# A Novel Technique for Reliable Image Transmission using Product Codes

Atta-ur-Rahman
SEAS, ISRA University,
Islamabad Campus
Islamabad, Pakistan

Ijaz Mansoor Qureshi
Air University
PAF Complex
Islamabad, Pakistan

M Tahir Naseem
SEAS, ISRA University,
Islamabad Campus
Islamabad, Pakistan

## ABSTRACT
Reliable image transmission is requirement of many fields of security and privacy nowadays for example, digital watermarking, stenography, encryption etc. Many researchers also consider secure image transmission as a robustness feature of digital watermarking. In this paper, product codes are proposed for secure image transmission due to their structural compatibility with the images. For decoding, a Modified Iterative Decoding Algorithm is used that is a suboptimum low complexity decoder whose easy hardware and software implementation makes it attractive for online applications. Mainly the purpose of this coding scheme is to make the image robust against various kinds of noise attacks during wireless transmission as the product codes have a great capability of correcting random as well as burst errors. Simulation results show the significance of proposed scheme.

## General Terms
Security, Product Codes

## Keywords
Product Codes; Modified Iterative Decoding Algorithm; BER; Digital Watermarking

## 1. INTRODUCTION
Security is one of the most important feature and requirement of almost every kind of data and applications especially when they are to be transmitted over some wireless medium. Such a medium is not in our control and it may cause our signal (text, image, videos) not recognizable at receiver end. Though the effect of most of these channel hostilities (noise, attenuation etc) is more harmful for the text compared to the images and videos but if the images or videos are watermarked then these kinds of noise attacks may cause tampering in the watermark or the original image. Mostly, retransmission is considered as a solution to this problem but only after the tampering is detected (a case of fragile watermarking) [1]. 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. [2]

To improve the throughput in presence of channel hostilities channel codes are mostly used in contrast to encryption techniques. But using both encryption and encoding separately makes the process computationally expensive at receiver end especially for handheld wireless devices (iPhones, Android, Pocket-PCs etc). So using a technique that provides security as well as robustness always a good choice [3].

A reliable wireless error correction technique for secure image transmission is proposed in [4], 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 [5]. 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) [6].

Orthogonal Frequency Division Multiplexing (OFDM) is one of the successful candidates for many 3rd and 4th Generation Systems In this technique a single very high data stream is divided into several low data rate streams. Then these streams are modulated over different orthogonal subcarriers. Inverse Fast Fourier Transform (IFFT) and Cyclic Prefix (CP) make it possible to make the subcarrier orthogonal. Since OFDM is the key to many modern communication systems so we found it an appropriate choice for analysis of our algorithm.

Rest of the paper is organized as follows. System model is given in section 2; section 3 contains a brief introduction of Product Codes and their decoding; image coding and transmission is given in section 4; section 5 contains simulation results of proposed scheme, while section 6 concludes the paper.

## 2. SYSTEM MODEL
The system model considered is OFDM equivalent baseband model with N number of subcarriers. It is assumed that complete channel state information (CSI) is known at both transmitter and receiver. The frequency domain representation of system is given by

$$r_k = h_k . \sqrt{p_k} . x_k + z_k ; \ \mathrm{k} = 1, 2, ....., N \qquad (1)$$

where $r_k$, $h_k$, $\sqrt{p_k}$, $x_k$ and $z_k$ denote received signal, channel coefficient, transmit amplitude, transmit symbol and the Gaussian noise of subcarrier $k = 1, 2, ....., N$, respectively. The system model is shown in figure 1.

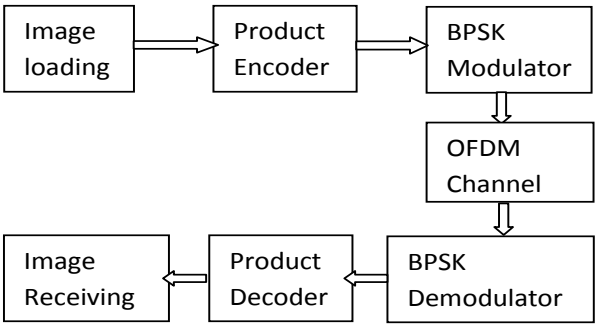


**Fig 1: Block diagram of system model**

# 3. PRODUCT CODES AND MODIFIED ITERATIVE DECODING ALGORITHM

## 3.1 Product Codes

Product codes are serially concatenated codes. Product codes were first presented by Elias in 1954 [7]. The concept of Product codes is quite simple as well as powerful, where much shorter constituent block codes are used instead of one long block code. Basically these are matrix codes where rows are encoded by one block code while columns are encoded by another block code. This arrangement enhances their error correction capability since errors are corrected row-wise as well as column-wise. Also these codes are burst error correcting codes since a row-wise burst can easily be corrected column-wise and vice versa. Since burst error in rows will become single error for column code and vice versa.

