A Novel Robust Watermarking Scheme using Cubic Product Codes

Atta Rahman, Neelam Saba, Noor-ul Ain
Barani Institute of Information Technology
Islamabad
Pakistan
ataurahman@biit.edu.pk, neelam@biit.edu.pk, noor@biit.edu.pk

ABSTRACT: *In this paper, a novel technique for robust digital image watermarking is proposed using cubic product codes (CPC). Cubic product codes are three dimensional product codes where the constituent codes in each dimension are linear block codes. The structure of CPC makes them suitable for the proposed scheme. The embedded watermark is vulnerable to various attacks on the image like compression, noise and geometric attacks namely translation rotation and scaling (TRS) etc. This could limit the performance of digital watermarking. Our proposal is to encode the watermark with CPC prior to embedding in the image. This could easily be done because the watermark is also a three dimensional data (image), so each dimension can easily be encoded with corresponding codes in CPC. A modified iterative decoding algorithm (MIDA) is employed to decode the CPC. Moreover, a Fuzzy Rule Based System is used to find the region in the image where watermark can be embedded. The scheme is tested against various attacks and compared with the well-known schemes in the literature for robust digital image watermarking.*

Keywords: Digital Watermarking, CPC, Robustness, linear block codes, MIDA, FRBS

Received: 14 November 2014, Revised 20 December 2014, Accepted 2 January 2015

1. Introduction

Digital watermarking for authentication and copyright protection is one of the interesting areas of research in information security. This technique is used for authentication, copyright protectin, owner identification and copy control etc of a digital document. This technique is no more limited to the images but also applied to the audio, video, softwares and databases.

There are three basic figure of merits in digital watermarking namely, capacity, imperceptability and robustness. Capacity means size of watermark being embedded, imperceptibility means embedding watermark results in slight degradation in the origional image. That degradation must not be noticible. Robustness means after embedding watermark in the image the watermarked image should be resistant to certain attacks on the image.

According to the watermarking terminology, an attack is an event that can cause tampering in the image, thus making the watermark difficult to detect. Mainly attacks can be divided into two categories, incidental and malicious. Incidental attacks are friendly attacks and are required sometimes for example, JPEG compression is used in many of internet applications to make the file size small. Malicious attacks can be divided into four main categories namely, geometrical attacks, removal attacks, protocol attacks and cryptographic attacks as discussed by Gokozan [1].

Product codes are serially concatenated codes and were initially proposed by Elias [2] in 1952. Product codes are two dimentional linear block codes. Later the same concept was extended to three dimensional codes, called Cubic Product Codes (CPC) by [3]. In this concept long codes were generated by using much shorter constituent block codes in each dimension. Construction process of the CPC is presented in a subsequent section.

Robust watermarking schemes allow both incidental and malicious attacks while the fragile watermarking schemes do not allow any modifications. Semi-fragile watermarking schemes are designed which are robust against friendly modifications but are fragile against friendly modifications.

Mostly, retransmission is considered as a solution to this problem but only after the tampering is detected (a case of fragile watermarking). But when the time is stringent then retransmission may be costly (online scenario) also there is no guarantee that after retransmission signal will be received error free and in retransmission throughput is compromised as well.

Similarly use of cryptography for security is always a good choice. But the property that makes a cipher strong, makes it sensitive to the channel error at the same time. Solution is again retransmission but at the cost of throughput [4].

A reliable wireless error correction technique for secure image transmission is proposed in [5], where turbo codes were used for error free communication in contrast to chaos based encryption technique. Real BCH (Bose Choudhary Hoqagan) codes have been investigated for robust image transmission using a joint source-channel coding technique [6]. Error Correcting Codes (ECC) provides error free communication at the cost of redundancy. There are two major types of ECC that is Convolutional Codes (CC) and Linear Block Codes (LBC) [7].

In [8], authors proposed a reversible watermarking technique that improves the security of medical images with additional features to detect the tampering region and then to recover the tampering region of the watermarked image.

A Residue Number System (RNS) based reversible watermarking was proposed in [9]. In this paper authors used RNS to secure the watermark. The proposed scheme was highly fragile against all kind of attacks.

Atta-ur-Rahman et al [10] proposed a novel technique for reriable image transmission using Product Codes. In that technique the image was encoded prior to transmission. Product codes being two dimensional block codes, were observed structurally compatible to the images.

