Localization Watermarking for Authentication of Text Images in Quran

with Spiral Manner Numbering

Syifak Izhar Hisham
Faculty of Computer Science and Software Eng.
Universiti Malaysia Pahang
Gambang, Malaysia
penawar85@gmail.com

'Afifah Nailah Muhammad
Information Technology and Communication Dept.
Politeknik Ungku Omar
Ipoh, Malaysia
anailah@puo.edu.my

Jasni Mohamad Zain
Faculty of Computer Science and Software Eng.
Universiti Malaysia Pahang
Gambang, Malaysia
jasni@ump.edu.my

Gran Badshah
Faculty of Computer Science and Software Eng.
Universiti Malaysia Pahang
Gambang, Malaysia
gran16178@gmail.com

***Abstract*— The phenomenon of widespread usage of smart phone has encouraged many android applications to be produced, by free or paid. Nowadays, with the trend of communicating through social networking applications and social networking sites, Muslims tend to share the image of verse from the Quran applications to the sites. Several concerns regarding security and copy control of the verse text image have aroused, and among the solution to this issue is watermarking. This paper has conducted a research proposing an authentication fragile watermark with spiral manner which shows a good numbering system of embedding. The watermarking scheme is imperceptible and can embed high capacity of data. The average Peak-signal-of-Noise-Ratio (PSNR) value of embedded image is 67.06dB and the average operating time is 1.29 seconds. Subsequently, it proposed a localization and restoration watermarking scheme to be applied in the Quran application as a function before sharing.**

Keywords- Quran application, watermarking; attacks; security; localization; recovery

I. Introduction

The increased and widespread usage of smart phone has encouraged many android applications to be produced, by free or paid. The holy Quran is among the popular application to be installed. With the technology moves on, and with increasing people are using smart phone nowadays, the applications are widely used and become popular. Nowadays, there are several Quran android applications that provide sharing verse feature which able to connect directly to social networking sites and social networking applications such as Facebook, Twitter, Whatsapp and Instagram.

The main motivation of this research focuses on the importance of the validity, integrity and security of electronic-format images of the Holy Quran. It is our concern that nowadays, there are vast activities of sharing the holy verse of Quran through the Internet and other social networking android applications, without being equipped with security system. The reason why text in Quran is important to be protected is because the text feature has various small symbols, lines and dots of letters, which even one small item is interrupted, the meaning can be misleading.

Mistakes, alterations and errors in shared Quran digital images may arise accidentally from the sharing activity or purposely by enemy of Islam. In one hand, we try to stop any attempt of producing incorrect meaning of verses or alterations.

Watermarking is in need as one of the method to control the problem issued. The aim is to verify the integrity and authenticity of data of Quran. Watermarking techniques can be classified according to how the watermark is embedded, which mainly are embedding in spatial domain and transform domain of the image [1]. The embedding technique in spatial domain does not produce serious distortion to the original image; however, it is usually fragile and rarely survives various attacks. Watermarking in transform domain is known to survive possible compression and more robust against geometric transformation [2].

Most image watermarking schemes try to meet the following requirements; perceptibility, robustness, capacity and computational complexity [3, 4, 5]. Though, for fragile watermarking, purposely not being robust can be an advantage for authentication purpose. If a fragile watermark is detected correctly in an image, it can be assumed that the image has not been altered or tampered since the watermark has been embedded [6].

The proposed watermarking in this paper is an enhancement from the Authentication Watermarking with Tamper Detection and Recovery (AW-TDR) by [7]. The contribution of this method is the integration of six concepts; block-based [8], separating authentication bits and recovery [9], hierarchical [10], average intensity as image feature [11], LSB embedding [12], and one dimensional transformation [7].

The proposed watermarking scheme capacity is high. It embeds all authentication data all over the image, regardless region-of-interest (ROI) or region-of-non-interest (RONI). This is to guarantee all data has authentication bits and recovery bits if one of the area is attacked or modified. The purpose is to ensure localization works at all data, as the fragility purpose is not to protect the data like robust watermarking, but to be alert with the altered location in the image. The spiral numbering method has a better distribution of embedded recovery bits.

