Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 7 (2012) pp. 156-163

Reversible and Robust Watermarking using Residue Number System and Product Codes

Atta-ur-Rahman[1], Muhammad Tahir Naseem[2] and Muhammad Zeeshan Muzaffar[3]

[1] School of Engineering and Applied Sciences, ISRAUniversity,
Islamabad Campus, Islamabad, Pakistan
ataurahman@biit.edu.pk

[2] School of Engineering and Applied Sciences, ISRAUniversity,
Islamabad Campus, Islamabad, Pakistan
mtahirnaseem@biit.edu.pk

[3] School of Engineering and Applied Sciences, ISRAUniversity,
Islamabad Campus, Islamabad, Pakistan
zeeshan.muzaffar@isra.edu.pk

***Abstract*: Reversible watermarking is a process in which the watermark is embedded in such a way that when the watermarked image passes through the authentication process, the original image is also recovered exactly along with watermark. Restoring the original image is important for the applications such as medical, military and law-enforcement etc. Reversible fragile watermarking scheme is presented by introducing the Residue Number System (RNS). One redundant bit is added as a watermark to some of the pixels and rest is changed into residues. By adding an extra bit, the watermarked pixel becomes nine bits and the residues became nine bits which makes the medical image secure by confusing the attacker that where the watermark is embedded. Robustness in digital watermarking is required especially when communication links are involved in image transmission. In this paper product codes are proposed since their structural properties are compatible with the images. For decoding of these codes modified iterative decoding algorithm is used which is a low complexity suboptimum algorithm. Results show that proposed scheme performs well against noise attacks.**

***Keywords*:** Reversible watermarking, Residue Number System(RNS) , Chinese Remainder Theorem (CRT), Product Codes, Modified Iterative Decoding Algorithm

I. Introduction

In digital watermarking, a noise like signal is embedded into an image for protection and authentication. The watermarking process usually introduces a degradation (bit replacement, quantization etc) into an image. Although this degradation is slight but is unacceptable in certain applications which are very sensitive like medical, military and law-enforcement etc.

Reversible watermarking is basically a digital watermarking with an additional feature that once the watermark has been authenticated, the original image is also recovered exactly [1]. In watermarking scheme, the watermark is sensitive to intentional or unintentional attacks and is subject of many applications like content authentication [2], finger printing [3] and source tracking [4].

Different techniques are developed by the researchers to solve the reversible watermarking issues. A low capacity reversible watermarking is discussed in [5] by using an invertible addition. The restriction is made on embedder to be additive and non-adaptive. Another scheme is discussed in [6] in which the author compresses one of the least significant bit planes of the host image, appends the payload and image hash, encrypts the final result and then replaces the original bit plane with the encrypted result.

Celik et al. [7] proposed a loss-less reversible watermarking scheme by quantizing and then compressing the coefficients and then appends payload to it. This scheme is capable of hiding 0.7 bits/pixel. A very high data-hiding capacity for color images is proposed in [8] which recover the original image exactly. The algorithm hides several bits in the difference expansion (DE) of vectors of adjacent pixels. Kalker et al. [9] proposed capacity bounds for reversible watermarking and also proposed error correction codes to make reversible watermarking robust to ordinary processing.

Ni et al. [10] utilizes zero or minimum point of histogram. If the peak is lower than the zero or minimum point in the histogram, it increases pixel values by one from higher than the peak to lower than the zero or minimum point in the histogram. While embedding, the whole image is searched. Once a peak-pixel value is encountered, if the bit to be embedded is '1' the pixel is added by 1, else it is kept intact. Alternatively, if the peak is higher than the zero or minimum point in the histogram, the algorithm decreases pixel values by one from lower than the peak to higher than the zero or minimum point in the histogram, and to embed bit '1' the encountered peak-pixel value is subtracted by 1. The decoding process is quiet simple and opposite of the embedding process.

