An enhanced technique for digital watermarking using multilevel DWT and error correcting codes

Mohsen Hussein Mohmmad[1] , Monia Abdullah Ahmed[1] and Adnan Abdullah Zain[2]
[1] Department of Information Technology, Faculty of Engineering, Aden University.
[2] Department of Electronics & Communications, Faculty of Engineering, Aden University
DOI: https://doi.org/10.47372/uajnas.2020.n2.a08

Abstract

Digital Watermarking has attracted researchers' attention because of its useful applications and, over the past decades, great efforts have been made to develop digital watermarking techniques and algorithms. Most researches use different transform techniques to enhance the robustness and quality of extracted watermark. This paper presents an enhanced technique for digital image watermarking based on multilevel Discrete Wavelet Transform (DWT) in conjunction with the well-known RS codes over finite fields. To observe and appreciate the significance of using the error correcting codes technique for enhancing the digital watermarking performance against attacks, a series of experiments were conducted. The enhanced methodology, presented and implemented in this research, achieved a very good performance. Regarding the significance of using error correcting codes in conjunction with DWT transform digital image watermarking; it was shown that, in all cases investigated, for all the attacks considered, there was an increase in the robustness of the digital watermark, in terms of the performance measure SSIM values. In some cases, it improves, to almost 27 times, the case without using error correcting codes. Among each class of codes, for all the attacks, Reed-Solomon block codes of length $n = 255$ over the Galois field $GF(2^8)$ with $k = 135$, performs better than all others.

Keywords: Discrete Wavelet Transform (DWT), image watermarking, Error Correcting Codes, watermarking embedding, watermarking extraction.

Introduction

Digital Watermarking embeds a digital image, known as a watermark, into a host image with the aim of being able to detect its presence at a later stage [4]. Its main uses are, but not limited to, establishing and proving ownership rights, tracking content usage, ensuring authorized access, facilitating content authentication and preventing illegal replication [3].

Digital watermarking has many branches where researches are involved with. These branches depend on how watermarking is classified. There are many ways to classify it as shown in Figure (1) [3,7,5]. In transform domain, there are many types of transforms such as discrete Fourier transform (DFT), discrete cosine transform (DCT), and discrete wavelet transform (DWT). Our research is applied for non-blind watermarking in transform domain with invisible watermark [6,5,8,11,9]. It is focusing on the ability of using DWT transform in conjunction with a family of RS cyclic error correcting codes of different rates to investigate its effectiveness on the robustness of the watermark against various well-known watermarking attacks. The remainder of this paper is organized as follows:

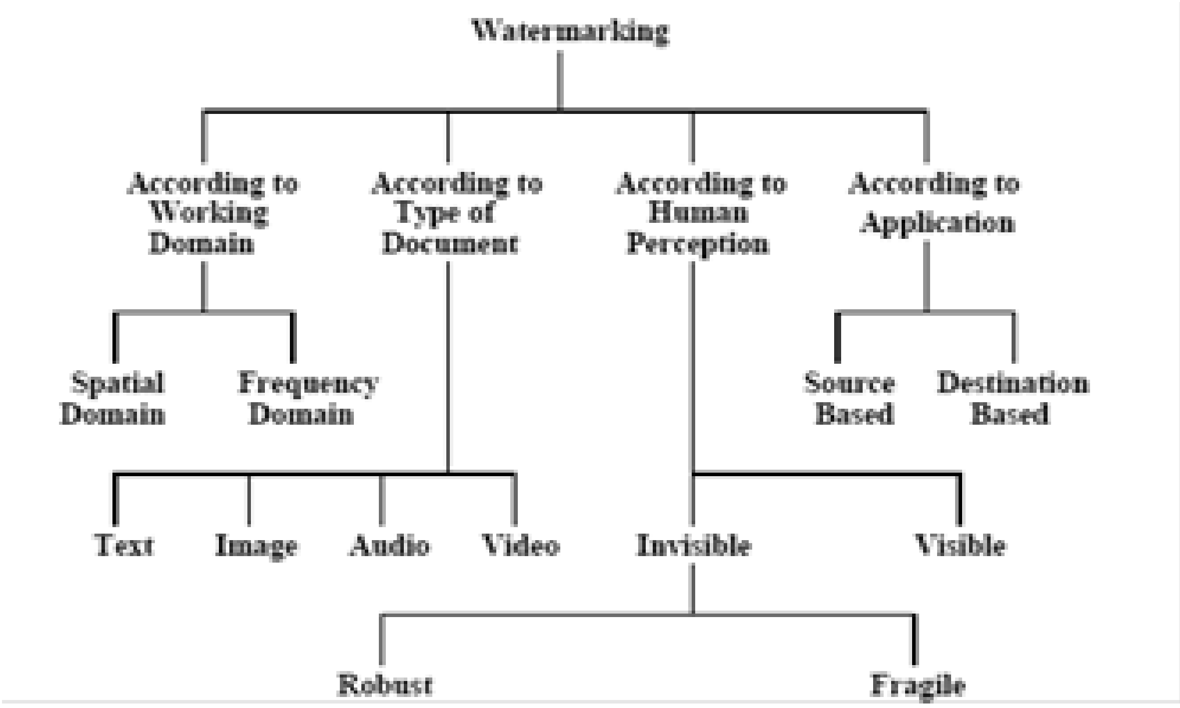

Figure 1: Watermarking Classification

Mathematical Preliminary & State of the Art

1.Discrete Wavelet Transform

Wavelet transform is one of the advanced mathematical transforms with many applications in different areas[1,6]. Due to its properties, Wavelet transform has become an important tool in image processing and watermarking. The basic idea of discrete wavelet transform (DWT) is to separate the frequency details of the image, and is based on wavelets, of varying frequency and limited duration. Each level of decomposition of (DWT) separates an image into four sub-bands, namely a lower resolution approximation component (LL) and three other corresponding to horizontal (HL), vertical (LH) and diagonal (HH) detail components. The LL sub-band is the result of low-pass filtering both the rows and columns and contains an approximate description of the image. The HH sub-band is high-pass filtered in both directions and contains the high-frequency components along the diagonals. The HL and LH images are the results of low-pass filtering on one direction and high-pass filtering in another direction. After the image is processed by the wavelet transform, most of the information contained in the original image is concentrated into the LL image. LH contains mostly the vertical detail information which corresponds to horizontal edges. HL represents the horizontal detail information from the vertical edges. The low pass sub-band can further be decomposed to obtain another level of decomposition[9,12,13]. This process is continued until the desired number of levels determined by the application is reached. The result of a three levels of decomposition of an image is shown in Figure 1.