Consider two linear block codes $\mathbf{A}_1$ and $\mathbf{A}_2$ with parameters $[n_1,k_1,d_1]$ and $[n_2,k_2,d_2]$ respectively, where $n_i, k_i$ and $d_i; i=1,2$ are the length, dimension and minimum Hamming distance $d_{\min}$ of the code $\mathbf{A}_i (i=1,2)$ respectively. Code $\mathbf{A}_1$ will be used as row code while $\mathbf{A}_2$ will be used as column code. The rates of individual codes are $R_1$ and $R_2$ respectively given by,

$$R_i = \frac{k_i}{n_i}, i=1,2 \qquad (2)$$

The product code $\mathbf{\Omega}$ can be obtained by codes $\mathbf{A}_i, i=1,2$ in the following manner.

- Place $k_1 \times k_2$ information bits in an array of $k_2$ rows and $k_1$ columns
- Encode $k_2$ rows using code $\mathbf{A}_1$, which will result in an array of $k_2 \times n_1$
- Now encode $n_1$ columns using code $\mathbf{A}_2$, which will result in $n_2 \times n_1$ product code

The resultant product code $\mathbf{\Omega}$ has the parameters $[n_1n_2, k_1k_2, d_1d_2]$ and the rate will be $R_1R_2$. In this way long block codes can be constructed using much shorter constituent block codes. This concept can also be viewed as that product code Ω is intersection of two codes $\mathbf{A}_1'$ and $\mathbf{A}_2'$. Where $\mathbf{A}_1'$ is a code represented by all $n_2 \times n_1$ matrices whose each row is a member of code $\mathbf{A}_1$, similarly $\mathbf{A}_2'$ is a code represented by all $n_2 \times n_1$ matrices who's each column is a member of code $\mathbf{A}_2$. This can be written as;

$$\mathbf{\Omega} = \mathbf{A}_1' \cap \mathbf{A}_2' \qquad (3)$$

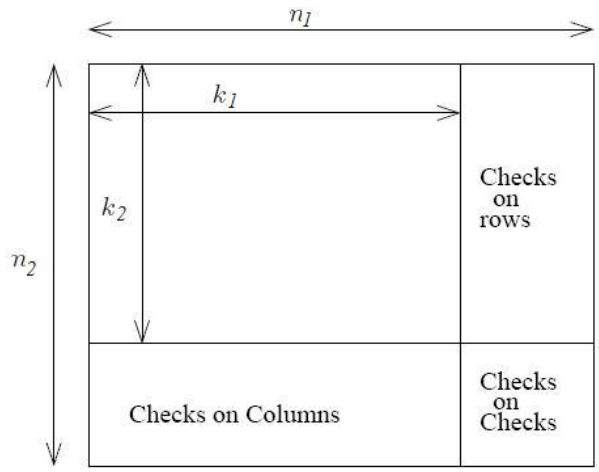


**Fig 2: Structure of the Product code**

## 3.2 Modified Iterative Decoding Algorithm

Iterative decoding algorithm (IDA) for product codes was originally presented by [8] in his Doctoral thesis that is based upon List Decoding also designated as Maximum Likelihood (ML) decoding of product codes. ML decoding is an optimum decoding with an exponential complexity. The iterative decoder was proposed to reduce the complexity of ML decoding, but yet it exhibits a huge complexity. Modified Iterative Decoding Algorithm (MIDA) is modification of IDA in which complexity of basic algorithm is reduced by using concept of Syndrome Decoding. The decoder is consisted of two sub-decoders namely row-decoder and column-decoder both placed in succession. Interested readers may visit original paper by the same author [9].

# 4. IMAGE CODING AND TRANSMISSION

Assume an image of size $K_1xK_2$ pixels with $K$ bits given to each pixel. So the net size of image is $K_1xK_2xK$.

## 4.1 Splitting the image into binary matrices

First of all the image will be split into $N$ binary matrices of dimension $K_1xK_2$ each.

$$[image]_{K_1xK_2xN} = [binMat]^0_{K_1xK_2} .....[binMat]^{K-1}_{K_1xK_2} \qquad (4)$$

Without loss of generality we can say that $[binMat]^0_{K_1xK_2}$ is the matrix of image's least significant bits (LSB) and $[binMat]^{K-1}_{K_1xK_2}$ is the matrix of image's most significant bits (MSB). The splitting process is shown in figure 3.

