it is not possible to recover this pattern because the number of errors exceeds the limit of $\left\lfloor \frac{n^2}{4} - 1 \right\rfloor = 15$

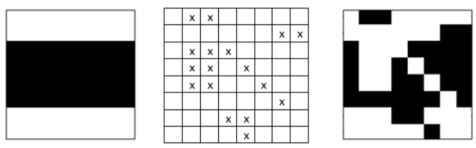
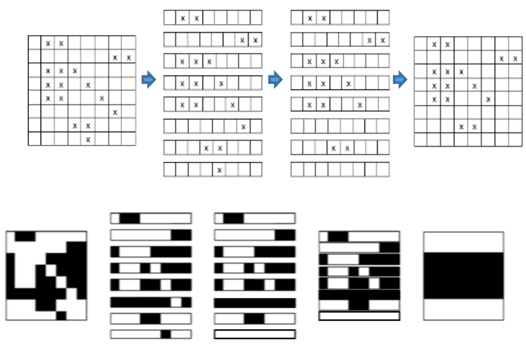


Fig. 6. Original Basis Pattern A_{71}, Error Mask, and the Corrupted Pattern

The main idea of the enhanced Hadamard Error Correcting Code is to reduce the total number of errors beyond the limit by applying at first one-



A B C D E

Fig. 7. Enhanced Hadamard Decoding Procedure on Error Mask and on Corrupted Basis Image

dimensional error correcting code for each row of the 2D Pattern.The functionality of the enhanced Hadamard decoding procedure is depicted in Figure 7. The steps of the algorithm could be described as follows:

- The corrupted basis image (A) is separated into its rows (B).
- On each row is applied 1D Hadamard decoding procedure. Rows which contain only one error are decoded error free (because of each row has the length of n=8). Rows No. 6 and No. 8 are now without any errors (C).
- Reassemble the pattern again (D). The renewed pattern contains now fewer errors as before, namely 15.
- Apply the 2D Hadamard decoding procedure according to Eq.(4). The result will be error free pattern (E).

We simulated the error correcting performances of the enhanced and standard Hadamard Error Correcting Codes with the codewords of the length n=64. The results are depicted in Fig. 8. On the x-axis, we have the number of bit errors, on the y-axis the number of corrected codewords in percentage. The enhanced Hadamard Code is depicted with a continuous line and standard Hadamard with dashed line. As described in chapter 2.1 the standard Hadamard Error Correcting Code has the following features: It can correct 100% of all corrupted codewords of the length n if the number of error bits occurring in the range [1,.., n/4-1] to [3n/4+1,…,n]. In case n=64 we can see, that standard Hadamard Code corrects all errors if their number is between 1 and 15 and between 49 and 64. In the case of Enhanced Hadamard Correcting Code, we can correct beyond these limits

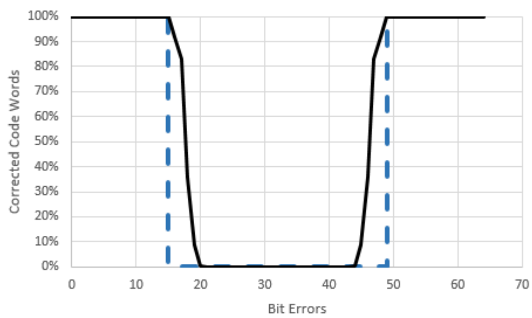


Fig. 8. Comparison of Error Correcting Capabilities of Standard Hadamard (dashed line) with 8x8 2D Enhanced Hadamard Code

For example, in the case of 16 errors, we correct 92% of all possible error pattern inside the codeword. In the case of 17 errors, it is still 83% of all error pattern that can be corrected. If we have 48 errors, in the case of Standard Hadamard Code no errors could be corrected on the contrary to the Enhanced Hadamard Code. It can correct 92% of all error pattern.

3 Enhanced 3D Hadamard Error Correcting Code

The performance of Enhanced Hadamard Code can be improved by diluting it to three dimensions. Instead of using basic images, we can use basic cubes for generating a code book.