In this paper, spatial domain reversible watermarking is proposed for medical images to achieve secrecy of each patient history which is very sensitive to detect any tampering in image and to recover original image. The algorithm

randomly selects some of the pixels (between the range 30% to 40%) from the image for embedding one bit for each pixel while rest of the pixels to residues which are recovered uniquely by Chinese remainder theorem (CRT) [11]. The randomly selected pixel value consists of 8 bits. One redundant bit is added for watermark embedding and one parity bit is also concatenated by making watermarked pixel to 10 bits. The residues consist of 9 bits and one parity bit is concatenated by making residues to 10 bits which ensures the security of watermarked system that where the watermark is embedded since, each watermarked pixel and residues are 10 bits both. The pixel value where watermark is embedded becomes a key and is known at receiver side for decoding. Moreover, the original image is also not needed in extraction process which is blind reversible watermarking. A comprehensive detail on reversible watermarking, past work and future dimensions are investigated in [12]. A modified idea of difference expansion scheme is presented in [13] originally motivated by [8], the scheme provides high hiding capability.

Robustness in digital watermarking is essential whenever images are transmitted over wireless channel especially. Channel hostilities may cause image as well as watermark unrecoverable at receiver side.

Error correcting codes are mainly used to recover the data at receiver side effectively. In this paper we have proposed product codes for sake of robustness due to two reasons. Firstly, product codes are matrix codes so this makes them compatible with images that are also consisted of matrix of pixels. Secondly, error-correcting capability of product codes is far better than simple one dimensional codes.

Decoding complexity of optimal decoder of Product codes makes them less attractive for real time transmission however, in this paper a Modified Iterative Decoding Algorithm (MIDA) is used for decoding process originally proposed by Atta-ur-Rahman et al [14].

The rest of paper is organized as follows: section 2 describes some typical features of reversible watermarking. The Residue number system (RNS) is discussed in section 3. The proposed watermarking scheme is described in section 4. Introduction to Product Codes and Modified Iterative Decoding Algorithm is given in section 5. Section 6 contains the encoding mechanism. Simulation results are discussed in section 7 and section 8 concludes the paper..

II. Features of Reversible Watermarking

A. Transparency

The watermark should be imperceptible to human beings after embedding.

B. Reversibility

The original image is perfectly recovered after the watermarked image passes through the authentication process.

C. Fragility

The watermark is expected to destroy when the watermarked image is attacked

D. Blind Extraction

The extraction process does not need original image.

E. Robustness

Resistance of the watermarked image and watermark against various attacks.

III. Residue Number System

The residue number system (RNS) is defined by the set of numbers $(m_1, m_2, ..., m_k)$ called moduli which are relatively prime such that $\gcd(m_i, m_j) = 1 \forall i, j = 1, 2, ..., n$. The integer X can be represented by the set of unique $k-tuple$ residues $(x_1, x_2, ...x_k)$ where

$$x_i = X \bmod m_i \qquad (1)$$

The dynamic range of RNS is 0 to $M-1$ where

$$M = \prod_{i=1}^{k} m_i \qquad (2)$$

Any positive integer X in the range $0 \le X < M$ can be represented by the unique $k-tuple$ residue sequence as

$$X \xrightarrow{FT} (x_1, x_2, ..., x_k)$$
$$X \xleftarrow[RT]{} (x_1, x_2, ..., x_k)$$

The conversion of integer X to residues is called forward transform (FT) and from residues to integer X is called reverse transform (RT) and it relies on Chinese remainder theorem (CRT) to calculate integer X back as.

$$X = [\sum_{i=1}^{k} M_i \mid x_i L_i \mid_{m_i}] \bmod M \qquad (3)$$

where M is defined in equation (2) and

$$M_i = \frac{M}{m_i} \quad \text{and} \qquad \left| L_i M_i \right|_{m_i} = 1$$

where L_i is the multiplicative inverse of M_i with respect to m_i.

IV. Proposed Watermarking Scheme

The watermarking scheme consists of two stages, first is embedding and second is extracting. Before embedding the watermark some pre-processing is done.