In this paper, cubic product codes (CPC) are proposed for making the watermark robust. A specific sized watermark (image) is encoded by CPC, prior to embedding into the image. The embedding positions (pixels) for the watermark are obtained from a fuzzy rule based system that highlights the positions intuetively. The scheme is varified for natural as well medical images.

Rest of the paper is organized as follows: Section 2 presents the construction of CPC, the fuzzy rule based system is given in Section 3, watermark embedding and extraction is discussed in Section 4, results of the proposed scheme are depicted in section 5 while section 6 concludes the paper.

2. Proposed System Model

Product codes are serially concatenated codes in which short constituent codes are used to construct bigger codes. In cubic block codes (CPC) all three dimensions are encoded by three different linear block codes. In this paper, Bose Chaudhuri Hocquenghem (BCH) codes [11] are considered as constituent codes in the construction of CPCs.

Let there be three BCH codes, namely A_1, A_2 and A_3 with the parameters $[N_1, K_1, D_1]$, and $[N_2, K_2, D_2]$ and $[N_3, K_3, D_3]$ respectively. N_i, K_i and D_i represent codeword length, message length and minimum hamming distance (d_{min}) of the code A_i, respectively and $i = 1, 2, 3$. The code rate of the constituent codes in 3D product codes can be written as:

$$R_i = \frac{K_i}{N_i} \quad i = 1, 2, 3 \qquad (1)$$

The 3D product code can be constructed in the following manner.

1. Place $K_1 \times K_2 \times K_3$ information bits in a cube like structure such that K_1 is height, K_2 as width and K_3 as depth of the cube.

2. Encode $K_1 \times K_3$ rows using code A_2, which will result in $K_1 \times N_2 \times K_3$ sized cube.

3. Encode $N_2 \times K_3$ rows using code A_1, which will result in $N_1 \times N_2 \times K_3$ sized cube.

4. Encode $N_1 \times N_2$ rows using code A_3, which will result in $N_1 \times N_2 \times N_3$ sized cube. This is the final codeword of the cubic product code.

This process is shown in figure 1. The parameters of the resultant cubic product code Ω are given as [N, K, D], where

$$N = N_1 N_2 N_3$$
$$K = K_1 K_2 K_3$$
$$D = D_1 D_2 D_3 \qquad (2)$$

And the resultant code rate of the CPC can be given as;

$$R' = \prod_{i=1}^{3} R_i \qquad (3)$$

Since CPCs possess a high minimum distance compared to their constituent codes, they have a much better error correction capability also. The error correction capability is given as;

$$t = floor \left[\frac{d_{min} - 1}{2}\right] \qquad (4)$$

Cubic product block codes can also be considered as the Cartesian product of its constituent linear block codes. Also in some definitions it is also considered as the intersection of the constituent linear block codes. Hence two different notions are used as given in Equation 7 and Equation 8.

$$X = A_1 \otimes A_2 \otimes A_3 \qquad (5)$$

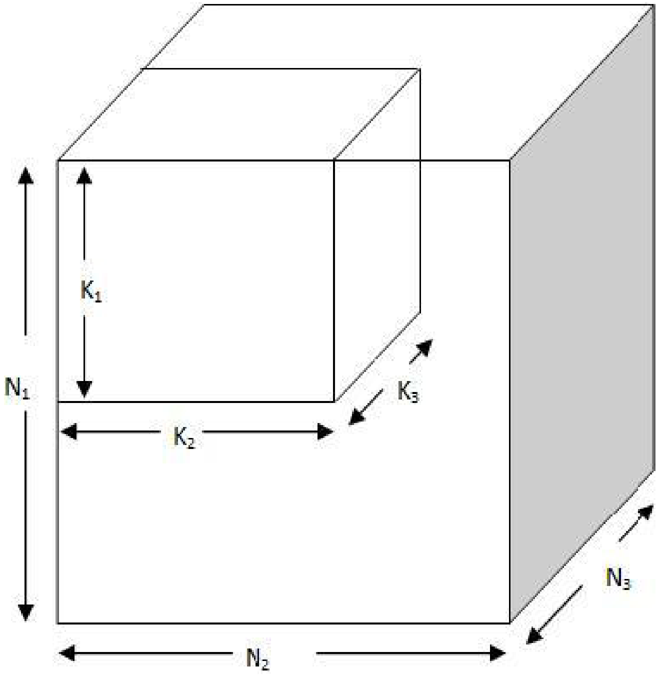


Figure 1. Cubic Product Codes

where ⊗ represents Kronecker product of two codes and X is resultant product code. Also it can be viewed as;

