Detection, Reconstruction, and Repairing the Distortion in Quran Pages Based on Watermarking

Afsaneh Arabzadeh[1,2], Alireza Naghsh [2,3*]
1- M.Sc. Student of Computer Architecture, Faculty of Computer Engineering, Najafabad Branch, Islamic Azad University, Najafabad, Iran.
Email: Afsaneharabzadeh68@gmail.com
2- Digital Processing and Machine Vision Research center, Najafabad Branch, Islamic Azad University, Iran.
3- Department of Electrical Engineering, Najafabad Branch, Islamic Azad University, Najafabad, Iran.
(Corresponding Author: naghsh.a@pel.iaun.ac.ir)

Received: July 2017 Revised: June 2018 Accepted: August 2018

ABSTRACT:
With the increasing exchange of information around the world and the use of telecommunication networks such as the Internet, the validity of digital documents has become very important because it may be destroyed or attacked intentionally or unintentionally. Muslims consider Quran as the most important book and so much effort has been made to protect the accuracy of this holy book. One of the proper methods to preserve Quran pages against distortion is using image watermarking in spatial domain. In digital watermarked images of Quran, the image information is used to detect and reconstruct distortions. The purpose of the presented method in this paper is to produce a robust image of the Holy Quran against cutting, destruction, and distortion using two-dimensional codes and (XOR) function. The watermarking algorithm in this method is able to recover distortions in addition to detecting them.

KEYWORDS: Watermarking, spatial domain, two-dimensional codes, Quran image, algebraic functions.

1. INTRODUCTION

In the present digital era, the validity of digital documents is very important because it may be distroyed or attacked intentionally or unintentionally. Muslims consider Quran as the most important book and so much effort has been made to protect the accuracy of this book. An important issue for Muslims is to use the information technology properly for having integrity and credibility in Quran. This technology is important to protect Quran against various attacks. The next reason is that intentional or unintentional changes of Quran are unrecognizable and it is necessary to do corrective operations in this regard. The use of smartphones and handheld devices have become a necessity for many people. Also, cell phone application and/or software developers are seeking to have a corner on the market. One of these important applications is the Qur'an software. However, some of them are suspiciousand the purpose of their production is to make fundamental distortions and attacks to destroy Muslims' unity and are widely produced and spread due to the lack of supervision and control of an official or islamic power against such malwares. Therefore, some methods are proposed to confront these types of attacks. In this paper, a fragile watermarking method is presented to protect the digital Qur'an against distortions , which detects, modifies and corrects the distorted parts of the Holy Quran. Actually, the main objective of the proposed method is the restoration of the cropped and/or distorted images. Restoration means retrieving the attacked parts of the images of Quran pages to the original image. The proposed flowchart shows the produced robust image as shown in figure 1.

2. LITERATURE REVIEW

Dueto the increasing development of communication in the present world, the need for the optimal control of communications in variousadministrative, multimedia, physical, and secure environments is evident. Data protection against copying and counterfeiting is very important. Accordingly, some techniques should be done to control copying. Watermarking is one of these methods. Watermarking means hiding the watermarking data in the host signal so that it can be detected with human eyes and only authorized personnel that are able to extract the data [1]. According to [2] and the different applications of data storage, watermarking is divided into three categories: fragile, semi-fragile, and robust watermarking. Infragile watermarking, the watermarking is easily destroyed by the slightest changes. Semi fragile method protects the information against intentional attacks, but robust watermarking is robust against various attacks.

In year 2011 projects being related to digital watermarking have been categorized into two groups based on their domains [3]: the spatial domain and

transform domain.The spatial domain requires shorter implementation time and less hardware in comparison to the transform domain and it has a great capacity for watermarking. However, this method will not last long against noise or compression attacks. The embedded watermarking in this method can be easily changed by a third party.