The method is efficient, simple and able to operate in short time, which is a requirement to be run on the internet. It only uses simple operations for the authentication, which are parity check approach and comparison between average intensities approach. It is effective as the scheme inspects the image twice with the inspection view increasing to a bigger block. With this, the accuracy of tamper localization can be ensured.

This scheme can perform both tamper detection and recovery for tampered images. Tamper detection is achieved through a block-based inspection of authentication bits with double checking. Recovery process is achieved by retrieving the recovery bits embedded in the LSB. It relies on its hidden information in another block that can be determined by a one dimensional transformation.

In the next section, the proposed method of spiral manner numbering techniques is presented. It is proven good by the calculation in the preliminary result [13] and from the achieved result of detection and recovery rate in Section 3. In Section 4, conclusion is made with some remarks.

II. Materials and Methods

The watermarking process is divided into two phases: (1) numbering and mapping, and (2) embedding. The process of authentication verification is done by undergoing the detecting phase. The samples tested in this testing are taken from the top four of android application for Quran. The top four is determined by the most downloaded by android users.

A. Numbering and Mapping

The proposed technique starts with numbering by the spiral manner. The scheme is to make sure the recovery bit of each original block will be embedded as far as possible to make sure although the image has been attacked with any vast attack, the recovery bit still can survive and the image is recoverable. The idea is the spiral numbering is a good numbering process which can ensure watermarked blocks are relocated a minimum distance away from the original blocks, thus, the watermark bits still survive from the tamper [13].

The blocks of rows and columns are divided by two to decide the central block of the image. Starting at the centre, numbering is done in spiral manner. Then each block is mapped (watermark embedding) using equation;

$$B = [(k \times s) \bmod Nb]+1, \quad (1)$$

where B is the watermarked block, s is spiral, Nb is block numbers, and k is the secret key which is the highest prime number from the result of block numbers divided by 2. As it works in spiral manner, which start at the centre, the image processed should be in square size to ensure all the blocks are numbered.

The following algorithm describes how to number the image blocks in spiral manner [13, 14]:

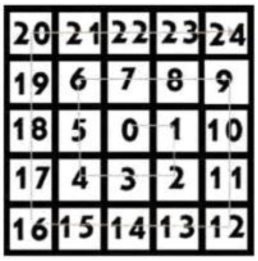
1) The block size is set. Blocks per row and blocks per column is calculated based on the width and the height of the image; (Height/block size, Width/block size).

2) The key number is set; (k=max(primes (numblock/2))).

3) Coordinate for each block is calculated [8, 9] to get the central block; [column- centre of columns, row-centre of rows]. Number the block from the centre in spiral manner.

4) Ring level of the blocks is determined, such as level 1 is for sequence number from number 0 until 8, level 2 is for sequence number from number 9 until 24, and so on (Fig. 1). From level, we could calculate the first number and last number of each level.

5) After all blocks is numbered in spiral manner, each block is mapped (watermark embedding) using equation (1).



20	21	22	23	24
19	6	7	8	9
18	5	0	1	10
17	4	3	2	11
16	15	14	13	12

Fig. 1. Spiral numbering starting from the centre; showing the ring level

B. Embedding

In this phase, a case of using intensity average comparisons and parity bits as the authentication watermark is presented. To localize tamper in a block, the watermark needs to be embedded directly into that block. If a block is being tampered locally, the intensities of the pixels involved will be changed. This will also change the average intensity of the block concerned. To ensure that this is not changed, a parity check will be used. However, a parity check alone will not guarantee that the block has not been changed, because local tampering usually causes burst error [15], meaning that if more than one bit has been changed, a parity check is no longer useful.

To overcome this, the intensity comparison is used as another guard if a parity check fails. This feature will also be used to break block wise independence. To break block wise independence, the intensity of the block is compared to the intensity of a larger block. Let B denote the bigger block and the smaller or sub block as Bs as shown in Fig. 2.