$$X = A_1' \cap A_2' \cap A_3' \qquad (6)$$

Hence this can also be written as the cubic product code is intersection of three codes that are A_i': $i = 1,2,3$, where A_1' is a code represented by all $N_1 \times N_2 \times N_3$ cubic matrices whose each element is a member of code A_1. Similarly A_2' is a code represented by all $N_1 \times N_2 \times N_3$ cubic matrices whose each element is a member of code A_2 and A_3' is a code whose each element of is a member of code A_3.

.

3. Human Visual System (HVS)

Uniform areas of image are very sensitive to the addition of watermark information so, only small amount of information can be added in the uniform areas whereas, the edge areas can support for embedding greater watermark information. The Human visual system (HVS) has been considered with several phenomenon that permits to adjust the pixel values to elude perception [21]. The FRBS has been used here to adapt the HVS different properties. In this scheme, we are considering texture, brightness and edge sensitivity, so that embedding the watermark information in these features makes the image imperceptible.

3.1 Brightness Sensitivity

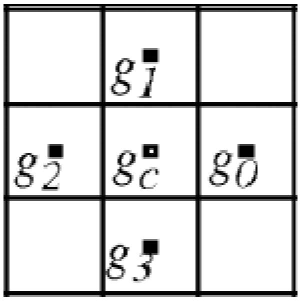
Brighter background areas are less sensitive than dark ones that way our proposed scheme search for pixels with high values of brightness which are chosen for embedding the watermark bit. The most common format of the pixel is the byte image that results in a value from 0 to 255 as the numbers in this range are stored in an 8-bit. The pixel value ‘0’ represents the maximum darkness in the image while the value ‘255’ represents the maximum brightness in the mage whereas, the grey shades represent the values in between.

3.2 Edge Sensitivity

To make the lower visibility of embed signal, higher edges are chosen for embedding the watermark [22]. A gradient analysis has been made to test the model by using different edge detection methods such as sobel, prewitt and canny. In the present scheme, we have used Canny method for calculating edge sensitivity (S_E).

3.3 Texture Sensitivity

The stronger the texture features, the lower is the visibility of the embedded data so, our scheme search for the pixels with the highest texture for embedding the watermark data. Texture sensitivity basically measures the activity of the center pixel with it neighbors as,



	g_1	
g_2	g_c	g_0
	g_3	

$$Activity = |g_c - g_0|^2 + |g_c - g_1|^2 + |g_c - g_2|^2 + |g_c - g_3|^2$$

Ojala et al. [23] proposed a local binary pattern (LBP) operator for calculating texture sensitivity that was based on the postulation that the texture has locally two paired aspects, strength and the pattern. The effectiveness has been proposed to be an operative descriptor in texture classification [24]. In experimental studies, LBP has became the strongest measure for texture analysis which can be comprehended as a uniting methodology to the traditionally different statistical and physical models of texture analysis [25]. The most important property of LBP operator in real world applications is its invariance against monotonic gray level changes”.

LBP is defined as a gray-scale invariant texture measure, resulting from a description of texture in a local neighborhood. A binary value from 0 to 255 is gained by concatenating the values of the neighborhood results in a clock wise direction for each pixel. In this scheme, we have used Local Binary Pattern (LBP) for texture sensitivity calculation. In the present scheme, we have used LBP method for calculating texture sensitivity(S_T).

4. Fuzzy Rule Based System

Here a Fuzzy Rule Based System is used to find those regions in the image where information can be embedded. This decision is based the HVS factors discussed in previous section. FRBS decides that how much data can be embedded in the certain regions of the image with a significant level of imperceptability.