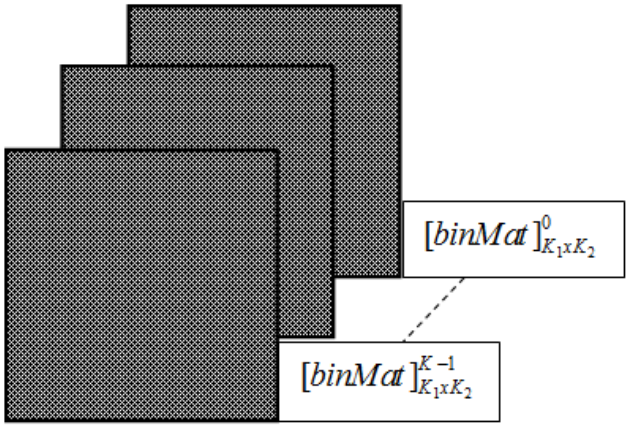


**Fig 3: Image in terms of binary matrices**

## 4.2 Encoding Image Matrices

As the image become $K$ matrices with $K_1xK_2$ dimension each. Now all of these $K$ matrices can easily be encoded using rate compatible Product Codes using the procedure described in section 3. The dimension of the code used as row code is assumed to be $[N_2, K_2, d_2]$ and the dimension of the code being used as column code is assumed to be $[N_1, K_1, d_1]$.

## 4.3 Image Combining

Once the encoding is done image can be reformulated using the same technique in reverse. This can be expressed as;

$$[binMat]^{0}_{N_1xN_2} .....[binMat]^{K-1}_{N_1xN_2} = [image]_{N_1xN_2xK} \quad (5)$$

As the codes being used as systematic codes so image's visibility is not disturbed only a frame will appear on bottom and right side of the image.

## 4.4 Image Transmission

OFDM frame architecture is also identical to that of images and Product codes. If we choose such a Product code whose column code dimension is equal to number of subcarriers in OFDM then it becomes a perfect match. And in our simulation we have made use of this fact.

## 4.5 Image Decoding

Upon receiving an image from OFDM channel image is decoded by taking the same steps in reverse. Firstly, the image will be split into $K$ matrices of dimension $N_1xN_2$ each. They are in fact $K$ number of code words of the Product code $[N_1N_2, K_1K_2, d_1d_2]$

Then these code words are passed through the Modified Iterative Decoder that is consisted of row and column decoder in succession. After desired iterations of MIDA decoder $K$ messages will be obtained each of size $K_1xK_2$.

After that these matrices can be rejoined to formulate the original image. This process is shown in figure 4. In this way all the matrices are simply augmented to formulate the image.

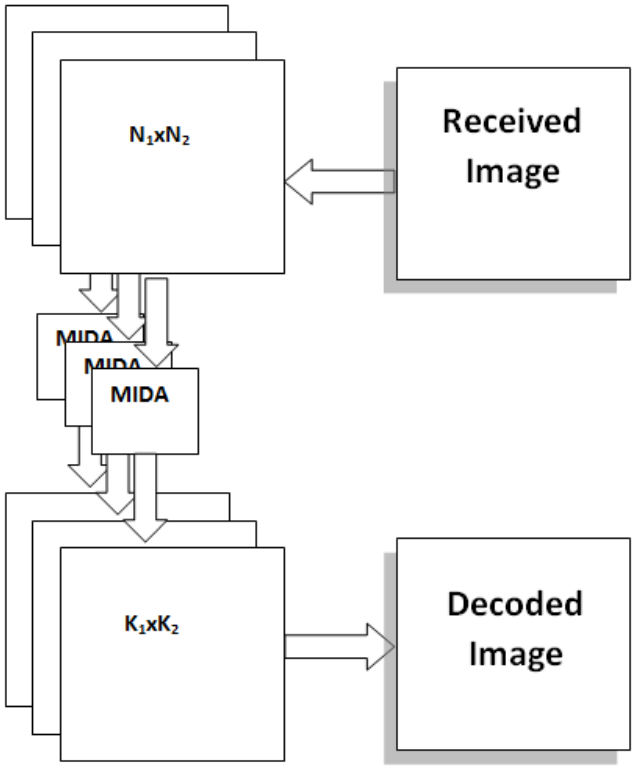


**Fig 4: The Decoding Process**

## 5. RESULTS

Coding schemes used for this framework are set of product codes. Since product codes are matrix codes, where rows contain one code and column contains another code. The set of row codes and column codes used in this paper are listed in table1. All of these codes are BCH codes.