2. Error Correcting Codes

In this subsection, an introduction to the well-known class of RS error correcting codes is presented[9]. RS codes are a subclass of cyclic codes and are characterized by their particular construction through minimal polynomials[2]. The construction of this kind of codes is very similar to generating cyclic codes, with the only difference that, choosing the zeros of the generating polynomial **(X)**.We to consider the elements of the Galois field **GF(q^m)** described by consecutive powers of the primitive element α. As a matter of fact, if we are required to correct t errors, we have to select 2t consecutive powers of the primitive element α so that to obtain a minimum distance **2t +1**. Reed-Solomon codes are minimum distance codes, that is a Reed-Solomon code of the **(n , k),** which will be denoted by **RS(n , k)** has got the smallest possible Hamming distance: **dmin(RS(n , k))= n – k + 1 [10].**

3.Proposed Methodology

This paper proposes an enhanced digital image watermarking technique that is based on the Multilevel Discrete Wavelet Transform (DWT) in conjunction with two families of powerful error correcting codes, RS codes over finite fields.

1. Digital Watermarking Algorithm

In general, a digital watermarking system consists of an embedding and an extracting procedure [1]. In the proposed scheme, an error correcting code is incorporated to correct the errors that occur due to the attacks on the watermarked image. The next subsections will present the Embedding and Extracting methods as well as the Encoding and Decoding of the digital image watermark.

1.Digital Watermarking Embedding

In this approach, the digital watermark image is encoded using RS block error correcting codes, then DWT is applied to the encoded digital watermark. On the other hand, the digital host image is DWT transformed directly. The embedding of the encoded digital watermark is performed using the well-known alpha blending technique [13,14] as explained below. Alpha blending technique used for Watermark Embedding. The formula of the alpha blending embedding technique is as follows:

$$\mathbf{WMI=k\times(LLj)|+q\times(EWMj)} \qquad \mathbf{(1)}$$

Where :

- **EWMj** is the j-levels low frequency approximation of the encoded watermark image.
- **LLj** is the j-levels low frequency approximation of the host image HI
- **WMI** is the watermarked image.
- **k** & **q** are the scaling factors.
- **j = 3** denotes the DWT decomposition level.

Figure (2) gives a block diagram that summarizes the above procedure.

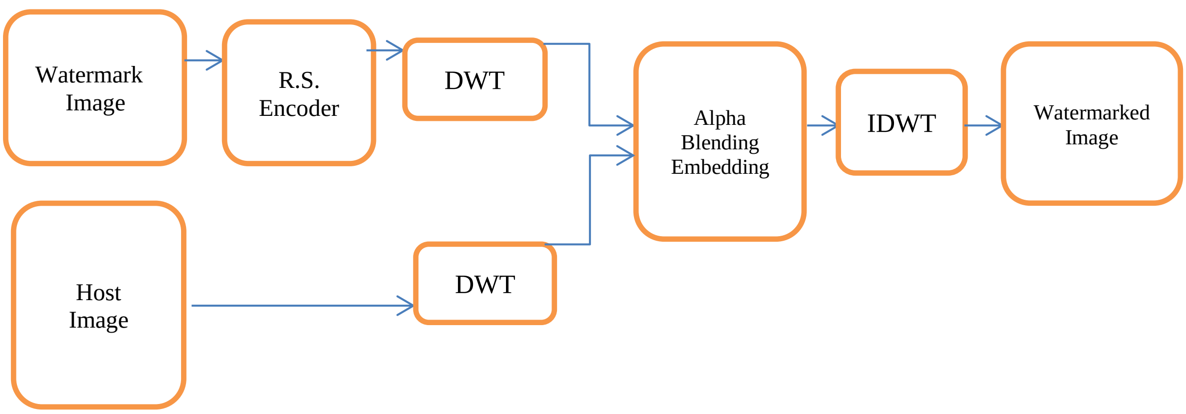

Figure (2) Watermarking Embedding

2.Digital Watermarking Extraction

In this research, various types of attacks on the watermarked image are considered. Addition of noise was the main focus of this research; the noise types considered are Salt & Pepper, Gaussian, and Speckle noise. In this subsection, the extraction of the digital watermark method is presented and illustrated.

Watermark Extraction using Alpha blending extraction technique:

Let **WMIA** denote the attacked digital watermarked image. The formula of the alpha blending extraction technique is as follows:

$$\mathbf{ERW = (WMIA - k \times LLj)/q} \qquad \mathbf{(2)}$$

Where :

- **ERW** is the low frequency approximation of the recovered encoded watermark.
- **LLj** is the j-levels low frequency approximation of the host image **HI**.
- **WMIA** is the attacked watermarked image.

Figure (3) gives a block diagram that summarizes the above procedure.