3.1 3D Hadamard Transform

We consider the representation of an Hadamard Matrix of order n as

$$H_n = [\upsilon_1(n), \upsilon_2(n), \ldots, \upsilon_n(n)] \tag{7}$$

where $\upsilon_k(n)$ is the column vector with the order n of the Matrix and $1 \le k \le n$.

The n order 3D Hadamard Transform of the 3D Signal $C_n(x,y,z)$ is defined as

$$S_n(k_1, k_2, k_3) = \sum_{i=1}^{n} B_n(k_1, k_{2,} i) \cdot \upsilon_{k_3}(i) \tag{8}$$

where

$$B_n(:,:,i) = H_n \cdot C_n(:,:,i) \cdot H_n^T \tag{9}$$

is the 2D Hadamard Transform of the 2D Signal Matrix $C_n(:,:,i)$ where $1 \le i \le n$

3.2 3D Hadamard Cubes and the Encoding Procedure

Hadamard cube is a basis image expanded in the third dimension by multiplying the pattern with Hadamard vectors.

$$D_{mlk} = A_{ml} \cdot \upsilon_k \tag{10}$$

where the basis image is represented by A_{ml} and υ_k is the k Hadamard vector of the order n. For example the pattern A_{41}

$$A_{41} = \begin{pmatrix} 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

and the Hadamard vector $\upsilon_2 = \begin{bmatrix} 1 & -1 & 1 & -1 \end{bmatrix}^T$ generates the cube D_{412}

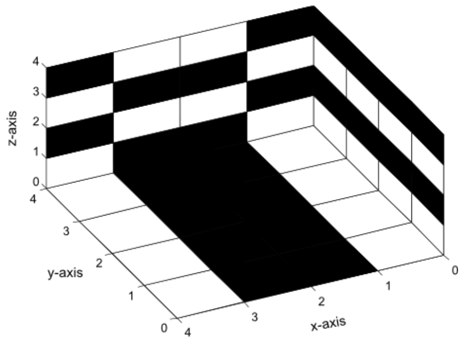


Fig. 9. Hadamard Cube D_{412}

The Encoding Procedure itself is similar to the encoding procedure in 2D case.(see Chapter 2.2.). All cubes are numbered all the way through and each is assigned to the message word. By using a mapping procedure we convert every cube into a one-dimensional pulse stream, which represents the code codeword. A Code Book looks similar as in 2D case (see Table 2) instead of n^2 code words we have in 3D case n^3.

The decoding procedure and the corresponding error correction work similar to the procedure described in Chapter 2.3. After the codeword is mapped back from pulse stream to the 3D cube, the Eq(7) can be applied and generate the 3D spectrum.

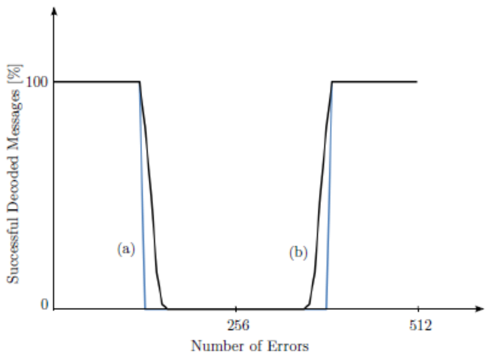


Fig. 10. Comparison of Error Correcting Capabilities of Stanard Hadamard (a) with 3D Enhanced Hadamard Code (b).

The coordinate of the biggest absolute value of the spectrum defines the corresponding message word. Before it can be applied the cube is resolved from the front side in separate layers. On each layer, the enhanced 2D Hadamard decoding procedure is applied. The Performance of the 3D Hadamard Code was simulated and compared with the Standandard Hadamard Code of the length n=512.The Cubes have the dimension 8*8*8. The results are depicted in Figure 10.

3.3 Fast Decoding Procedure for 3D Hadamard Cubes

The speed for the decoding procedure of Hadamard cubes can be increased significantly by utilizing some characteristics of Hadamard Matrices.