**Table. 1 Product Codes**

| Sr. | Row Code | Column Code | Product Code | Code rate | Error Correction Capability |
|---|---|---|---|---|---|
| C1 | [63,63,1] | [63,63,1] | [3969,3969,1] | 1 | 0 |
| C2 | [63,57,3] | [63,63,1] | [3969,3591,3] | 0.9 | 1 |
| C3 | [63,51,5] | [63,63,1] | [3969,3213,5] | 0.8 | 2 |
| C4 | [63,36,11] | [63,63,1] | [3969,2268,11] | 0.57 | 5 |
| C5 | [63,63,1] | [63,57,3] | [3969,3591,3] | 0.9 | 1 |
| C6 | [63,57,3] | [63,57,3] | [3969,3249,9] | 0.82 | 4 |
| C7 | [63,51,5] | [63,57,3] | [3969,2907,1 | 0.73 | 7 |

| Sr. | Row Code | Column Code | Product Code | Code rate | Error Correction Capability |
|---|---|---|---|---|---|
| | | | 5] | | |
| C8 | [63,36,11] | [63,57,3] | [3969,2052,33] | 0.51 | 16 |

So set of code is initially consisted of four different product codes. That is

$$C = \{C_i\}; 1 \le i \le 8 \qquad (6)$$

The error correcting capability of a block code can be found by the following equation.

$$t = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor \qquad (7)$$

In first four codes that is C1 to C4 column code is considered as rate 1 that is [63, 63, 1] while in last four codes that is C5 to C8 [63, 57, 3] is considered as column code. The significance of column code in terms of bit error rate (BER) can be found in figure 11.

In the following simulations C6 Product code is used for encoding. Figure 5 shows the original Lena image of dimension 57x57 pixel. Figure 6 shows the received noisy image without Product codes.

As the constituent codes are systematic codes so even after encoding image is visible. This is shown in figure 7. Now the encoded image is passed through the additive white Gaussian noise (AWGN) that end up in figure 8.

After passing the image of figure 8 from the Product decoder the original image is recovered that is depicted in figure 9. A slight degradation can be noticed but the difference is not significant.

**Fig 5: Origional Image**

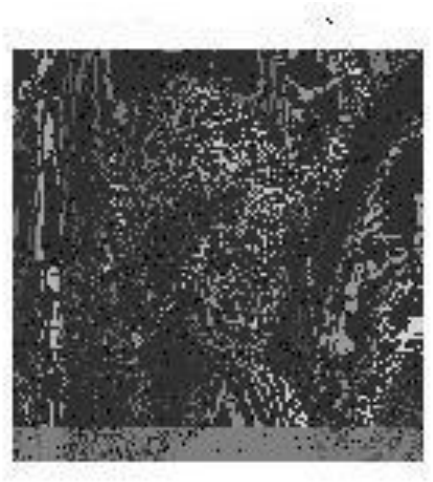

**Fig 6: Received Noisy Image**

**Fig 7: Encoded Image**

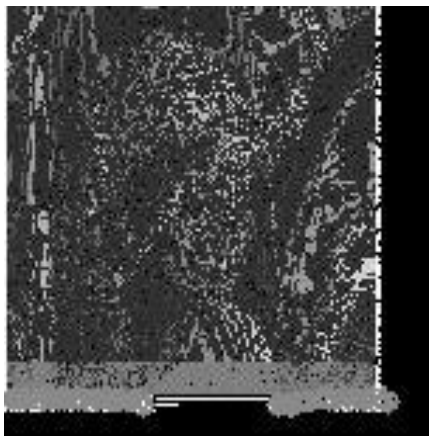

**Fig 8: Received Encoded Noisy Image**

**Fig 9: Decoded Image**

Figure 10 shows the analysis of first four product codes that is C1 to C4 over AWGN channel listed in table-1. Product code C1 that have maximum code rate that is 1, have the poor bit error rate performance since its error correction capability is null. Product code C2 and C3 are compartively better than C1, as their minimum distances are 3 and 5 respectively and their error correction capabilities are 1 and 2 respectively. Product code C4 has the poor code rate but has a high minimum distance that is 11 so its error correction capability is 5. The relationship between the error correction capability and the minimum distance is given in equation. Fig-11 shows the significance of product codes where column code is also error correcting code. And this performance is comparable to that of turbo codes performance used by [4].