A. Pre-Processing

Given a gray-scale image I of size $(M \times N)$, with intensity level of a pixel varies from 0 to 255. The value 255 is factorized to 15 and 17 which become the corresponding moduli (m_1, m_2) of image respectively and are relatively prime. Since, the dynamic range of RNS is 0 to 254; every 255

intensity value is treated as 254 which do not rigorously affect the visual quality of an image.

B. Watermark embedding

Randomly selected pixels (30% to 40%) are to be watermarked by embedding one bit and change the rest of pixels into residues by equation (1). Calculate the even parity of residues and append with the corresponding residues. For each pixel to be watermarked by $w \in \{0,1\}$, the embedding procedure is as under:

1. a bit '0' is padded at left side of MSB as
$$I_p^{'} = 0.I_p$$
where I_p is a pixel to be watermarked.
2. Calculate the even parity of $I_p^{'}$ as
$$P_e = even\_parity(I_p^{'})$$
3. The corresponding watermarked pixel is
$$w_p^{'} = I_p^{'} + A.(P_e \oplus w) \quad (4)$$
where $A = (256)_2$ and
(.) Denotes the binary equivalent and
$\oplus$ Denotes X-OR operator
4. Calculate the even parity of watermarked pixel $w_p^{'}$ and append it with $w_p^{'}$ as
$$P_e = even\_parity(w_p^{'})$$
$$w_p = (w_p^{'}, P_e)$$
5. The parity checked watermarked pixels are appended to the residues to form the watermarked image.

This embedding procedure is explained pictorially in Figure1.

C. Watermark and Original Image Extracting

Given the watermarked image, identify the location of pixels which are watermarked (location is known at decoding stage). The rest of values will be residues. Check parity of each residue and if each residue has same parity as in encoding side then apply equation (3) on residues to get back pixel values then for each watermarked pixel, the extracting procedure is done as follows.

1. Count the number of one's (even parity) in w_p and if the number of ones are even, then exclude parity of w_p and apply 2, 3, 4 and 5.
2. Calculate the most significant (MSB) of the watermarked pixel $w_p^{'}$ as
$$M = MSB(w_p^{'}) \quad (5)$$
3. After extracting MSB again calculate the even parity of remaining part as
$$P_e = even\_parity(remaining)$$
4. Watermarked bit is extracted as
$$w = M \oplus P_e \quad (6)$$
From equation (6), the watermarked bit is extracted and from equation (5) after extracting MSB from the watermarked pixel values, the original image coefficients are extracted.
5. Append residues and original image coefficients to form the original image.

Similar extracting procedure is explained in Figure 2.

D. A Simple Example

Take the pixel value 136 and 254 and $w = 1$. Consider 136 for watermarking then 254 will be the considered for residue.

136 = (10001000)

where (.) denotes the binary equivalent

then, $I_p^{'} = 010001000$

$P_e^{'} = 0$

By using equation (4), the watermarked pixel becomes

110001000 = $w_p^{'}$

Even parity of $w_p^{'}$ becomes $P_e = 1$

So, the value 1100010001= w_p becomes the watermarked pixel (P_e is concatenated with $w_p^{'}$).

By using equation (1), the residues of 249, by taking $m_1 = 15, m_2 = 17$ are {14, 16}.

So,
$$254 \xrightarrow{m_1,m_2} \{14,16\} = (111010000) = I_r^{'}$$

Even parity of $I_r^{'}$ is calculated as

$$P_e = 0$$

So, the 1110100000 = I_r becomes the residue (P_e is concatenated with $I_r^{'}$).