The Hadamard Cube can be considered as Hadamard Pattern (basis Image) expanded in the third dimension. It can be thought of as n- pattern concatenated in the z-aches. These patterns are Hadamard basis images only multiplied by 1 or -1, depending on the vector $\upsilon_k(n)$ of the Hadamard Matrix H_n. We have the total number of n^2 basis images and each of them can be multiplied by n column vectors of an Hadamard Matrix H_n, so we have a total number of n^3 cubes.

We can conclude , that the pattern of the front side of the cube and the Hadamard vector $\upsilon_k(n)$ define unambiguously the cube.

In order to relate any number j, $1 \leq j \leq n^3$, to the distinct cube the basis pattern number P_b and column Hadamard number k, which define the cube, have to be determined as follows:

$$P_b = \left\lceil \frac{j}{n} \right\rceil$$
$$k = \begin{cases} j \bmod n \\ n & j \bmod n = 0 \end{cases} \tag{11}$$

The cube number C_b can now be assigned as follow:

$$C_b = (P_b - 1) \cdot n + k \tag{12}$$

The decoding procedure consists of determining the front and top pattern of the cube. The front pattern is Hadamard pattern enclosed by x- and y axes. The top pattern is Hadamard pattern enclosed by x and z-axis.

As a vector in a Hadamard matrix always starts with a leading 1, a cube's front pattern is always the base pattern which was used to generate the cube. In Figure 11 are these pattern depicted and numbered. The Hadamard Cube D_{412} (Fig.9) has the front pattern number P_b= 4 and the top pattern number P_t=8. From the top pattern number is possible to calculate the number k

$$k = \begin{cases} P_t \bmod n & 1 \le P_t < n \\ n & P_t \bmod n = 0 \end{cases} \qquad (13)$$

The related cube number now can be calculated according the Eq(12). If the top pattern is corrupted and it identification is not possible, then the column number k can be defined by a side pattern, which is determined by z-and y axis. In this case the number k is calculated

$$k = \left\lceil \frac{P_s}{n} \right\rceil \qquad (14)$$

Where P_s the side patter nmuber.

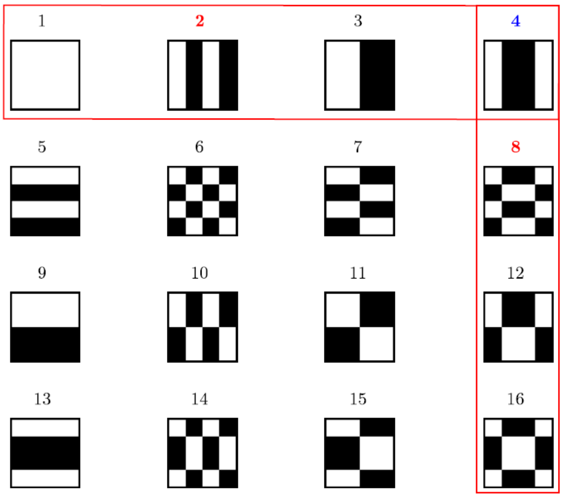


Fig.11 Base Pattern and their Number

In case the front pattem cannotbe determined, the top pattern together with the side pattern uniquely identify the original (front) pattern. To illustrate this, the cube from Figure 9 is considered. The rows of the top pattern are based on the highest row of the front pattern, only varying in signedness. As stated earlier, the number of sign changes describes the column in the matrix of the Hadamard pattems set, where the base pattern is originated. As the side pattern is based on the far right column of the original pattern, the row in the matrix of the set is specified. Therefore, the front pattem can be defined by interpreting the top pattern and side pattern as column and row, respectively, in the matrix of the Hadamard patterns set. For the example of cube D_{412} the top pattem number is 8, therefore the cube column where pattern 8 is located also includes the front pattern. The side pattern number 2 then identifies the front pattem as it specifies the row inside the column.

After identification of the front pattem, the cube number can then be calculated with Eq.(12). Depending on the pattem quality of the front top and side pattem, Eq. (13) or rather Eq.(14) is used to calculate k.

As a result, it can be seen that three sources of information are available, but only two of them are necessary to rebuild the cube.