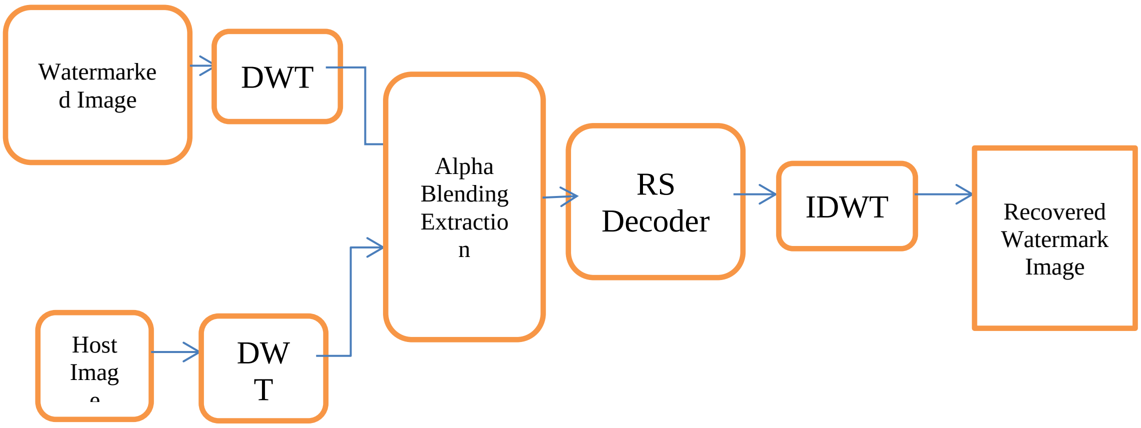

Figure 3: Watermark Extraction

3.Performance Evaluation & Measures

For non-blind digital watermarking systems, the digital watermark image(WM), should not affect the appearance of the host image(HI) ; in image processing terminology this is known as a distortion [9,15,16]. The Peak Signal to noise ratio is given as follows:

$$\mathbf{PSNRdB = 10 * \log10 \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} HI^2(i.j)}{\sum_{i=1}^{M}\sum_{j=1}^{N} [H(i.j) - WMI(i.j)]^2}} \qquad \mathbf{(3)}$$

For copy write protection application of the digital watermarking systems, the inserted digital watermark should be extracted successfully even though the watermarked image undergoes severe attacks. The similarity between the inserted digital watermark and the extracted digital watermark is a good measure adopted in such type of applications.

Structured Similarity Image Value SSIM [9]

$$\mathbf{SSIM} = \frac{(2\mu x\ \mu y| + c1)\ (2\sigma xy + c2)}{(((\mu x^{\wedge}2)\ (\mu y^{\wedge}2) + c1)\ ((\sigma x^{\wedge}2) + (\sigma y^{\wedge}2) + c2))} \qquad \mathbf{(4)}$$

Where"μ","б",&"бxy are mean, variance, and covariance of the digital watermark image and the recovered digital watermark image. "c1"," c2" are the stabilizing constants. SSIM has a value between 0–1.Similar images have SSIM value near to 1.

Experimental Setup & Results Discussions

To validate the enhanced proposed algorithm, a series of experiments are designed and implemented using the well-known software package MATLAB.

1.Experimental setup & Demonstration of Watermark Embedding

(4a)Host Image

(4b) Watermark Image

(4c)Watermarked Image

Figure (4a) shows the host image, Figure (4b) shows the watermark image, and Figure (4c) shows the watermarked image.

To obtain the optimal values for the scaling factors r & q , extensive experiments were conducted. Below, it is shown that the optimal values are r = 0.99 and q = 0.001. For comparison, the worst case values for r & q were recorded. So, throughout the experimental setup, these optimal values are used.

2.Scenario 1: Comparing between the noise level with and without RS ECC

In this experiment, three types of noises were added (to simulate the attack), with different levels. The resulting SSIM & PSNR were computed for two cases, case 1: without using RS ECC code, and case 2: with using RS ECC code. The results are shown in Table 1.

Table 1: With / Without RS ECC in Three Attacks

Noise Level	Salt & Pepper Attack		Gaussian Noise Attack		Speckle Noise Attack	
	Without ECC	With RS ECC	Without ECC	With RS ECC	Without ECC	With RS ECC
	SSIM	SSIM	SSIM	SSIM	SSIM	SSIM
0.0001	0.7042	0.8971	0.2602	0.4476	0.3368	0.4633
0.0003	0.4142	0.8453	0.1960	0.4266	0.2896	0.4384
0.0005	0.3052	0.7955	0.1621	0.4146	0.2649	0.4263
0.0007	0.2639	0.6675	0.1370	0.4047	0.2469	0.4185
0.0009	0.2323	0.6260	0.1208	0.3967	0.2324	0.4121
0.01	0.0442	0.4170	0.0128	0.3579	0.0954	0.3729

- **Salt & Pepper**

In this case, a noise of type Salt & Pepper is added to the watermarked image with different levels. Table 1 shows the values of SSIM for each noise level for both cases: with and without RS ECC block code.

It can be observed that around 9 times an improvement is gained when using RS codes at the noise level (0.01), this is obtained from (0.4170 / 0.0442). Figure (5), illustrates, in bar plots, the significant increase in SSIM when using RS codes, for various noise levels.