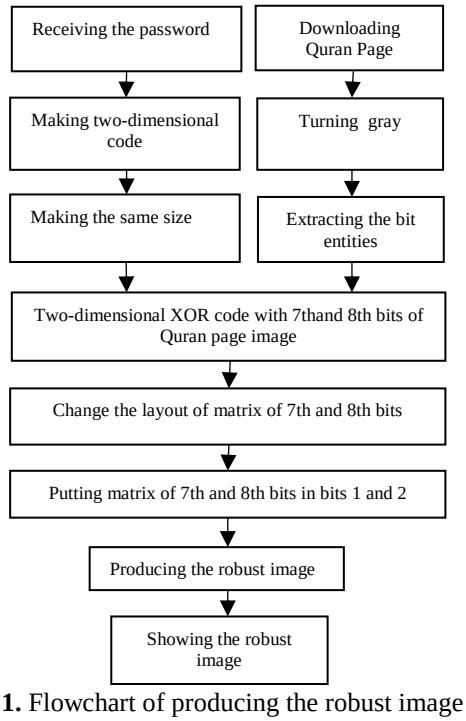


Fig. 1. Flowchart of producing the robust image

The transform domain method has been highly regarded due to its robustness against most attacks. In [4] the transform domain watermarking consists of the discrete Fourier transform, the discrete cosine transform, the discrete wavelet transform, and the discrete Fourier transform. Mousavi et al (2016) in [5] have presented a method to protect this type of image due to the expansion of digital images and maintain the accuracy of such images against authorized and unauthorized operations and/or attacks. Watermarked image quality in digital images is measured by some criteria such as signal to noise ratio, bit error rate, and measured structural similarity. Khalil et al. in [6] have proposed a strong fragile algorithm that is able to detect attacks on black and white images. In this design, a two-layer watermarking of wavelet and spatial domain are introduced to increase the sensitivity of watermarking and the ability to defend against attacks. In this method, a chaotic map is used to secure the watermarking against local attacks. This watermarking detects location changes and focuses on it. It is efficient for simple and smart attacks. Amira et al. (2010) have presented zero Watermarking algorithm. The algorithm is highly related to and comparable with Digital Signatures algorithms. Zero Watermarking is used to access the status of Quran quets and verses. In this paper, a fragile Watermarking method is proposed, which is able to detect attacks and disturbances of the gray pages without refering the original text [7].

There are two ways in [8] to hide information in the text. The first one is Line shifting, and the second one is Word shifting. In line shifting, the text lines shift up or down. In this way, the information bits are stored in the places that are suitable for image texts. The same procedure is performed in word shifting. This method is suitable for texts that the space between words are changed. In 2007, an open space method is proposed for watermarking in [9]. Embedding process is performed in the way that a white space is added to the text. This white space is situated at the end of each line, or between words, or each character. This method has the potential to be used in any arbitrary text so that it does not attract the reader's attention. Kurniawan et al. [10] have introduced a fragile watermarking algorithm that performs the embedding operation in the spatial and transform domains. In this method, the input image is sent to the frequency domain for watermarking operations. Therefore, the proposed method is robust against attacks because there is a correlation between watermarking blocks. significant hidden bits in wavelet coefficients makes this method safe against local attacks. Experimental results show that this method can produce an image with great quality based on the standards of image quality. In 2014, a fragile Watermarking algorithm is proposed that works on preserving the accuracy of digital Qurans. This method works on the spatial domains and wavelet of the digital images of the Quran. The authentication bit in each block is embedded by the image wavelet transform. Then, the least significant bit of pixels are considered to be embedded in other authentication bits [11].

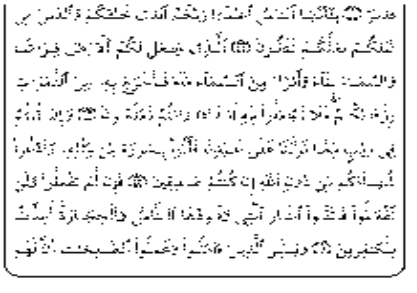
Farmani et al In 2011, described implementation of a high-speed encryption algorithm with high throughput for encrypting the image.Therefore, an almost safe AES encryption algorithm (Advanced Encryption Standard) has been selected to increase the speed and power using the pipeline method in four steps, the control unit based on logical gates, the optimal design of multiple blocks in the mixcolumn phase And at the same time, the keys to production and the rounds.Such procedure makes AES suitable for fast image encryption. Implementation of a 128-bit AES on FPGA of Altra company has been done and the results are as follow: throughput, 6 Gbps in 471MHz. The time of encrypting in tested image with 32*32 size is 1.15ms, [12]. Information is significant in every aspect of human life. Like any other property, it needs protection. There are different cryptographic algorithms available to secure information. However, most of them are computationally intensive, either deals with huge numbers and complex mathematics or involves several iterations. Advanced Encryption