4 Application of Enhanced Hadamard Code in Watermarking Technology

Digital Watermarking is a very prospective new technology, that offers a huge number of new applications [8]. Especially the challenge to protect intellectual properties of multimedia data against illegal usage or tempering can be solved by watermarking technologies [9]. One of the important components is an error correcting code. Especially when watermarked video sequences undergo a very hard compression the error correcting code used in the watermarking scheme plays a decisive role in surviving of watermarks[10]. For this reasons, we choose these techniques to demonstrate the efficiency of Enhanced Hadamard Error Correcting Code (EHC). To underline the performance of EHC, it was compared with the well known Reed-Solomon Code [11,12] used in the same watermarking scheme.

4.1 Proposed Watermarking Scheme

The proposed watermarking scheme works in the spectral domain and uses an Interframe Discrete Wavelet Transform (DWT) [13] of video sequences and an Intraframe Discrete Cosine Transform (DCT) for embedding procedure [14,15]. In the Fig. 12, the whole encoding process is illustrated. The raw format of the luminance channel of the original video stream is decomposed by multi-level Interframe DWT with Haar Wavelet. This low pass filtered part of the video stream undergoes a block-wise DCT Transform. From DCT spectrum, special coefficients are selected and used for embedding procedure with 2D Hadamard coded watermarks. The embedding procedure itself is realized through QIM (Quadrature Index Modulation) techniques [16].

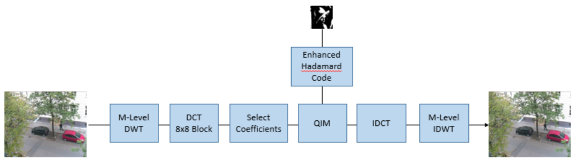


Fig. 12. Watermarking Encoding Process

The decoder procedure is depicted in Fig.12. At the beginning of the decoding procedure, the embedded video sequence undergoes the same multi-level Inter-frame DWT and Intraframe DCT transforms as on the encoder side.

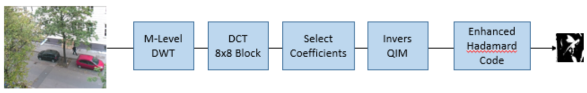


Fig. 13. Watermarking Decoding Process

After the selection of the proper DCT coefficients, the inverse QIM (IQIM) is applied. It delivers the decoded code words (pulse stream). Through the help of Enhanced Hadamard Error Correcting Code, the original watermark is extracted.

4.1.1 Multi-Level DWT
As mentioned above a multi-Level Interframe DWT with Haar Wavelet was used to deliver a low pass filtered video. The Fig.14 illustrates the operating principle of this transform.

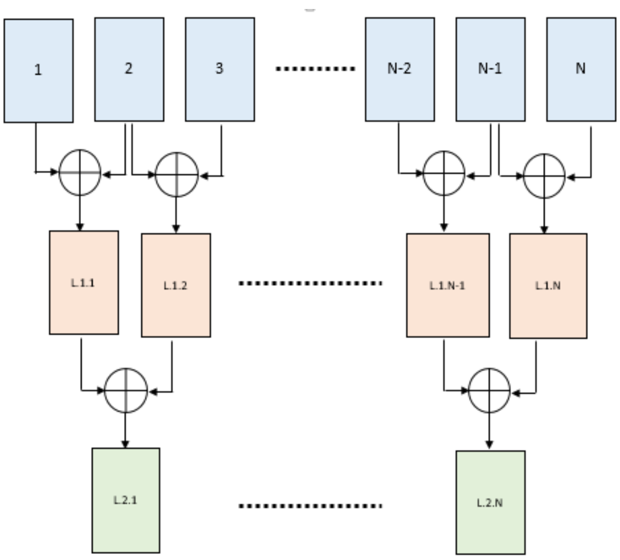


Fig. 14. Multi-Level Interframe DWT

In the first level, the two consecutive frames are averaged. In the second level, the frames from level one are averaged and so forth. In this watermarking schemes, we used DWT levels from12 till 16.