Then (w_p, I_r) are concatenated to form the watermarked image so,

W.I = (w_p, I_r)

At decoding side, I_r are the residues and the number of ones are even so, applying (3) on I_r (excluding parity) gives original pixel value back which is,

$$(14,16) \xrightarrow{CRT} 254$$

Since, the watermark is embedded in w_p so calculate even parity of w_p also w_p = 1100010001

$$P(w_p) = 0$$

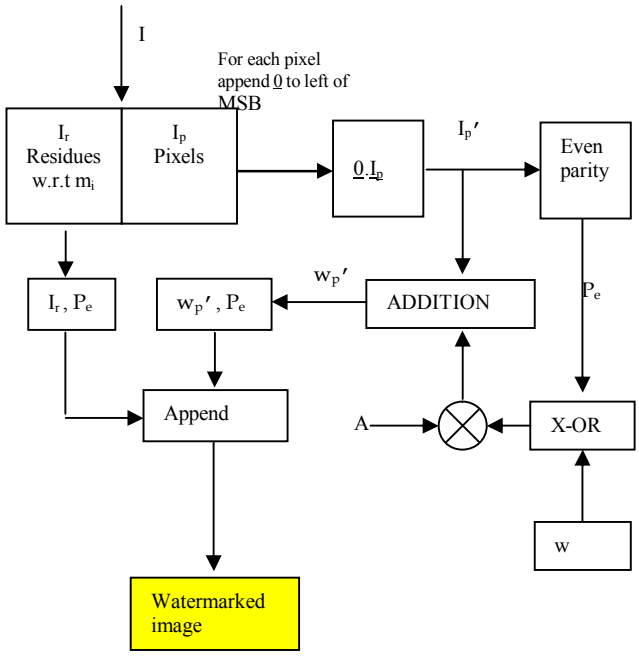

Figure 1: Watermark Embedding

Since the number of ones in w_p are even so, MSB of w_p is extracted and even parity is calculated again after extracting MSB and excluding the LSB of watermarked pixel w_p.

$$MSB(w_p) = 1$$
$$P_e = 0$$
$$w = MSB(w_p) \oplus P_e = 1$$

After extracting MSB and excluding the LSB of w_p, the remaining value becomes the original pixel value $136 = I_p = 10001000$ where I_p is the original pixel where the watermark w = 1 was embedded.

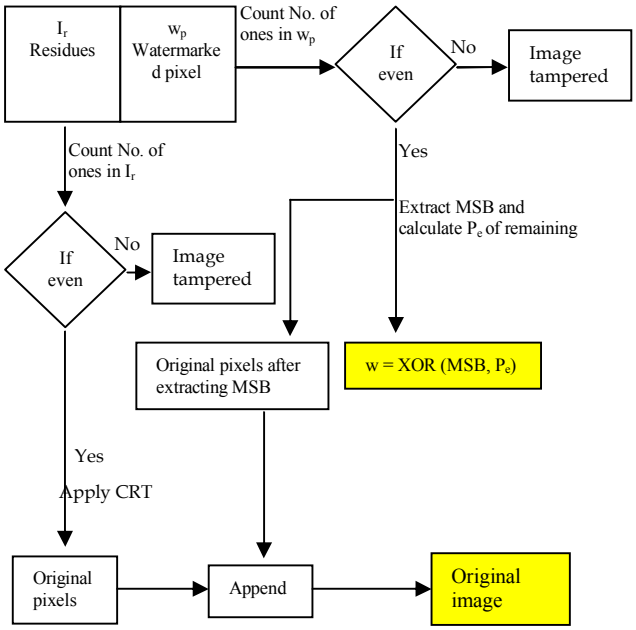

Figure 2: Watermark and Original Image Extracting

V. Product Codes and Modified Iterative Decoding Algorithm

Product codes were first presented by Elias in 1954 [15]. The concept of Product codes is quite simple as well 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.

Consider two 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,

$$R_i = \frac{k_i}{n_i}, i = 1,2 \qquad (7)$$

The product code $\boldsymbol{\Omega}$ 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.