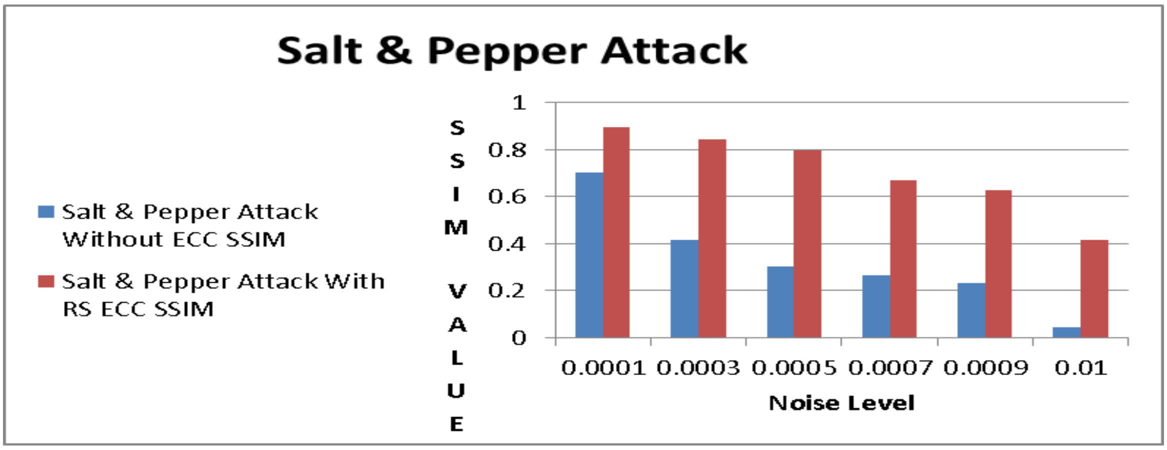

Figure 5 : SSIM Value / Noise Level With RS ECC & Without ECC

- **Gaussian Noise Attack**

In this case, a noise of type Gaussian Noise is added to the watermarked image with different levels. Table 1 shows the values of SSIM for each noise level for both cases: with and without RS ECC block code.

It can be observed that around 27 times an improvement is gained when using RS codes at the noise level (0.01), this is obtained from (0.3579 / 0.0128). Figure (6), illustrates, in bar plots, the significant increase in SSIM when using RS codes, for various noise levels.

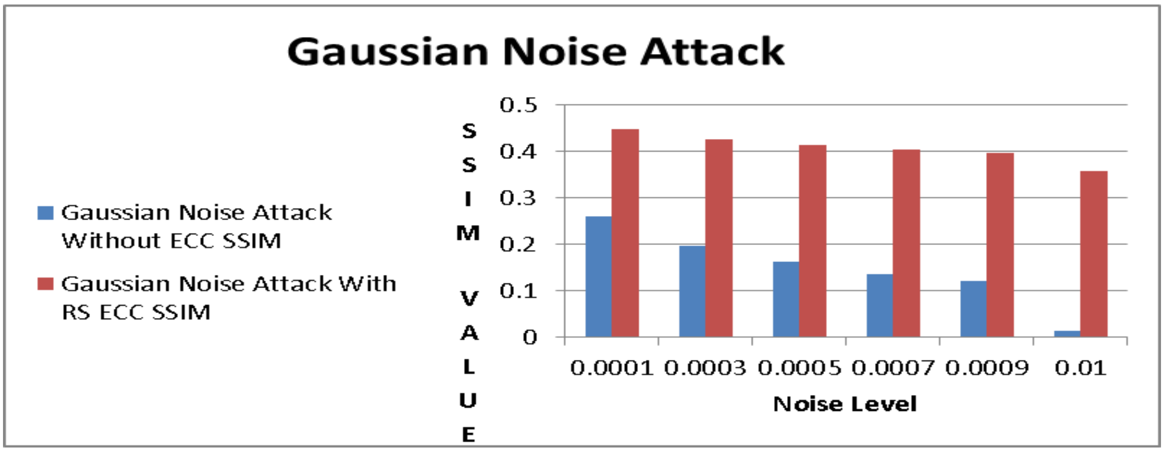

Figure 6: SSIM Values / Noise Level With RS ECC & Without ECC

- **Speckle Noise Attack**

In this case, a noise of type Speckle Noise is added to the watermarked image with different levels. Table 1 shows the values of SSIM for each noise level for both cases: with and without RS ECC block code.

It can be observed that around 4 times an improvement is gained when using RS codes at the noise level (0.01), this is obtained from (0.3729 / 0.0954). Figure (7), illustrates, in bar plots, the significant increase in SSIM when using RS codes, for various noise levels

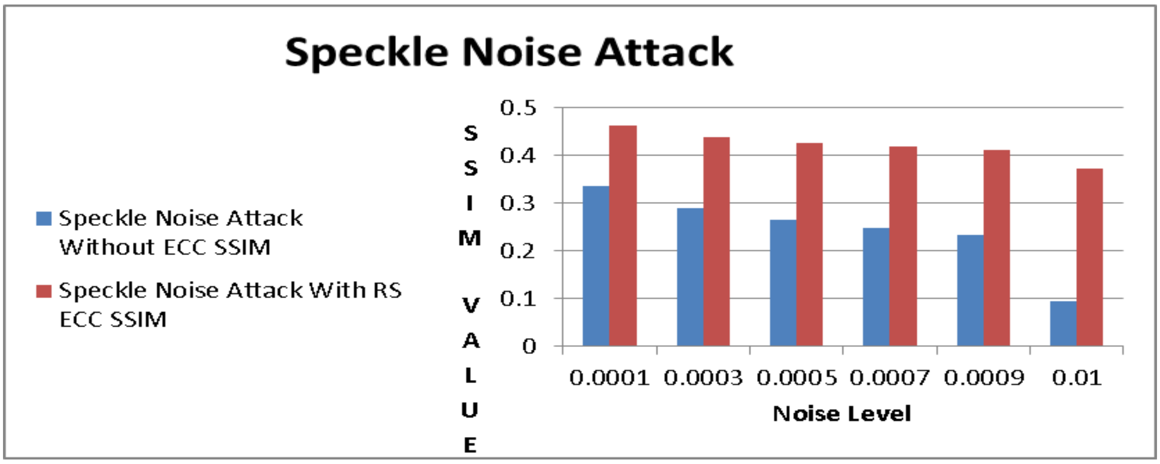

Figure 7: SSIM Values / Noise Level with RS ECC & Without ECC

3.Scenario 2: Comparing between RS ECC with different rates

In this section, we investigate the robustness improvement gained by using powerful family of error correcting codes named Reed-Solomon block codes of length n=255 over the Galois field GF2^8 with different code rates,

k=135,165,175,183,191,205,225&233.

The watermarked image was subjected to three different attacks, addition of Salt & Pepper noise, and addition of Gaussian noise and addition of Speckle noise in DWT L3.