4.1.2 Selection of Embedded Coefficients
To realize the embedding procedure, some coefficients from the DCT spectrum of DWT filtered video sequence must be selected. The Fig.15 shows which coefficients are qualified for watermarking. These are mostly from the yellow area.

1	9	17	25	33	41	49	57
2	10	18	26	34	42	50	58
3	11	19	27	35	43	51	59
4	12	20	28	36	44	52	60
5	13	21	29	37	45	53	61
6	14	22	30	38	46	54	62
7	15	23	31	39	47	55	63
8	16	24	32	40	48	56	64

Fig. 15. Coefficients of DCT Spectrum which fits for embedding

4.1.3 Quadrature Index modulation (QIM)
To embed the watermark bits into selected coefficiants, the so called Quadrature Index Modulation Method was seleceted. It is a method for information hiding which means binary digits (i.e., 0 and 1) can beembedded in any number rational number n.

Different from other embedding routines, tltis approach not only changes the value of a. certain number, but takes its actual value into account. This leads to a.more robust embedding procedure and to a higher video quality.

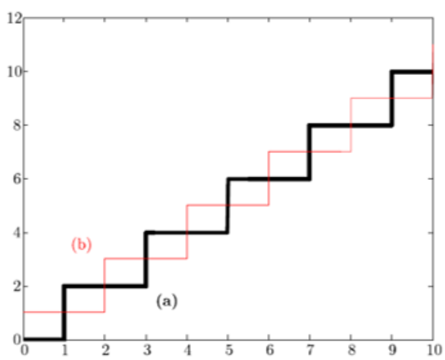


Fig. 16. (a)- 1 function (b) 0-function for quantizing data

Basically, QIM consists of two step functions: one function represents the 0-function and the other represents the 1-function [16]. Figure 16 shows the example for Δ=1.
It can simply be said that on the x-axis the values are located before embedding and on the y-axis the resulting values are located after the embedding. Depending on whether 0 or 1 is to be encoded, the data holding the DCT coeflicients are quantized using the function f_1 or f_0 defined in equation 15.

$$f_1 = 2\Delta\left\lfloor \frac{x+\Delta}{2\Delta} \right\rfloor$$

$$f_o = \left(2\left\lfloor \frac{x}{2\Delta}+1 \right\rfloor -1\right)\cdot\Delta \tag{15}$$

An important factor is the quantization width Δ, which determines the actual embedded values. This parameter influences the overall video quality the most, as it directly introduces noise to data.
For decoding embedded data., y-values of both functions have to be calculated for a. specific value, read from the specified DCT coeflicient. The smallest distance between the value and the calculated y-values of the both functions determine whether 0 or 1 would be enco-ded.

4.2 Investigation with 3D Enhanced Hadamard Error Correcting Code

The investigation was done with HDTV video sequence with the resolution of 1080x1920 and 25fps. The video was captured with an AVCHD Camera. The watermarking processing was performed only for the luminance channel (after converting RGB into YCrCb color space) because it is more robust against distortions than any other channels. It was investigated how many embedded watermark bits survive compression attacks without causing significant impairments. The degradation of the watermarked output video was measured with SSIM (Structural Similarity) index. SSIM is based on the human eye perception and so the expressiveness about distortion is better than in the traditional methods like PSNR (Peak Signal to Noise Ratio) or MSE (Mean Square Error) [17].
It was chosen the Enhanced 3D Hadamard Code of the size of 8x8x8, which means the code word length of 512 bits. This implies the message code length of 8 bit (log2(n) messages). The DCT block size was 8x8 and from each block were selected 16 coefficients. With these, information is easy to calculate the total number of embedded watermark bits for each frame.

$$E = \frac{H\cdot W}{B^2}\cdot\frac{M}{W}\cdot C = \frac{1920\cdot 1080}{8^2}\cdot\frac{9}{512}\cdot 16 = 9112\,\text{Bit/Frame}$$