4.1 Design of FRBS

As mentioned earlier, first FRBS has three input variables namely *brightness sensitivity*, *texture sensitivity* and *edge sensitivity* duly defined in previous section. The input range of brightness and edge sensitivity is between 0-255 and edge sensitivity could either be 0 or 1. Five membership functions are used to cover the input space of *brightness sensitivity* (very dark, dark, dim, bright and very bright), two membership functions are used to represent edge sensitivity (low, high) and five membership function for texture sensitivity (very smooth, smooth, average, rough and very rough). These relationships are shown in fig-3, 4 and 5 respectively. There is one output variable named capacity factor (alpha). Five membership functions (very low, low, medium, high and very high) are used to cover the range which is between 0 and 1 as shown in figure 6.

As cardinality of rule base is the product of number of membership functions in each input variables, there are fifty rules in the rule base. As all three features are somewhat in directly proportional to the output, the rules are formulated accordingly. The possible values of variable *edge sensitivity* are 0 or 1, so twenty-five rules are formulated for each case. Rules can be found in table-1 and table-2 for edge sensitivity 1 and 0 respectively. Each table contains twenty-five rules. The first row and first column of each table contains IF part while rest of the table contains according value of THEN part. A rule format can be expressed as;

IF (*Texture* =‘*Average*’ *AND Brightness* = ‘*Dim*’*AND Edge* = ‘1’) *THEN* (*Alpha* = ‘*Medium*’)

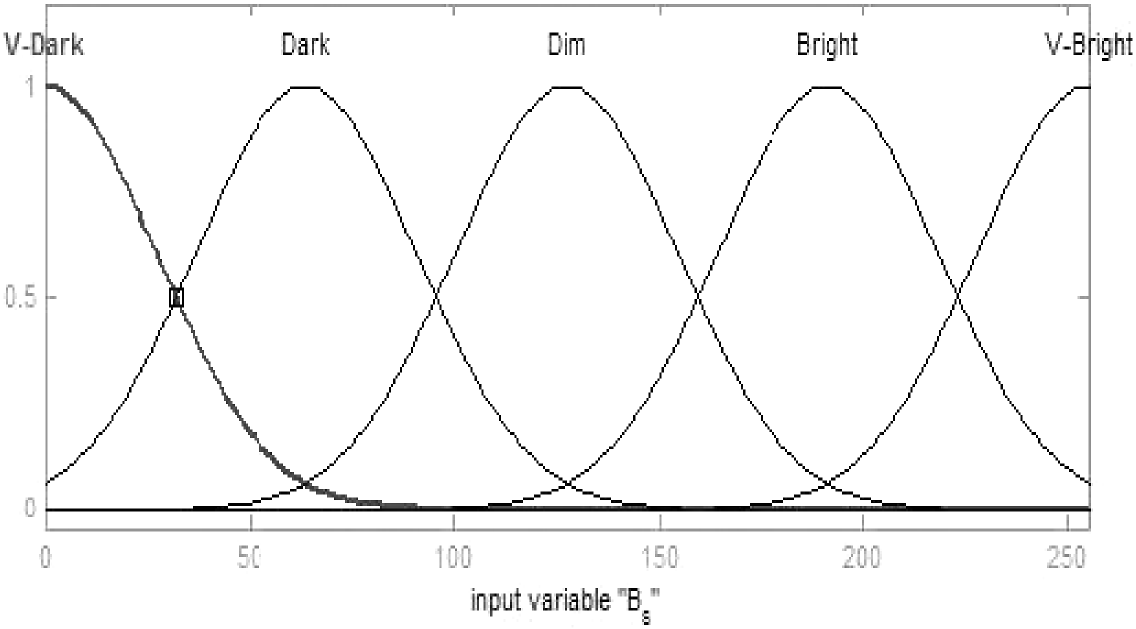


Figure 3. Input variable “Brightness sensitivity (Bs)”

The surface views between texture and brightness for edge-1 and edge-0 are shown in figure 7 and figure 8 respectively. Both of these figures narrate that higher the values of brightness and texture sensitivity, image capacity factor, alpha, is higher. However, this impact is more when edge sensitivity is 1 and less when edge sensitivity is 0, which conforms to the definitions given in previous section.