Table 2 gives the results obtained when the watermarked image was subjected to the addition of Salt & Pepper Noise Attack, Gaussian noise Attack, and Speckle Noise Attack for different RS code rates (k), in L3-DWT level.

Table 2: PSNR & SSIM /k (RS) for three attacks

k	Salt & Pepper Attack		Gaussian Noise Attack		Speckle Noise Attack	
	PSNR	**SSIM**	**PSNR**	**SSIM**	**PSNR**	**SSIM**
135	34.51176	0.95655	34.51176	0.3521	34.51176	0.54815
165	34.19876	0.954655	34.19876	0.354142	34.19876	0.558767
175	34.09614	0.896696	34.09614	0.353491	34.09614	0.559498
183	33.9816	0.887883	33.9816	0.352017	33.98168	0.55948
191	33.88936	0.641625	33.88936	0.354138	33.88936	0.557081
205	33.72112	0.473849	33.72112	0.353348	33.72112	0.558032
225	33.52062	0.444321	33.52062	0.350088	33.52063	0.563479
233	33.46185	0.440716	33.46185	0.352456	33.46185	0.562944

It can be observed that, for different k values, the PSNR variation is very small and is limited between 33 & 34 dB in all the three noise types.

In order to compare the performance of each RS code, under each type of noise attack, the following results are obtained.

- **Salt & Pepper Attack**

For this type of noise, it can be observed from Table 2, that the eight RS ECC codes used can be arranged, with the best code in the beginning as follows:

$\boldsymbol{RS(255,165)}$, $\boldsymbol{RS(255,191)}$, $\boldsymbol{RS(255,175)}$, $\boldsymbol{RS(255,205)}$, $\boldsymbol{RS(255,233)}$, $\boldsymbol{RS(255,135)}$, $\boldsymbol{RS(255,183)}$, $\boldsymbol{RS(255,225)}$.

This result is illustrated in Figures 8a&b.