Where H is, the height and W is the width of the frame. The letter B denotes the block size of DCT transform; the letter M is the message code length; the letter W represents the code word length of the 3D Hadamard Code and the letter C is the number of selected spectral coefficients.
In Table 2, the results of capacity and robustness measurements are presented. The compression attacks were done by H.264 codec with different compression ratios. Because the method works in the raw video, the original data rate is 1.2 Gbit/s. As a watermark was used a chessboard pattern of the size of 30x30 Pixel.
The watermarks were inserted successively into the frames. The Delta QIM gave the width of the quantization steps and was tuned to value 11. Generally, the Delta value determines the noise distortion in the host video.
The embedded video sequence was compressed with different compression ratios. In the case of compression to 5 Mbit/s, which correspond to a compression ratio of 1:240 it is still possible to extract all watermarks error free. The quality comparison between originally compressed video and embedded and compressed shows, that there is only slightly difference. The SSIM index Video is in this case 98%.

Data Rate	Compression Ratio	DWT Levels	Delta QIM	Selected Coefficients	Embedded Bits	Extracted Watermark	SSIM Watermarking	SSIM Video
6 Mbit/s	1:200	16	11	9	9112		1	0,95
5 Mbit/s	1:240	16	11	9	9112		1	0,95
4 Mbit/s	1:300	16	11	9	9112		0,92	0,93
3 Mbit/s	1:400	16	11	9	9112		0,89	0,91
2 Mbit/s	1:600	16	11	9	9112		0,56	0,90

Table 2. Results for 3D Enhanced Hadamard Code

4.3 Comparison of 3D Enhanced Hadamard with Reed-Solomon Code

In order to show the performance of Enhanced Hadamard Code, a comparison between EHC and well known Reed-Solomon Code was carried out. Reed-Solomon Code is well known as an error correcting code and it has a plenty of practical implementations for example in consumer electronics like CD, DVD, Blu-Rays, QR-Code or in data transmission.

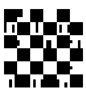
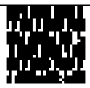
Data Rate	EHC	Err. %	Reed-Salomon	Error %
5 Mbit/s		0		17,5
4 Mbit/s		1,7		27,6
3 Mbit/s		6,8		35,3
2 Mbit/s		41,2		40,8

Table 3. Comparison of Enhanced Hadamard with Reed-Salomon Code

To make the Reed-Solomon Code comparable to Enhanced Hadamard Code we have to select two parameters: the length of the symbol and the redundancy. The symbol length (block length) is equal to the message of 9 bit. The 3D Enhanced Hadamard Code has a codebook, where to every message of 9 bit a cube is assigned with codeword length of 512 bits. The Reed-Solomon Code has a codebook, where for each message of 9 bit a string of 4599 bits (512 Symbols, each symbol is 9 bit long) is assigned. The redundancy of Reed-Solomon Code was selected in such a way, that the number of correctable symbols should approximately correspond to the number of correctable bits of Hadamard Code, which is n/2. So we get an RS Code of [511, 255] with a codeword length of n=511 symbols and the message of k=255 symbols, where a symbol is 9 bit long.
The comparison of the performance of both codes is documented in Table 3. At the data rate of 5Mbit/s, which correspond to the compression ratio of 1:240, the EHC Code can still recover the whole watermark without errors. In contrary the RS Code shows a recovered watermark with 17% errors. At the data rate of 3Mbit/s, the performance advantage of EHC is even more visible. EHC Watermark has an error of 1,7%. In contrary the RS Watermark is barely visible and has an error of 27,6%. In all these considerations we should take into account, that concerning the capacity EHC code is superior against RS code because the EHC codeword length is much shorter (512 bits) than an RS codeword (4599 bits).