Standard (AES) is a cryptography algorithm proved to have the best quality between 15 candidates by National Institute of Standards and Technology (NIST). AES has high security with relatively little memory and CPU resource requirements. This paper describes the implementation of a low power and high-speed encryption algorithm with high throughput for encrypting the image. Therefore, it's been chosen a highly secured symmetric key encryption algorithm AES (Advanced Encryption Standard), in order to decrease the power using retiming and glitch and operand isolation techniques in four stages, control unit based on logic gates, optimal design of multiplier blocks in mixcolumn phase and simultaneous production keys and rounds. Such procedure makes AES suitable for fast image encryption. Implementation of a 128-bit AES on FPGA of Altera Company has been done, and the results are as follows: throughput, 6.5 Gbps in 441.5 MHz and 130mw power consumption. The time of encrypting in tested image with 32*32 sizes is 1.25ms [13].

3. ROBUSTING QURAN IMAGES AGAINST DISTORTIONS

3.1. Producing robust images

Watermarking methods are used in the spatial domain to produce a robust image of Quran against cutting, disturbances and/or attacks using two-dimensional codes and algebraic functions. At first,one page of Quran, which does nothave any attack or distortion is recievedandits bit components are obtained. Then, the 7th and 8th matrix bits that contain the maximum amount of information among eight bits of the image are divided into four parts, and we produce these four parts of the original matrix with a new matrix layout as shown in Figure 2 and 3.



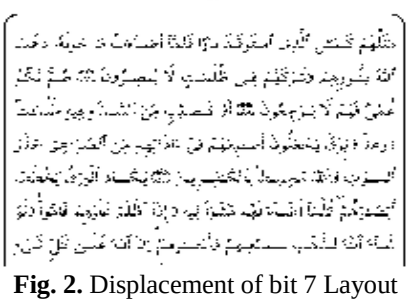


Fig. 2. Displacement of bit 7 Layout

Fig. 3. Displacement of bit 8 Layout

A two-dimensional code generation algorithm of this software uses the number of Quran pages as the code number, generates a two-dimensional code(Fig. 4). Afterwards, the same size matrix with the original image received by 4 barcodes is generated that contains 4 barcodes that the size of the image is the same as the size of Quran pages (Fig. 5).

Fig. 4. The two-dimensional code

Fig. 5. generating the same size images of the original image

In the next stage, the changed matrix of the seventh and eighth bits will have the same size image seperately from the two-dimensional code and the original image by xor function (Fig. 6 and 7). Then, the obtained two matrices from xor function are located instead of the first and second bits of the original image and a robust image of the Quran is obtained (Fig. 8).

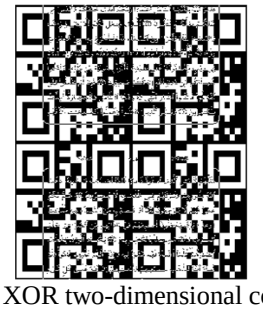


Fig. 6. The XOR two-dimensional code image with the seventh bit

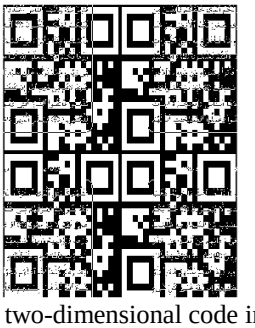


Fig. 7. The xor two-dimensional code image with the eighth bit

Fig. 8. Generating robust image page

3.2. Image reconstruction against cutting attack

At this stage, the cut robust image is received (Fig. 9).Initially, the first and second low-value matrices are received by the robust image and are placed in xor function with a two-dimensional code generated by the two-dimensional code generation algorithm.

Then, the result is divided into four parts and according to a predetermined pattern, its layout is returned to the original state. Reconstruction is taken place according to the reconstruction flowchart of the cropped image (Fig. 10). An image with two bits is produced (Fig. 11 and 12). The cropped image is checked and analyzed pixel by pixel via an algorithm. If the original image pixel is cut, that pixel is replaced with the pixels of the generated two bits image (Fig. 13).