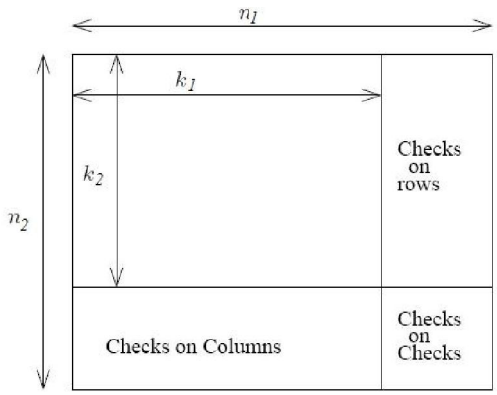

Figure 3: Structure of the Product code

The resultant product code $\boldsymbol{\Omega}$ has the parameters $[n_1 n_2, k_1 k_2, d_1 d_2]$ and the rate will be $R_1 R_2$. 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;

$$\boldsymbol{\Omega} = \mathbf{A}_1^{'} \cap \mathbf{A}_2^{'} \qquad (8)$$

The concept of Iterative Algorithm for Product was proposed by Al-Askary [16] in his doctoral thesis. The complexity of algorithm was quite high especially when the constituent codes are longer. To overcome the complexity of this algorithm a suboptimum modified iterative decoding algorithm was proposed [14] whose performance was comparable to that of native algorithm. In this paper MIDA is used for decoding of Product Codes. Interested reader may study the original paper.

VI. Image Encoding/Decoding Mechanism

As the image is consisted of pixels with each pixel originally consisted of 8bits and after embedding watermark they become 9bits long. For sake of encoding, image is broken into 9matrices from LSBs of each pixel in image to MSBs of each pixel in the image as shown below.

$$[120\text{x}120\text{x}9] = [120\text{x}120]_{\text{LSB}} \ldots\ldots [120\text{x}120]_{\text{MSB}}$$

So the image matrix whose dimensions are 120x120x9 is broken into 9 matrices each of dimension 120x120. This is also depicted in figure 4.

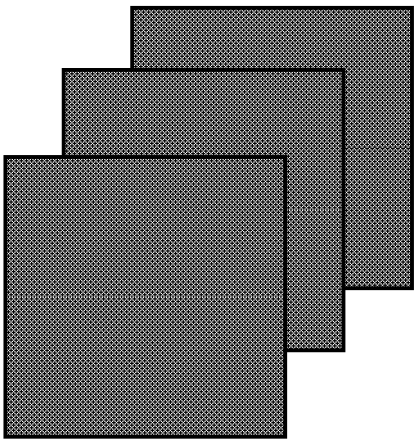

Figure 4: Image's binary matrices after watermark embedding

So in this way we have 9 binary matrices. Now each of these matrices is encoded using the product codes with parameters listed in table 1.

After encoding each matrix all the matrices are augmented to formulate the image again. Now the size of image will become 127x127 according to the code size.

Similarly on receiver side same image will be broken into 9 matrices each of size 127x127 then each of these 9 matrices will be passed through MIDA decoder in parallel fashion. And after decoding it will the original image. Since the decoders will be applied in parallel way so the decoding time of 9 code matrices is identical to that of decoding time of any constituent matrices.

This process is depicted in following flow diagram.

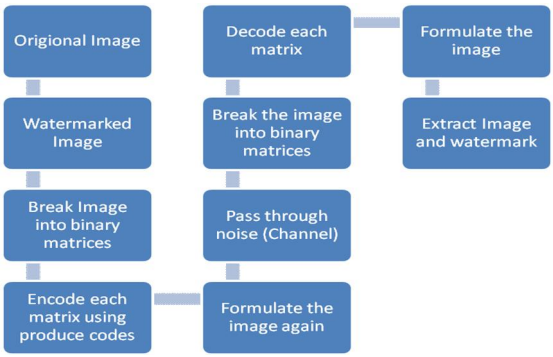

Figure 5: Image's binary matrices after watermark embedding

VII. Simulation Results

To see the effectiveness of proposed system, experiments were conducted in MATLAB 7.0.

Figure 6 shows the original Lena image of size 120x120 pixels chosen for watermarking. Figure 7 shows the random binary watermark of size 120x120 pixels.