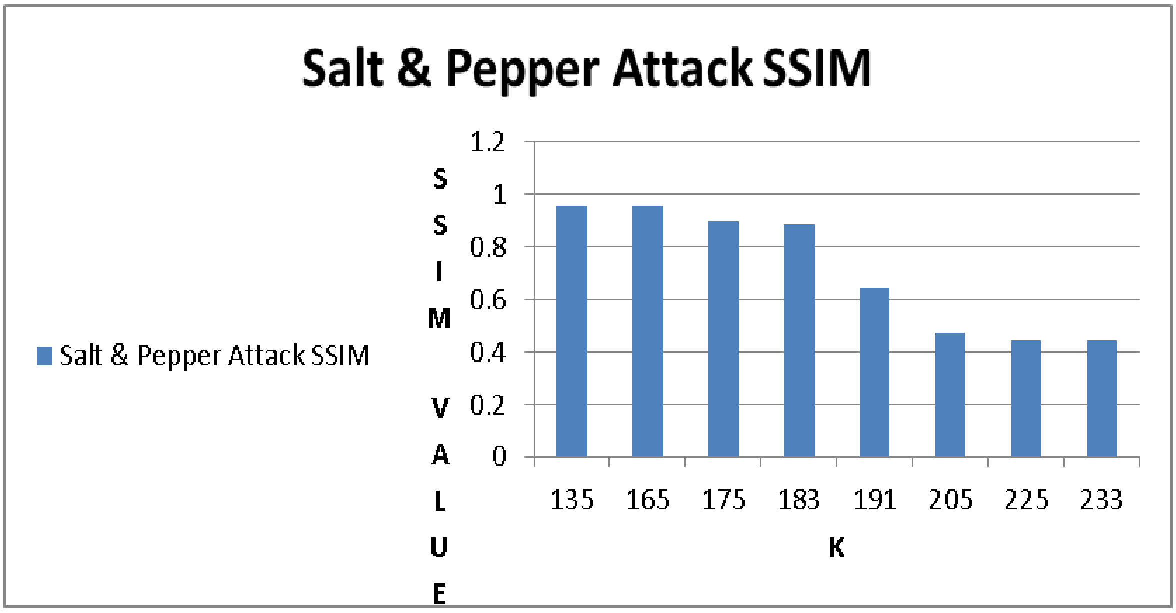

Figure 8(a): SSIM Values with RS in DWT L3

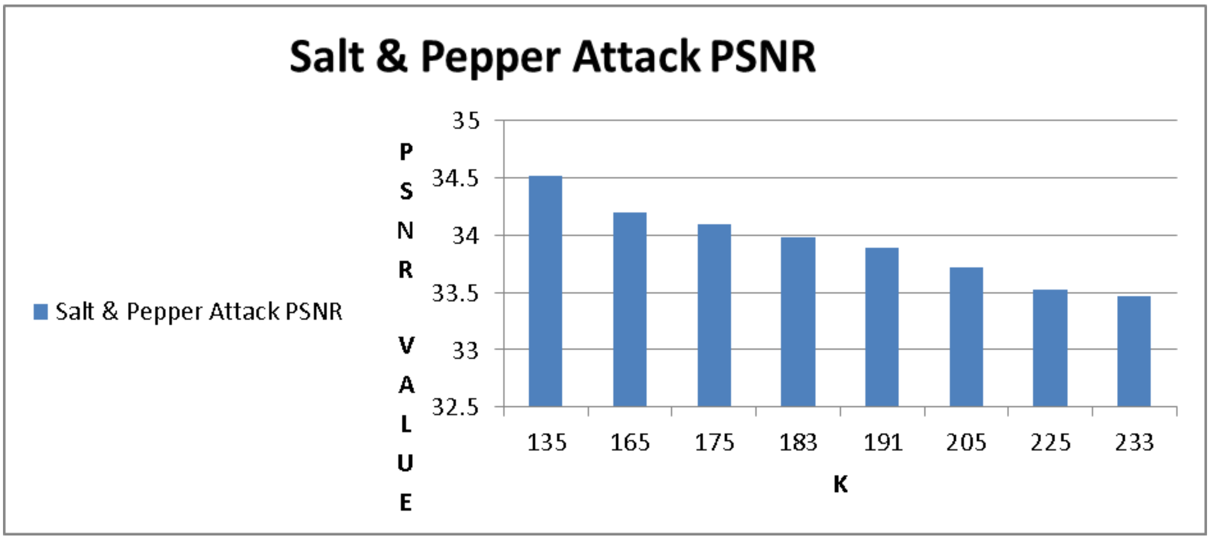

Figure 8(b): PSNR Values with RS in DWT L3

- **Gaussian Noise Attack**

For this type of noise, it can be observed from Table 2, that the eight RS ECC codes used can be arranged, with the best code in the beginning as follows:
$\boldsymbol{RS}(\mathbf{255},\mathbf{225})$, $\boldsymbol{RS}(\mathbf{255},\mathbf{233})$, $\boldsymbol{RS}(\mathbf{255},\mathbf{175})$, $\boldsymbol{RS}(\mathbf{255},\mathbf{183})$, $\boldsymbol{RS}(\mathbf{255},\mathbf{165})$, $\boldsymbol{RS}(\mathbf{255},\mathbf{205})$, $\boldsymbol{RS}(\mathbf{255},\mathbf{191})$, $\boldsymbol{RS}(\mathbf{255},\mathbf{135})$.

This result is illustrated in Figures 9a&b.

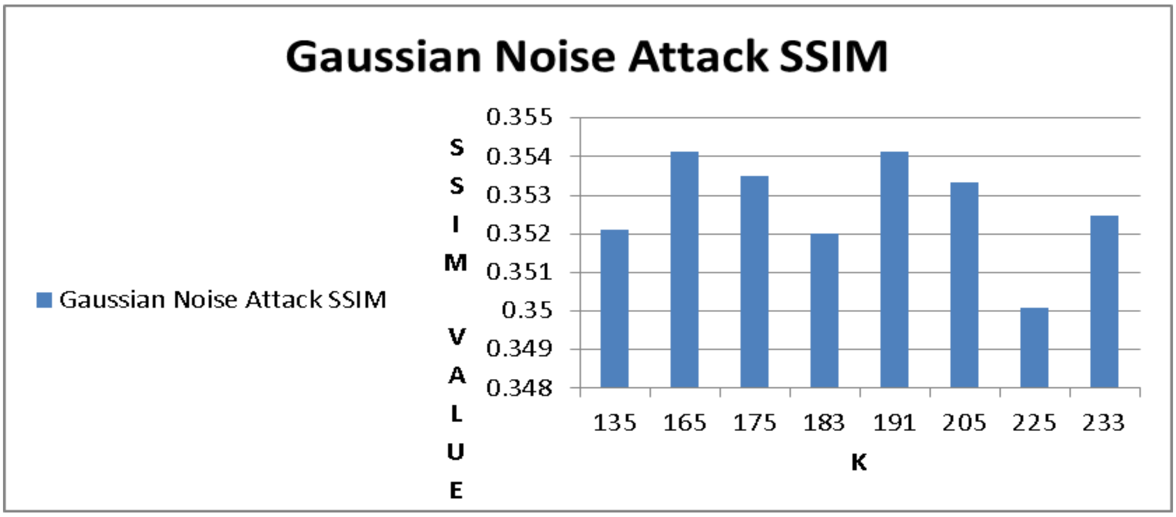

Figure 9(a): SSIM Values with RS in DWT L3

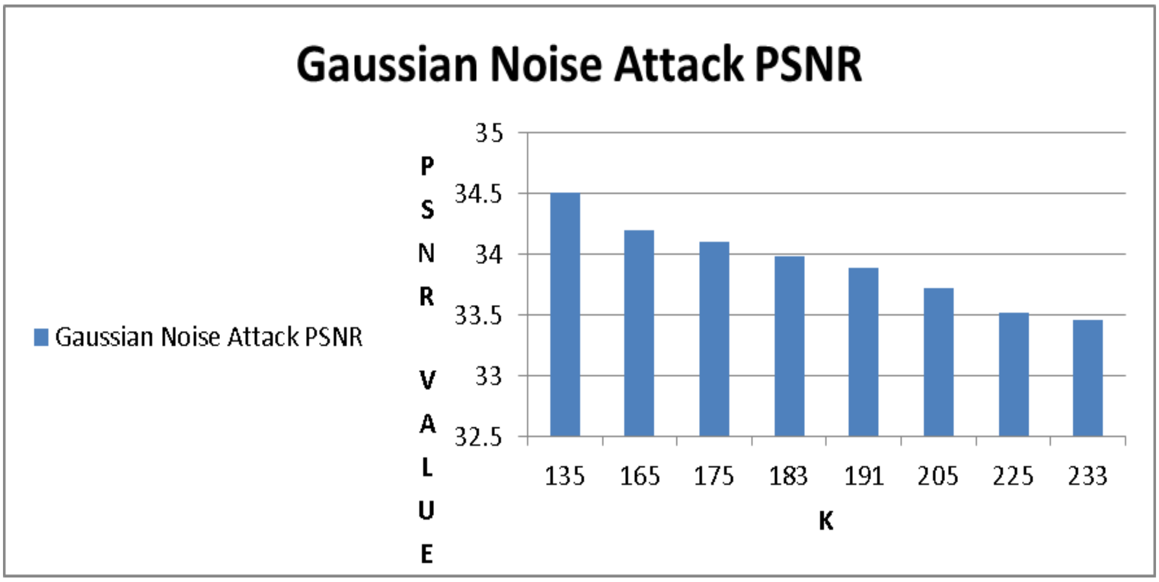

Figure 9(b): PSNR Values with RS in DWT L3

- **Speckle Noise Attack**

For this type of noise, it can be observed from Table 2, that the eight RS ECC codes used can be arranged, with the best code in the beginning as follows:
$\boldsymbol{RS}(\mathbf{255},\mathbf{225})$, $\boldsymbol{RS}(\mathbf{255},\mathbf{233})$, $\boldsymbol{RS}(\mathbf{255},\mathbf{175})$, $\boldsymbol{RS}(\mathbf{255},\mathbf{183})$, $\boldsymbol{RS}(\mathbf{255},\mathbf{165})$, $\boldsymbol{RS}(\mathbf{255},\mathbf{205})$, $\boldsymbol{RS}(\mathbf{255},\mathbf{191})$, $\boldsymbol{RS}(\mathbf{255},\mathbf{135})$.