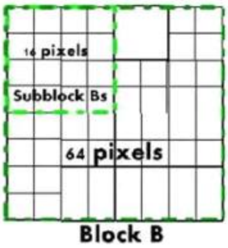


Fig. 2. B denotes the bigger block and Bs as the smaller sub block

For each block B of 8 x 8 pixels, we divide it into four sub-blocks of 4 x 4 pixels. The following algorithm describes how the 3-tuple watermark of each sub-block is generated and embedded:

1) Set the LSB of each pixel within the block of B to zero.

2) Calculate the average intensity of the block, Avg_ B and each of its sub-blocks, Avg Bs, respectively.

3) Generate the authentication watermark, v, of each sub-block.

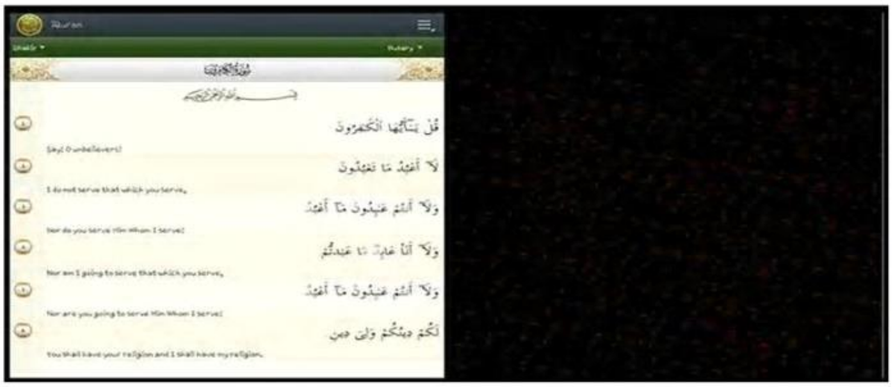
4) Generate the parity check bit, p, of each sub-block.

5) From the mapping sequence done at the first phase, obtain original image, A, whose recovery information will be stored in block B.

6) Again, compute the average intensity of each sub-block (As) within A, Avg_As.

7) Obtain the recovery intensity, r, of As by taking the seven MSBs in Avg_As.

8) Embed the 3-tuple watermark (v, p, r), each in one LSB of each pixel in Bs.



قُلْ يَٰٓأَيُّهَا ٱلْكَٰفِرُونَ

Say: O unbelievers!

لَآ أَعْبُدُ مَا تَعْبُدُونَ

I do not serve that which you serve,

وَلَآ أَنتُمْ عَٰبِدُونَ مَآ أَعْبُدُ

Nor do you serve Him Whom I serve:

وَلَآ أَنَا۠ عَابِدٌ مَّا عَبَدتُّمْ

Nor am I going to serve that which you serve,

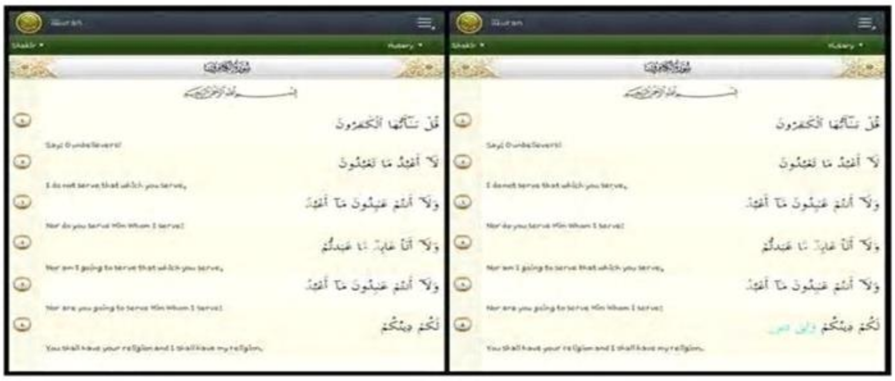
وَلَآ أَنتُمْ عَٰبِدُونَ مَآ أَعْبُدُ

Nor are you going to serve Him Whom I serve:

لَكُمْ دِينُكُمْ وَلِىَ دِينِ

You shall have your religion and I shall have my religion.