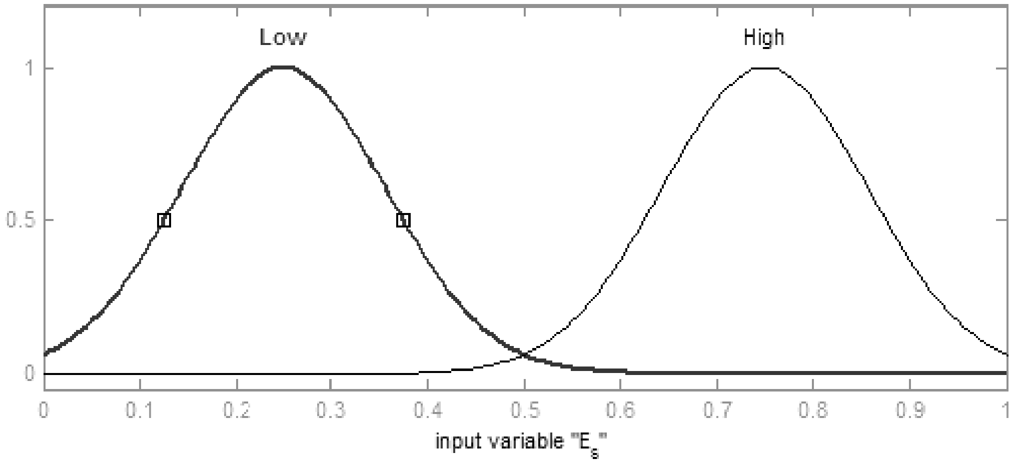


Figure 4. Input variable “Edge sensitivity (Es)”

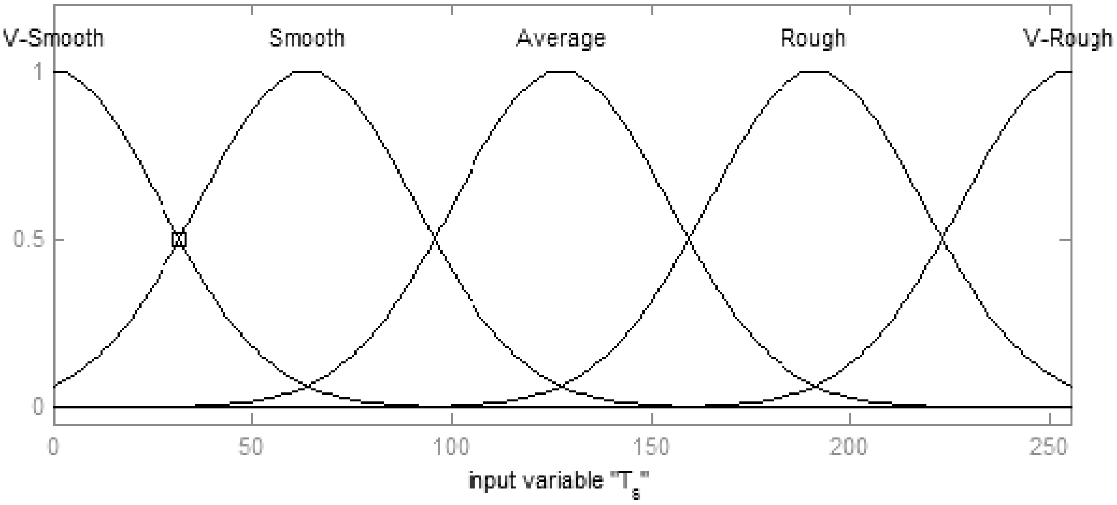


Figure 5. Input variable “Texture sensitivity (Ts)”