Figure 8 shows the watermarked image. Since, the host image is altered during watermark embedding phase the watermarked image is not same as the original host image. The watermark is embedded using the proposed technique discussed above.

Figure 9 shows the extracted watermark. Visible experiment depicts that it is same original images which is shown in Figure 7. Figure 10 shows the recovered original host image. Figure 11 shows the noisy watermarked image after passing through salt and pepper noise with noise density 0.05. Figure 12 shows the watermark which is tampered and Figure 13 shows the tampered image. Since, the image has been tampered during transmission, so, the watermark is not exact and thus, the image is not authentic.

The same image is watermarked then encoded by the Product codes then passed through the same salt and pepper noise with the same noise density is shown in figure 14. Then after passing through the decoder the recovered image is shown in figure 15 while recovered watermark is shown in figure 16.

Product codes are used to make the scheme robust against the noise attacks. As far as visible experiments are concerned results show that proposed scheme with the product codes perform even in presence of noise. This effect can be noticed in figure 13 and 15 respectively.

In figure 13 there is no coding scheme is used while in 15 image is encoded prior to noise addition and then decoded.

The parameter used for row and column codes used as product codes are given in table 1.

Code	Row/Column	Rate/Error Correcting Capability
[127,120]	Rows	0.94/1
[127,120]	Colums	0.94/1

Table 1: Coding PARAMETERS

Hamming codes are used for construction of Product codes. Also same code is used for rows and columns. The reason for choosing these codes is that they have high code rate that is 0.94 so payload is less. Also they are 1bit error correcting codes so if row-wise entire pixel value is gone column code can recover it fully and vice versa.

So in this way many random as well as burst errors will be corrected and this will make the whole image secure.