Fig. 3. (From left) The original text image; The embedded watermark in bits



قل يا أيها الكافرون

Say; O unbelievers!

لا أعبد ما تعبدون

I do not serve that which you serve,

ولا أنتم عابدون ما أعبد

Nor do you serve Him Whom I serve;

ولا أنا عابد ما عبدتم

Nor am I going to serve that which you serve,

ولا أنتم عابدون ما أعبد

Nor are you going to serve Him Whom I serve:

لكم دينكم

You shall have your religion and I shall have my religion.

قل يا أيها الكافرون

Say; O unbelievers!

لا أعبد ما تعبدون

I do not serve that which you serve,

ولا أنتم عابدون ما أعبد

Nor do you serve Him Whom I serve;

ولا أنا عابد ما عبدتم

Nor am I going to serve that which you serve,

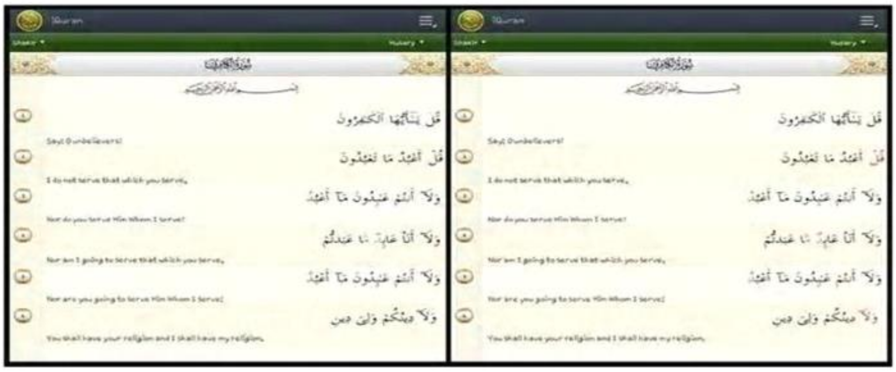
ولا أنتم عابدون ما أعبد

Nor are you going to serve Him Whom I serve:

لكم دينكم ولي دين

You shall have your religion and I shall have my religion.

Fig. 4. (From left) The tampered image; The detected areas in blue



قل يا أيها الكافرون

Say; O unbelievers!

قل أعبد ما تعبدون

I do not serve that which you serve,

ولا أنتم عابدون ما أعبد

Nor do you serve Him Whom I serve;

ولا أنا عابد ما عبدتم

Nor am I going to serve that which you serve,

ولا أنتم عابدون ما أعبد

Nor are you going to serve Him Whom I serve:

ولا دينكم ولي دين

You shall have your religion and I shall have my religion.

قل يا أيها الكافرون

Say; O unbelievers!

قل أعبد ما تعبدون

I do not serve that which you serve,

ولا أنتم عابدون ما أعبد

Nor do you serve Him Whom I serve;

ولا أنا عابد ما عبدتم

Nor am I going to serve that which you serve,

ولا أنتم عابدون ما أعبد

Nor are you going to serve Him Whom I serve:

ولا دينكم ولي دين

You shall have your religion and I shall have my religion.

Fig. 5. (From left) The tampered image; The detected areas in red.

TABLE 1. COMPARISON WITH OTHER USED WATERMARKING METHODS IN DIGITAL TEXT OF QURAN IMAGES.

Method	Average PSNR Value (dB)	Average Processing Time (s)	Detection	Recovery
Spiral Manner Numbering	67.06	1.29	Yes	Yes
Enhanced SVD Technique [16]	44.60	0.98	Yes	No
Discrete Wavelet Transform (DWT) [17]	49.06	Not stated	Yes	No

III. RESULT AND DISCUSSION

From algorithm applied, our results show that the block spiraling and starting the numbering in the middle will have a greater chance of recovery, comparing with a scheme by [16, 17, 18]. A page of Surah Al-Kafiruun in a Quran android application is shown in Fig. 3 as one of the samples. The image underwent the watermarking process, and the embedded data is shown in red in Fig. 3. This scheme embeds the watermark in spatial domain, which is in the LSB of the image pixels. It is imperceptible as it does not produce serious distortion to the original image [19].