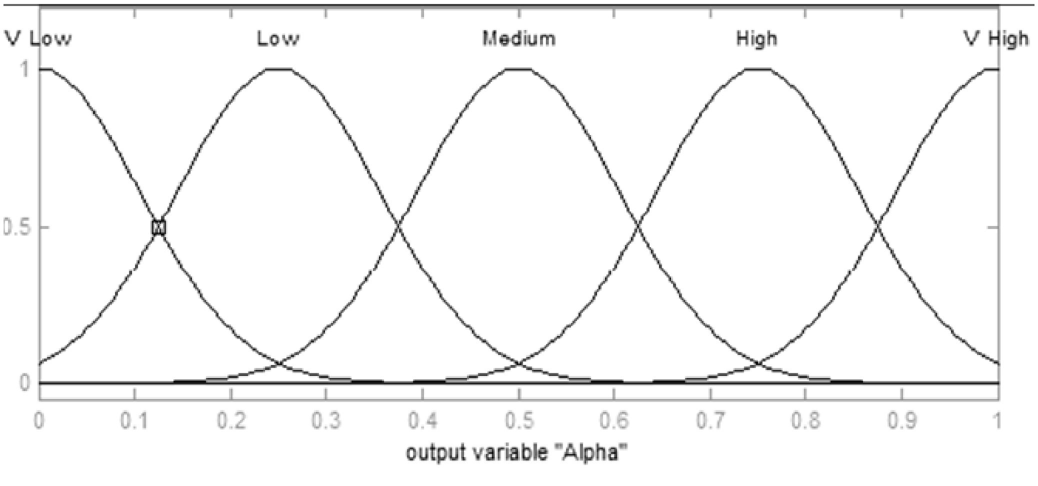


Figure 6. Output variable “Capacity factor (alpha)”

Edge = 1		Brightness				
		V-Low	Low	Dim	High	V-High
Texture	V-Smooth	VL	L	L	M	M
	Smooth	L	L	M	M	H
	Average	L	M	M	H	H
	Rough	M	M	H	H	VH
	V-Rough	M	H	H	VH	VH

Table 1. Rulebase With Edge Sensitivity = 1

Edge = 0		Brightness				
		V-Low	Low	Dim	High	V-High
Texture	V-Smooth	VL	VL	L	L	M
	Smooth	VL	L	L	M	M
	Average	L	L	M	M	H
	Rough	L	M	M	H	H
	V-Rough	M	M	H	H	VH

Table 2. Rulebase With Edge Sensitivity = 0

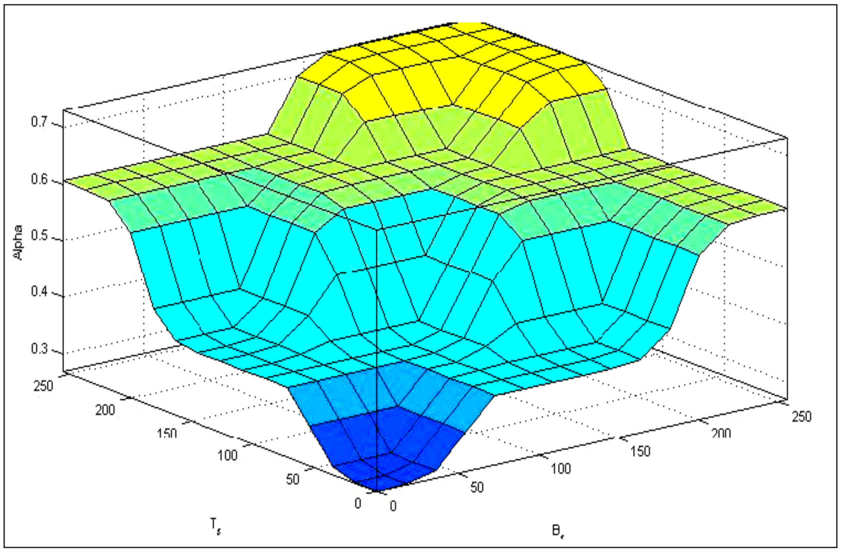


Figure 7. Surface view with edge sensitivity = 1

4.2 Components of Fuzzy Rule Base System

- **Fuzzifier**: Standard Gaussian fuzzifier is used to transform crisp values of input into corresponding fuzzy values.

- **Inference Engine:** Mamdani Inference Engine (MIE) is used for inferring that an input vector is mapped on to which corresponding output point by making use of rules in the rule base. In MIE, fuzzy operation AND is chosen as MIN while OR is chosen as MAX.

- **De-Fuzzifier:** Standard Center Average Defuzzifier (CAD) is used to transform the fuzzy output value into crisp value, due to its effectiveness as well as less computational requirements.