This result is illustrated in Figures 10a&b.

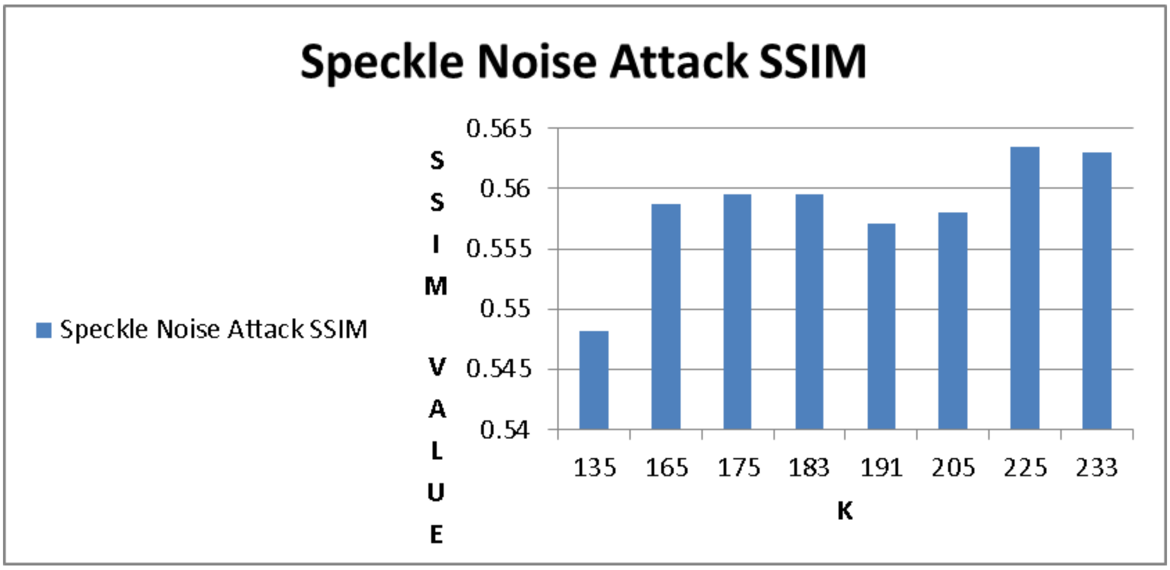

Figure 10(a): SSIM Values with RS in DWT L3

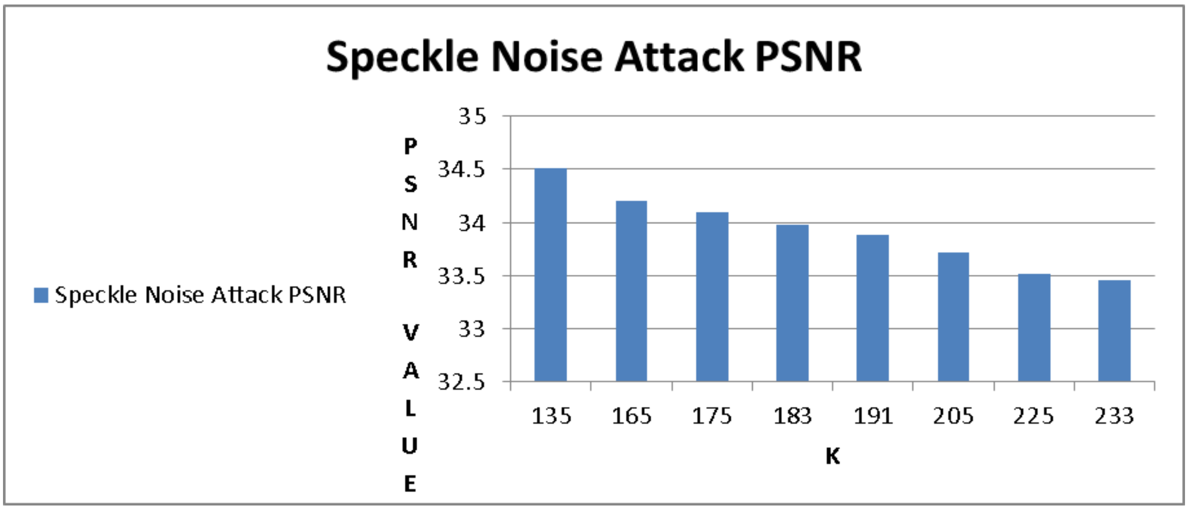

Figure 10(b): PSNR Values with RS in DWT L3

4-Conclusions

Many models and algorithms have been designed to address copyright problems. This paper dealt with the invisible digital watermarking where the mark is a digital image (LOGO) of Aden University, and the cover is another commonly used digital image (Lenna). The research investigated the performance the well-known Digital Wavelet Transform (DWT) in conjunction with the technique of block error control coding classes, RS under various well-known attacks. The enhanced methodology, presented and implemented in this research, achieved a very good performance. Regarding the significance of using error correcting codes, in conjunction with DWT transform digital image watermarking, it was shown that, in all cases investigated for all the attacks considered, there was an increase in the robustness of the digital watermark, in terms of the performance measure SSIM values. In some cases, it improves to almost 27 times the case without using error correcting codes. Among each class of codes, for all the attacks, Reed-Solomon block codes of length $\mathbf{n = 255}$ over the Galois field $\mathbf{GF(2^8)}$ with$\mathbf{k = 135}$, performs better than all others, which is supported by the theory of error correcting codes.