In Fig. 4, we erased the last word of the sixth verse which covers 211 blocks area. Two-level detection is then performed. We managed to detect the tamper and marked it in blue, as shown in Fig. 4. We managed to recover the missing word and get back the real verse. The operating time of detecting and recovery is 1.99 seconds.

For the second tamper, we cloned two first words of second verse and sixth verse, shown in Fig. 5. The tamper area is 349 blocks in total. The detection feature managed to localize and mark both tampers in red. Plus, it is also recoverable. The elapsed time of detection and recovery is 2.34 seconds, which is the longest operating time among all tests. From the various attacks purposely done in the tests, the most intensive attacks are compression, blur filter and clone attack. Other tested attacks are Noise, Emboss, and Crystallize filter, crop, paint and line removal technique, Mosaic effect, and JPEG compression.

Table 1 shows the comparison with other used watermarking methods in digital text of Quran images. The tests are done with 70 samples of Quran text image. The average operating time for this spiral numbering method is 1.29 seconds. The time taken is in the range of 0.2 to 2.5 seconds. The average PSNR value is 67.06dB, with the highest value is 80dB. The lowest PSNR value is produced by the image that has been compressed. It is proven that compression is among the great alteration. Comparing with another two studies [16, 17], this spiral numbering can be claimed as better as the PSNR value is much higher and it has another added feature which is recovery.

As the holy Quran exists in original version, it is less important for the recovery process to be done since we can refer to the original contents. The most important process is to determine whether there is any attack to the verse shared in the internet. However, this scheme is also enhanced with recovery feature as it is very helpful to have recovery process for the user to simply know what the true verse of the verses is.

After doing comparison test, the proposed scheme in this paper proved that the detection and recovery rate is better than the scheme proposed by [7]. Although the elapsed time is similar, the spiral manner numbering can lead up to 100% detection rate and recovery. From the results, there is no issue to recover small and huge tamper, spread tamper and various filter attacks. It is proven if we tamper with small block anywhere in the image, with the spiral method, we can protect the embedded watermark bits that contain the authentication and recovery bits.

The usage of block average intensity in tamper localization is proven as easy to perform without much computation needed [20]. The times taken in each experiment were short. Although there is an argument saying that in countering several great attacks, average intensity cannot maintain the performance of 100% recovery, but the recorded performance is up to 99.99% [20].

IV. CONCLUSION

The proposed watermarking scheme is imperceptible and fragile. The PSNR value is high when comparing the original image and watermarked image. It can embed high capacity of data in the image as it is able to embed one full image data in the image LSB itself. It is an enhanced scheme that can localize tamper in watermarked text image of Quran and recover the tampered image. The result is very promising with up to 100% recovery. The purpose is to verify the integrity and authenticity of Quran verse images which are usually be shared among believers in the Internet, especially in social networking sites and social networking applications. Admittedly, if we did not imply the security system for the images, there might be technical mistakes that change the meaning and integrity of the verse when it is widely spread in the Internet. Moreover, foes of Islam can attack the shared images to carry misleading meaning of the verse.

The needed work to do in the future is to integrate the proposed watermark feature to the Quran application in smart phone so that the sharing function can watermark the image of the sharing verse first before parceling out in the internet.

ACKNOWLEDGMENT

Our thanks to RESEARCH AND DEVELOPMENT DEPARTMENT OF UNIVERSITI MALAYSIA PAHANG for funding the research by PRG scheme.

REFERENCES

[1] S. C. Liew, and J. M. Zain, "A Review of Medical Image Watermarking and Its Implementations", *Proceedings of Malaysian Technical Universities Conference on Engineering and Technology (MUCEET2009)*, 20-22 June 2009, Kuantan, Pahang, Malaysia.