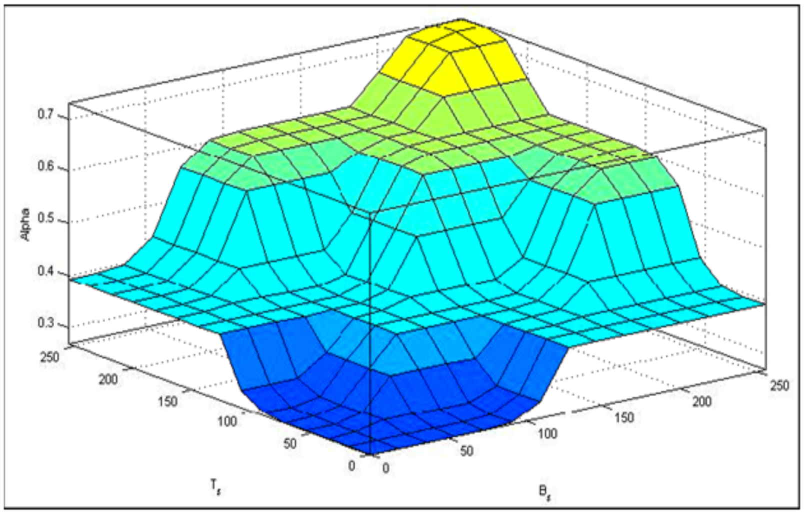


Figure 8. Surface view with edge sensitivity = 0

5. Results

In this section, effectiveness of the CPCs is shown inititally in terms of bit error rate (BER) and their immunity against certain attackes in digital image watermarking. The simulation paramters used in the experiment, are listed in table-1 below.

Sr. #	Parameter	Value
1	Constituent code-1	[16,11,4]
2	Constituent code-2	[31,21,5]
3	Cubic Product Code-1	[16,11,4]3
4	Cubic Product Code-1	[31,21,5]3
5	Decoder	MIDA [3]
6	Attack type-1	AWGN
7	Attack type-2	Salt & Pepper noise
8	Attack type-3	JPEG Compression

Table 1. Simulation Parameters

Two different BCH codes are used for the experiment. First one is [16, 11, 4], in which the minimum distance is 4, that means the error correction capability is 1. The second one is [31, 21, 5] with a minimum distance of 5, that means it is a two bit error correction code. Moreover, same code is used in all three dimensions.

Figure 9 shows the performance of CPC in terms of BER over an Additive White Guassian Noise (AWGN) channel. It is apparant from the figure, that the CPC with [31,21,5] performs better than CPC with [16,11,4]. This is because this code has a greater minimum distance.

Figure 10 shows the origional cover image of Baboon while the watermark image is shown in figure 11. It is a custom designed watermark, just to make it suitable for encoding with the CRC being used.

After encoding the image by the CRC [31,21,5], the watermark is embedded in the regions of the origional image selected by the Fuzzy Rule Based System (FRBS) discussed in the previous section. The watermarked image is shown in figure 12.

The image is then offered a number of attacks and the recovered watermark is shown.

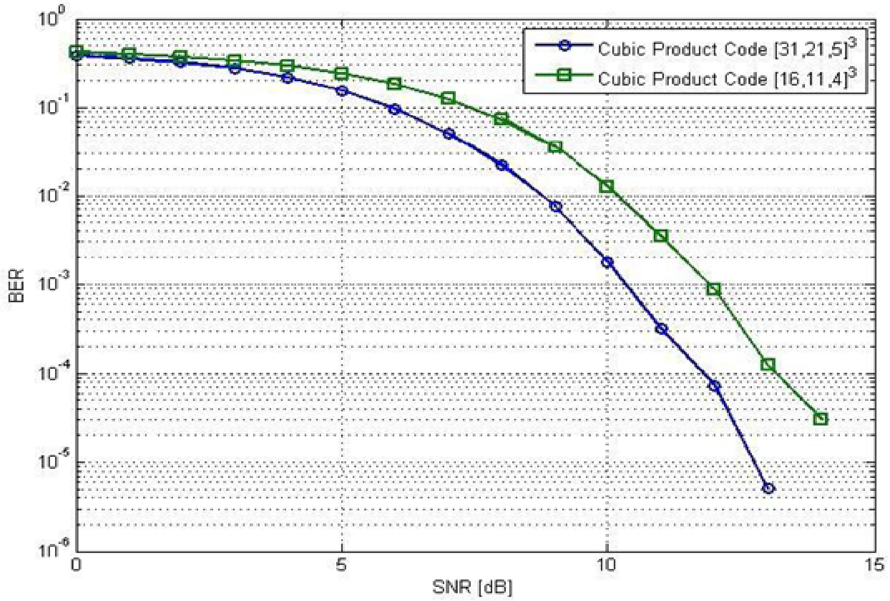


Figure 9. Performance of CPC over AWGN

Figure 10. The cover image

Figure13 shows the recovered watermark after attack speckle noise with variance 0.01 resutling in Nc = 0.873. Here Nc is the similarity index between orgional image and the recovered image. So higher the index, more robust will be the image. Though required value of Nc varies from application to application however, as a common practice, value of Nc higher than 0.7 is considered as a good level of robustness.