Figure 6: Original Image

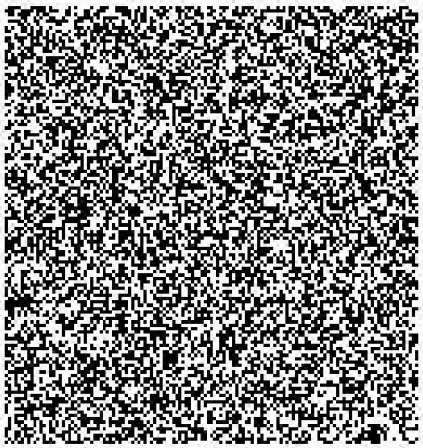

Figure 7: Watermark

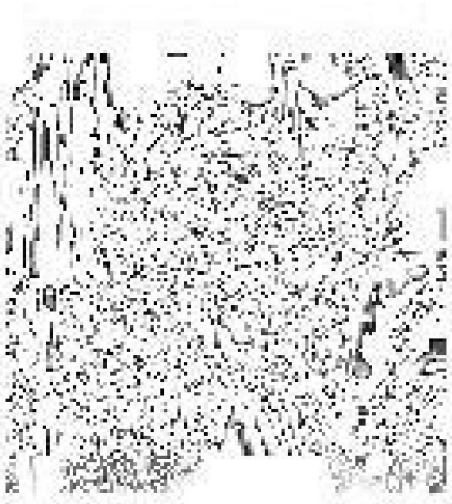

Figure 8: Watermarked Image

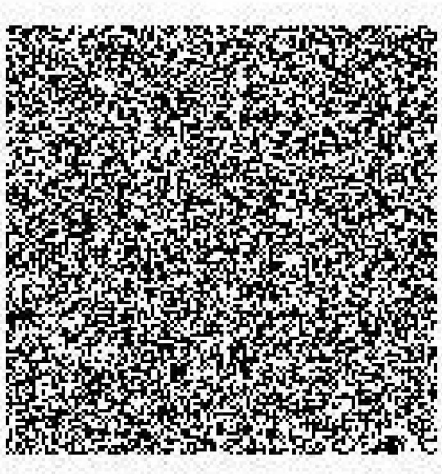

Figure 9: Extracted Watermark

Figure 10: Recovered Image

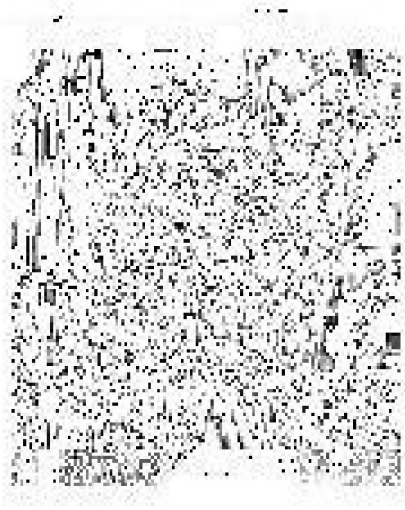

Figure 11: Noisy Watermarked Image

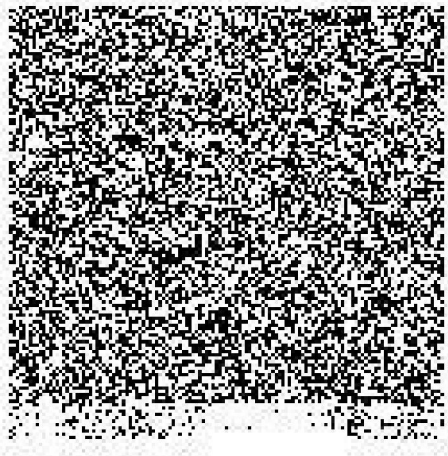

Figure 12: Recovered Watermark

Figure 13: Recovered tampered Image

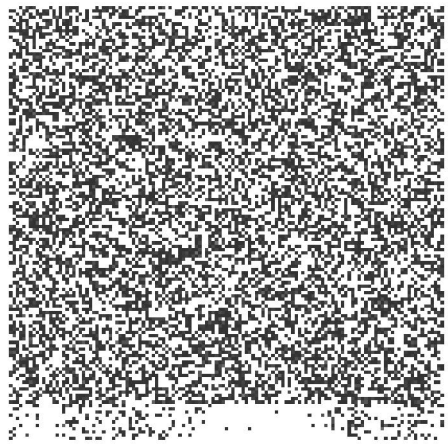

Figure 14: Encoded Noisy Image

Figure 15: Recovered Tampered Image after decoding

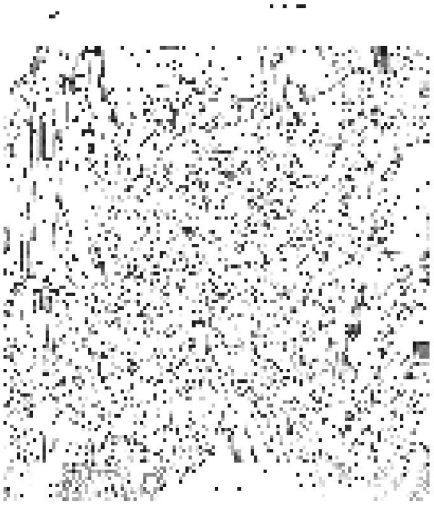

Figure 16: Recovered Watermark

VIII. Conclusions

In this paper, a reversible watermarking technique is proposed to embed binary watermark into digital images in such a way that when the watermarked image passes through the authentication process, the exact image coefficients are also recovered. Unlike traditional watermarking techniques, during watermark embedding, original host is not altered at all. In this technique, the original host image is altered to provide security and the watermark information is not sent on the transmission channel thereby, providing maximum security.

In order to make the scheme overall robust a novel encoding technique is proposed for image transmission with an interesting encoding mechanism using Product Codes. Decoder is employed in parallel way so no extra time complexity is introduced for decoding process.

Results show the viability of the scheme. And it is shown that encoding pays off in terms of image robustness against noise.

IX. Acknowledgements

This research work is sponsored by Higher Education Commission (HEC), of Pakistan.