[2] C. Song, S. Sudirman, M. Merabti, and D. Llewellyn-Jones,"Analysis of Digital Image Watermark Attacks", *Proceedings of the 7th IEEE Consumers Communications and Networking Conference*, pp. 1-5, 2010.

[3] I. J. Cox, M. L. Miller, and J. M. G. Linnartz, "A review of watermarking principles and practices", *IEEE Digital Signal Processing for Multimedia System*,1:461-482, 1999.

[4] M. Kutter, and F. Hartung, "Introduction to watermarking techniques", *Information Techniques for Steganography and Digital Watermarking*, 1:97-119, 1999.

[5] P. Meerwald, and A. Uhl, "Watermark security via wavelet filter parameterization", *Proceedings of the International Conference on Image Processing*, pp.1027-1030, 2001.

[6] S. C. Liew, and J. M. Zain, "Reversible Medical Image Watermarking For Tamper Detection and Recovery", *Proceedings of the 3rd IEEE International Conference on Computer Science and Information Technology(ICCSIT2010)*, Chengdu,China, 9-11 July 2010.

[7] J. M. Zain, and A. R. M. Fauzi, "Medical Image Watermarking With Tamper Detection and Recovery", *The 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, New York, USA, 1-4 September, 2006.

[8] J. Fridrich, M. Goljan, and A. C. Baldoza, "New fragile authentication watermark for images", *International Conference on Image Processing (ICIP 2000)*, Sep 10-13, 2000, Vancouver, BC, IEEE Computer Society pp. 446- 449.

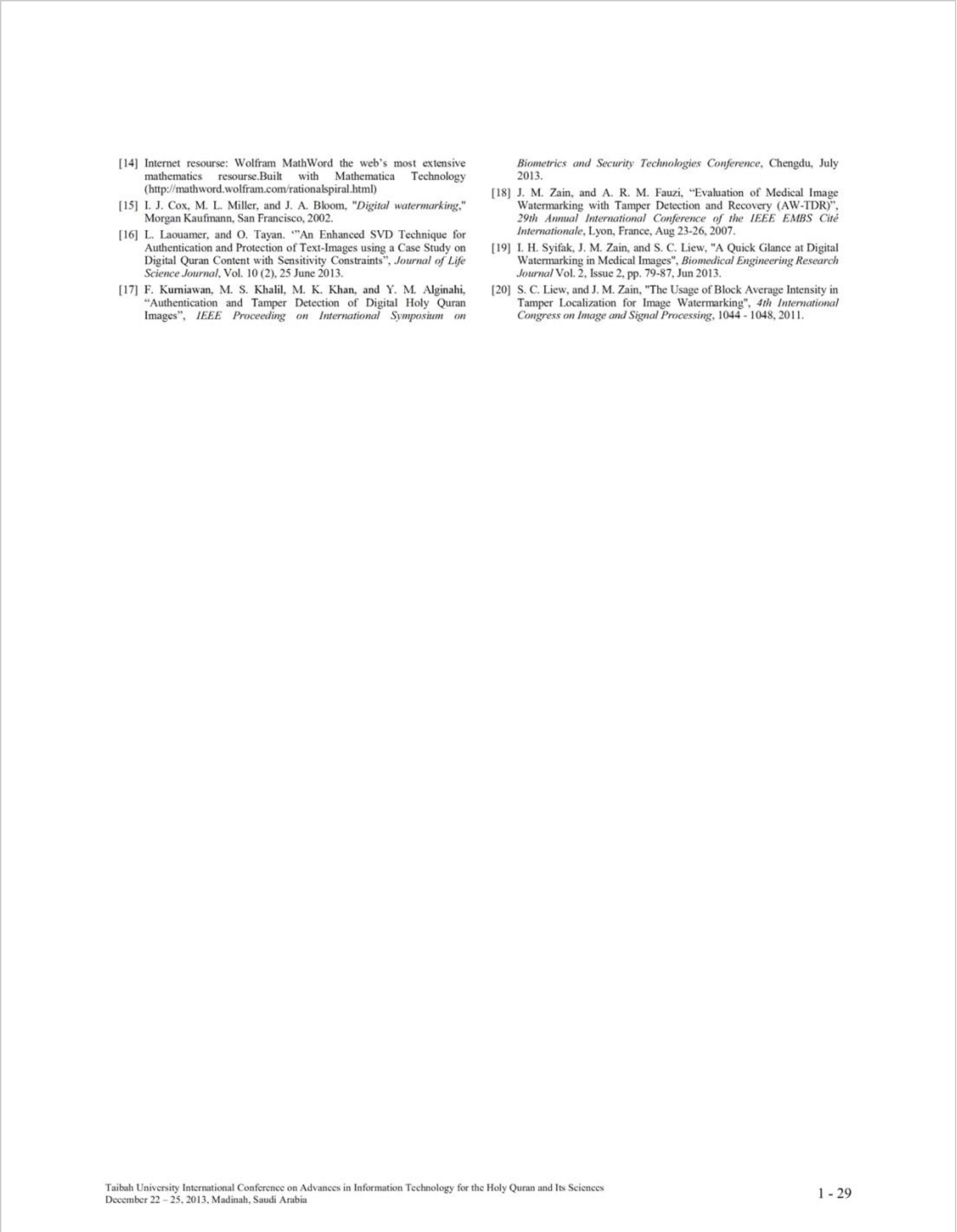
[9] C. Lin, and S. Chang, "A Robust image authentication method distinguishing JPEG compression from malicious manipulation", *IEEE Transactions on Circuits and Systems for Video Technology*,11(2),pp. 153-168, 2001.