Figure 14 shows watermark after attack of gaussian noise with variance 0.01showing Nc = 0.794.
Figure 15 shows the recoverd watermark after attack of Salt & pepper noise with variance 0.01, having Nc = 0.863.
Figure 16 shows the recoverd watermark after rotation attack of 2 degrees, having Nc = 0.851.

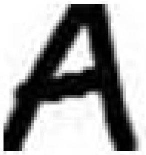


Figure 11. The watermark

Figure 12. The watermarked imaged

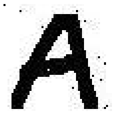


Figure 13. Recoverd watermark after attack of speckle noise with variance 0.01 showing Nc = 0.873

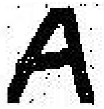


Figure 14. Recoverd watermark after attack of gaussian noise with variance 0.01, having Nc = 0.794

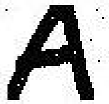


Figure 15. Recoverd watermark after attack of Salt & pepper noise with variance 0.01, having Nc = 0.863

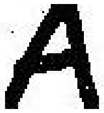


Figure 16. Recoverd watermark after rotation attack of 2 degrees, having Nc = 0.851

6. Conclusions

This paper presents a novel idea of using cubic product codes (CPC) for making the watermark robust in a digital image watermarking scenario. In a number of applications, the watermark is more important as compared to the cover image, so making the watermark robust is the major focus of the field.

A fuzzy rule based systems (FRBS) is proposed to highlight the areas of the cover image (pixels) where the watermark can be inserted with a significant level of imperceptability. Due to their error correcting capabilites, CPCs has shown the notable performance in the resutls shown above and the watermark is become robust against certain attacks.

References

[1] Gokozan, T. (2005). Template Based Image Watermarking in the Fractional Fourier Domain, MSc thesis, Middle East Technical University (METU).

[2] Elias, P. (1954). Error-free coding, *IEEE transactions on Information Theory*, 4, p. 29-37.

[3] Atta-ur-Rahman., Qureshi I.M. (2014). Effectiveness of Modified Iterative Decoding Algorithm for Cubic Product Codes, *In*: proceedings of International Conference on *Hybrid Intelligent Systems* (HIS'14), p. 260-265, December.

[4] Nanjunda, C., Haleem, M., Chandramouli. Robust encryption for secure image transmission over wireless channels.

[5] Mathur, C., Narayan, K., Subbalakshmi, K. (2006). On the design of error-correcting ciphers, EURASIP J*ournal onWireless Communications and Networking*, 2006, p.1-12, November.

[6] El-Iskandarani, M. A., Darwish, S., Abuguba, S. M. Reliable Wireless Error Correction Technique for Secure Image Transmission

[7] Gabay, A., Kieffer, M., Duhamel, P. (2007). Joint Source-Channel Coding Using Real BCH Codes for Robust Image Transmission. *IEEE transactions on Image Processing*. 16 (6), June.

[8] Zain, J. M., Fauzi, A. R. M. (2006). Medical Image Watermarking with Tamper Detection and Recovery, *In: Proceedings of 28th IEEE EMBS Annual International Conference*, p. 3270-3273.

[9] Atta-ur-Rahman., Naseem, M.T., Qureshi, I. M., Muzaffar, M. Z. (2011). Reversible watermarking using Residue Number System. *IEEE 7th International Conference on Information Assurance and Security* (IAS'11), p. 162 - 166, 5-8 December, Melacca, Malaysia.

[10] Atta-ur-rahman., Qureshi, I. M., Naseem M. T. (2013). A Novel Technique for Reliable Image Transmission using Product Codes". *International Journal of Computer Applications* (IJCA) 65 (4), p. 12-17, March.