References

1. Chandan Kumar, A. K. Singh & ,P. Kumar,2018,“Improved Wavelet-Based Iimage Watermarking Through SPIHT”, Multimedia Tools and Applications volume 79, pages11069–11082 .
2. Clark, Jr., George C.; Cain, J. Bibb (1981), “Error-Correction Coding for Digital Communications”., New York, USA: Plenum Press, ISBN 0-306-40615-2. ISBN 978-0-306-40615-7.
3. Dennis Wong M.L., Antionette W.T. Goh, and Hong Siang Chua,2009 , “Medical Image Authentication Using DPT Watermarking: A Preliminary Attempt”, ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering , PP. 42–53.
4. Devasis Pradhan,2017“Implementation of Invisible Digital Watermarking Technique For Copyright Protection Using DWT SVD and DCT”, International Journal of Advanced Engineering Research and Science (IJAERS) ,Vol-4, Issue-7.,PP 220–240.

5. Furht B., Muharemagic E. and Socek D., 2005, “Multimedia Encryption And Watermarking”, Springer US, PP.195-197.
6. Heba Abdul Jaleel Al-Asadi,2017,” Watermarking Algorithm Based On Discrete Wavelet Transform Using Two Types Of Images”, International Journal of Science, Engineering and Technology Research (IJSETR),Volume 06, Issue 05, ISSN: 2278 -7798.
7. Hwai-TsuHua,Ling-YuanHsub,Hsien-HsinChoua,2020.“An improved SVD-based Blind Color Image Watermarking Algorithm With Mixed Modulation Incorporated”, Information Science, Volume 519, Pages 161-182 .
8. Jong Jin Chae, Debargha Mukherjee, and Manjunath B. S.,1998, " A robust Embedded Data From Wavelet Coefficients". In Proceedings of the SPIE, Electronic Imaging, Storage and Retrieval for Image and Video Database, volume 3312, pages 308 – 317, San Jose, CA, USA.
9. Martin Zlomek, 2007 .“Video Watermarking”, master thesis, Charles University in Prague.
10. Maurice F. Aburdene and Thomas J. Goodman,2005,”The Discrete Pascal Transform and Its Applications”, IEEE Signal Processing Letters, Vol. 12, No. 7,PP 304– 318.
11. Mohanty S. P., 1999, “Digital Watermarking : A Tutorial Review”, volume 132 pp. 221_237.
12. Piper A., Naini R. S., 2009, “How to Compare Image Watermarking Algorithms”, Transactions on Data Hiding and Multimedia Security IV, PP1-28.
13. Su, Q., Niu, Y.,Wang, G., Jia, S. and Yue, J., (2014). “Color Image Blind Watermarking Scheme Based on QR Decomposition,”Signal Processing, Vol. 94, No. 1, pp. 219_235 .
14. Wicker, Stephen B. (1995). “Error Control Systems for Digital Communication and Storage. Englewood”Cliffs, NJ, USA: Prentice-Hall. ISBN 0-13-200809-2. ISBN 978-0-13-200809-9.
15. Zear A, Singh AK, Kumar P,(2018), “A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine”. Multimedia Tools and Applications , Vol 77(4):4863–4882,
16. Zhao F., Huang Q., Gao W., 2006 ,“Image Matching By Normalized Cross-Correlation”, IEEE, volume 312, pages 310 – 318.

تقنية محسّنة للعلامات المائية الرقمية باستخدام تحويل المويجات المنفصلة متعدد المستويات ورموز تصحيح الخطأ

[1]محسن حسين محمد, [1]منية عبدالله أحمد و [2]عدنان عبدالله زين
[1] قسم التكنولوجيا والمعلومات، كلية الهندسة، جامعة عدن.
[2] قسم الاتصالات الالكترونية، كلية الهندسة، جامعة عدن.
DOI: https://doi.org/10.47372/uajnas.2020.n2.a08

الملخص

جذبت العلامات المائية الرقمية انتباه الباحثين بسبب تطبيقاتها المفيدة، وعلى مدى العقود الماضية، بُذلت جهود كبيرة لتطوير تقنيات وخوارزميات العلامات المائية الرقمية. تستخدم معظم الأبحاث تقنيات تحويل مختلفة لتعزيز متانة وجودة العلامة المائية المستخرجة. تقدم هذه الورقة تقنية محسّنة للعلامة المائية للصور الرقمية بناءً على التحويل المويجي المنفصل متعدد المستويات (DWT) جنبًا إلى جنب مع أكواد RS المعروفة على الحقول المحدودة. لملاحظة وتقدير أهمية استخدام تقنية أكواد تصحيح الأخطاء لتحسين أداء العلامة المائية الرقمية ضد الهجمات، تم إجراء سلسلة من التجارب. المنهجية المحسنة المقدمة والمنفذة في هذا البحث حققت أداءً جيدًا للغاية. فيما يتعلق بأهمية استخدام أكواد تصحيح الأخطاء بالتزامن مع العلامة المائية لتحويل الصورة الرقمية DWT؛ تبين أنه في جميع الحالات التي تم التحقيق فيها، بالنسبة لجميع الهجمات التي تم النظر فيها، كانت هناك زيادة في متانة العلامة المائية الرقمية، من حيث قيم قياس الأداء .SSIM في بعض الحالات، يتم تحسين الحالة إلى ما يقرب من 27 مرة دون استخدام أكواد تصحيح الأخطاء. من بين كل فئة -Reed Solomon من الرموز، بالنسبة لجميع الهجمات ذات الطول.

$n = 255$ الحقل Galois $GF(2^8)$ with $k = 135$

بأداء أفضل من جميع الرموز الأخرى.

الكلمات المفتاحية: تحويل المويجات المنفصل، وضع العلامات المائية على الصورة، رموز تصحيح الخطأ، تضمين العلامة المائية، استخراج العلامة المائية.