[10] M. U. Celik, G. Sharma, and A. M. Tekalp, "Hierarchical watermarking for secure image authentication with localization", *IEEE Transactions on Image Processing*,11(6), pp.585-594, 2000.

[11] D. C. Lou, and J. L. Liu, "Fault resilient and compression tolerant digital signature for image authentication", *IEEE Transactions on Consumer Electronics*, 46(1),pp. 31-39, 2000.

[12] J. M. Zain, M. Clarke, and P. Baldwin, "The effect of reversible LSB manipulation to the quality of image", in *PREP2004*, University of Hertfordshire, April 2004.

[13] N. M. Afifah, and J. M. Zain, "Using Spiral Scan Technique for Medical Image Watermarking with Tamper Detection and Recovery", *Proc. in National Conference on Software Engineering and Computer System 2007 (NacSes 07)*, 20-21 August 2007, Cherating, Malaysia.



[14] Internet resourse: Wolfram MathWord the web's most extensive mathematics resourse.Built with Mathematica Technology (http://mathword.wolfram.com/rationalspiral.html)

[15] I. J. Cox, M. L. Miller, and J. A. Bloom, "*Digital watermarking*," Morgan Kaufmann, San Francisco, 2002.

[16] L. Laouamer, and O. Tayan. ‘”An Enhanced SVD Technique for Authentication and Protection of Text-Images using a Case Study on Digital Quran Content with Sensitivity Constraints”, *Journal of Life Science Journal*, Vol. 10 (2), 25 June 2013.

[17] F. Kurniawan, M. S. Khalil, M. K. Khan, and Y. M. Alginahi, “Authentication and Tamper Detection of Digital Holy Quran Images”, *IEEE Proceeding on International Symposium on Biometrics and Security Technologies Conference*, Chengdu, July 2013.

[18] J. M. Zain, and A. R. M. Fauzi, “Evaluation of Medical Image Watermarking with Tamper Detection and Recovery (AW-TDR)”, *29th Annual International Conference of the IEEE EMBS Cité Internationale*, Lyon, France, Aug 23-26, 2007.

[19] I. H. Syifak, J. M. Zain, and S. C. Liew, "A Quick Glance at Digital Watermarking in Medical Images", *Biomedical Engineering Research Journal* Vol. 2, Issue 2, pp. 79-87, Jun 2013.

[20] S. C. Liew, and J. M. Zain, "The Usage of Block Average Intensity in Tamper Localization for Image Watermarking", *4th International Congress on Image and Signal Processing*, 1044 - 1048, 2011.