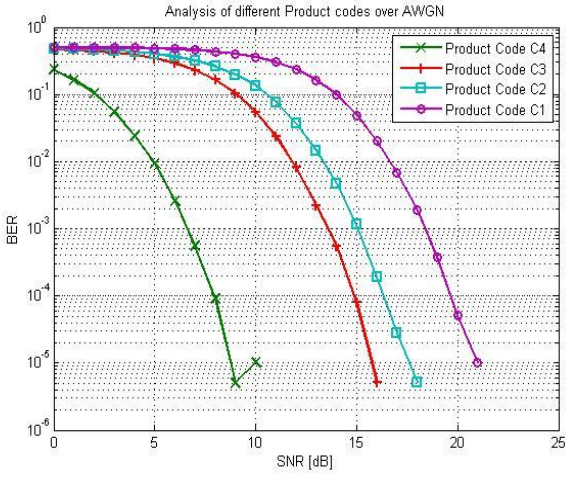


**Fig 10: Analysis of Prodcut codes with rate one colum code over AWGN**

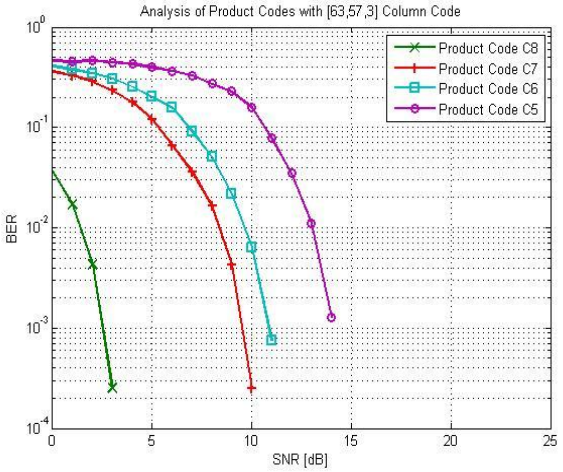


**Fig 11: Anaylysis of Product codes with [63,57,3] column code**

## 6. CONCLUSIONS

In this paper product codes are proposed for secure image transmission due to their structural compatibility with the images. By the comparison it is shown that Product codes can play a vital role in almost error free communication of images when redundancy is high. For example, in case of code rate 0.57 the BER=4x10e-6. The vitality of the scheme is demonstrated by different simulations. The scheme can be used with any other security technique like water-marking, stenography and cryptology.

## 7. ACKNOWLEDGMENTS

This research work was supported by Higher Education Commission (HEC) of Pakistan.

## 8. REFERENCES

[1] Atta-ur-Rahman, Naseem, M.T., Qureshi, I.M., Muzaffar, M.Z. “Reversible watermarking using Residue Number System”. 7th International Conference on Information Assurance and Security (IAS), pp. 162-166, 5-8 Dec, 2011.

[2] C. Nanjunda, M. Haleem and R. Chandramouli, “Robust encryption for secure image transmission over wireless channels,”

[3] C. Mathur, K. Narayan and K. Subbalakshmi, “On the design of error-correcting ciphers,” EURASIP Journal onWireless Communications and Networking, Vol.2006, pp.1-12, November 2006.

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

[5] A. Gabay, M. Kieffer, P. Duhamel,”Joint Source-Channel Coding Using Real BCH Codes for Robust Image Transmission”. IEEE transactions on Image Processing. Vol. 16, No. 6, June 2007.

[6] M.Williams, F. J. and N. A. Sloane: The theory of error correcting codes. I and II. Amsterdam: North-Holland Publishing Co. North-Holland Mathematical Library, Vol. 16, 1977.

[7] P. Elias, “Error-free coding,” IEEE transactions on Information Theory, vol. 4, pp. 29-37, 1954.

[8] O. Al-Askary,"Coding and iterative decoding of concatenated multi-level codes for the Rayleigh fading channel", in Doctoral thesis in Radio communication systems, Stockholm, Sweden: KTH Information and Communication Technology, 2006.

[9] Atta-ur-rahman, Ghouri S.A., Adeel H., Waheed.A, "Performance of Iterative Decoding Algotihm for Product Code". Proceedings of International Conference on *Computational Aspects of Social Networks* (CaSoN), pp. 147 - 151, 19-21, Salamanca, Spain. Oct. 2011.