References

[1] J. Tian , "Reversible data embedding using difference expansion", IEEE Trans. On Circuits and Systems for Video Technology, 13(8): pp. 890-896, August 2003

[2] J. Cox, L. Miller and A. Blossom, "Digital watermarking (1st edition)", USA: Morgan Kaufmann Publishers, 2002.

[3] M. Fridrich and A. Baldoza, "New Fragile Authentication watermark for Images", in Proc of IEEE Integrated conference om Image Processing, pp. 10-13, Sep 2000.

[4] J. Fridrich, M. Golijan and R. Du, "Invertible Authentication", in Proc of SPIE Photonics West Security and Watermarking of Multimedia Contents, vol. 3971, san Jose, CA, pp. 197-208, Jan 2001.

[5] C.W. Hansiger. P.W. James, M. rabbani and J.C. Stoffel, "Lossless Recovery of an Orignal Image containing Embedded Data", U.S Patent 6, 278, 791, 2001.

[6] J. Fridrich, M. Golijan and R. Du, "Lossless data embedding – new paradigm in digital watermarking", EURASIP Journal on applied Signal Processing, vol 2, No. 2, pp. 185-196, Feb 2002.

[7] M. Celik, G. Sharma, "reversible Data Hiding", in Proc IEEE Int. Conference on Image Processing, vol 2, pp. 137-160, sep. 2002.

[8] A. Alattar, "Reversible Watermark using the Difference Expansion of a Generalized Integer Transform", IEEE Transaction On Image Processing, vol. 13, No. 8, August 2004.

[9] T. Kalker and F.M. Willems, "Capacity bounds and Code construction for reversible data-hiding", in Proc. Of Electronic Imaging, Security and Watermarking of Multimedia contents, santa Clera, California, Jan 2003.

[10] Z. Ni, Y.Q. Shi, N. Ansari, and W. Su, "Reversible Data Hiding, In Proc. of International Symposium on Circuits and Systems, Bangkok, Thailand, Vol. 2, pp. 912-915, 25-28 May 2003.

[11] K. W. Watson, "Self-checking computations using residue arithmetic, " Proc. IEEE, vol. 54, pp. 1920–1931, Dec. 1966.

[12] Jen-Bang Feng, Iuon-Chang Lin, Chwei-Shyong Tsai, Yen-Ping Chu. Reversible Watermarking: Current Status and Key Issues. International Journal of Network Security, 2(3):161171, 2006.

[13] M.K. Yaqub, A. Al-Jaber. Reversible Watermarking Using Modified Difference Expansion. International Journal of Computing & Information Sciences, 4(3):134-142. 2006

[14] 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), Salamanca, Spain. Oct. 2011.

[15] P. Alias, "Error-free coding," *IEEE transactions on Information Theory,* vol. 4, pp. 29-37, 1954.

[16] 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.

Author Biographies

Atta-ur-rahman received the B.S. degree in Computer Science from The University of Punjab, Pakistan and M.S. degree in Electronic Engineering from International Islamic University, Islamabad, Pakistan in 2004 and 2007, respectively. He is now senior PhD research student at ISRA University Islamabad Campus, Pakistan. His research interests are Digital/Wireless Communications, Digital Signal Processing, Information and Coding Theory, Soft-computing, Artificial Intelligence, Fuzzy and Hybrid Intelligent Systems.

Muhammad Tahir Naseem received the B.S. degree in Computer Science from The University of Punjab, Pakistan and M.S. degree in Electronic Engineering from International Islamic University, Islamabad, Pakistan in 2005 and 2008, respectively. He is now PhD research student at ISRA University Islamabad Campus, Pakistan. His research interests are Digital Watermarking, Digital Signal Processing and Information Security.

Muhammad Zeeshan Muzaffar received the MSc degree in Computer Science from Islamia University Bahawalpur, Pakistan and M.S. degree in Electronic Engineering from International Islamic University, Islamabad, Pakistan in 2005 and 2008, respectively. He is now PhD research student at ISRA University Islamabad Campus, Pakistan. His research interests are Digital Stenography, Digital Signal Processing and Information Security.