5 Conclusion

In this paper a new type of multidimensional Hadamard Error Correcting Code, we called it Enhanced Hadamard Error Correcting Code (EHC) was introduced. It has remarkable property, it can overcome the limit of n/2-1 correctable bit errors of a standard Hadamard Code, where the codeword length and the Hamming distance d have the same value n. The application of this Code in Video Watermarking gives also a strong prove of its effectiveness.
Compared to Reed-Solomon Code the Enhanced Hadamard Code is much more effective. The watermarks of a video, protected by EHC, can survive a very strong compression attack, in opposite to RS-Code.
EHC protected watermarks can be easily recovered error-free from a video with a compression ratio of 1:240, which corresponds to a data rate of 5 Mbit/s.
If the same embedding process is using RS Code instead of EHC the error free recovery of the watermarks is not possible. It has an error of about 17,5% and the content of a watermark can barely be recognized.
All these results are very promising, and they show that the new Enhanced Hadamard Code is very powerful and can be successfully used in video watermarking.

Performed research was supported by National Science Centre, Poland, Amis project number 2015/16/Z/ST7/00559.

References

[1] PLOTKIN, M.: *Binary Code with specified minimum distance, IRE Transactions, IT-6:445-450, 1960*

[2] BOSE, R.C., SHRIKHANDE, S.S.: *A note on the result in the theory of code construction. Inf. And Control 2, 183-194 (1965)*

[3] PETERSON, W.W.: Error correcting codes. The M.I.T. Press, Massachusetts Institute of Technology & J.Wiley & Sons, New York 1961
[4] LEVENSHTEIN, V.I.: Application of Hadamard matrices to a problem in coding. *Problems of Cybernatics, 5*, 166-184, 1964
[5] Combinatoric in Space, The Mariner 9 Telemetry System, http://www.math.cuden.edu/~wcherowi/courses/m6409/mariner9talk.pdf
[6] HORADAM, K.J.: Hadamard Matrices and their Applications. *Published by Princeton University Press*, ISBN-13:978-0-691-11921-2
[7] AGAIAN S.,SARKHANYAN H, EGIAZARIAN K., ASTOLA J. : Hadamard Transforms, *Published by SPIE*, ISBN: 978-0-8194-8647-9

[8] SWANSON, M.D., K. M. T. A.: Multimedia Data-Embedding and Watermarking Technologies. In: *Proceeding of IEEE* 86 (1998), S. 1064-1087
[9] LIN, S. D., S. C.-F.: A Robust DCT-Based Watermarking for Copyright Protection. In: *IEEE Transactions on Consumer Electronics* 46 (2000), S. 415
[10] SWANSON, M.D., K. M. T. A.: Multimedia Data-Embedding and Watermarking Technologies. In: *Proceeding of IEEE* 86 (1998), S. 1064-1087
[11] SHU LIN, DANIEL J.COSTELLO, JR.: Error Control Coding, *Prentice-Hall, Inc. Englewood Cliffs, New Jersey 07632* (1983)
[12] MACWILLIAMS, F.J., Sloane, N.J.A.: The theory of error-correcting codes. *North Holland, New York, 1977*
[13] PIK-WAH CHAN, M. R. L.: A DWT-Based Digital Video Watermarking Scheme with Error Correcting Code. In: *Information and Communications SecurityLecture Notes in Computer Science* 2836 (2003), S. 202-213
[14] ZHAO, D., C. G. L. W.: A Chaos-Based Robust Wavelet-Domain Watermarking Algorithm. In: *Chaos, Solutions and Fractals* 22 (2004), S. 792
[15] I.J.COX, J. KILLIAN, F. L. & VOL.6 PP., T. S.: Secure Spread Spectrum Watermarking for Multimedia. In: *IEEE Transactions on Image Processing* 6 (1997), S. 1673-1687
[16] CHEN, B., W. G., WORNELL: Quantization Index Modulation for Digital Watermarking and Information Embedding of Multimedia. In: *Journal of VLSI Signal Processing* 27 (2001), S. 7-33

[17] HARTUNG, F. & KUTTER, M.: Multimedia Watermarking Techniques. In: *Proceeding of IEEE* 87 (1999), S. 1079-1107
[18] HO ANTONY T.S., SHEN JUN, SOON HIE TAN, KOT ALEX C..: Digital image-in-image watermarking for copyright protection of satellite images using the fast Hadamard transform. In: *Geoscience and Remote Sensing Symposium* 6 (2002), S. 3311 – 3313