Fig. 9. The cropped robust image

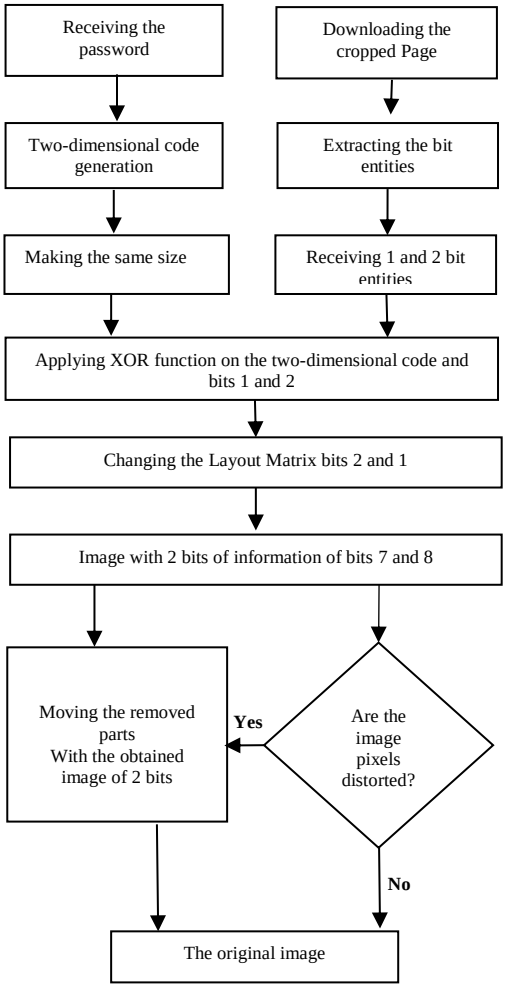


Fig. 10. Flowchart of the reconstruction of the cropped image

Fig. 11. Reconstruction of the seventh bit of the cropped image

Fig. 12. Reconstruction of the eighth bit of the cropped image

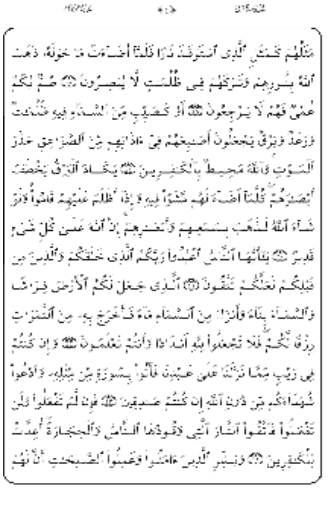


Fig. 13: Reconstruction of the cropped image

3.3.Robusting against distorted attacks

At this stage, the robust distorted image is recalled to the software (Fig. 14). At the begining, the bit components are received. Then, the first and second low-value matrices are received and are located in the xor function separately by two-dimensional code generation algorithm. The obtained two matrices of the function are divided into four sections and their locations are corrected based on the original pattern. Finally, an image with 2-bit information of the robust image is generated with these two matrices and that image is converted into a logical matrix. Then, the robust matrix is converted to a logical matrix and the difference matrix of these two logical matrices is obtained. After applying morphological operations, the distorted location is highlited in the robust image with a linear blue color(Fig. 15). In the following, the obtained image of the first and second bit matrices as a complete image is compared to the robust distorted image pixel by pixel. In case of havingdifference between the pixels of the two images, the different parts are reconstructed with a function (Fig. 16). This flowchart shows the detection of the distorted location and reconstructingthem (Fig. 17).

Fig. 14. distorted image

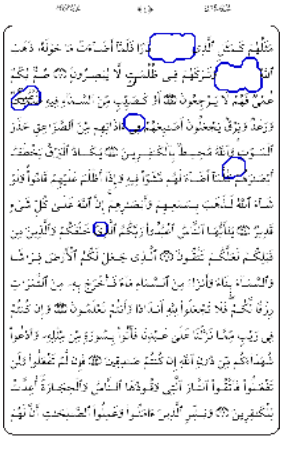


Fig. 15: Detection of the distorted location

4. RESULS

After reviewing and checking the algorithms in MATLAB that are stated in 3, the robust image isachieved which is tested according to Which is tested according to Equations (1) and (2). In these equations, I(i,j) represents the original image, I_w is the watermarked image, and the image dimensions are shown by N×M.

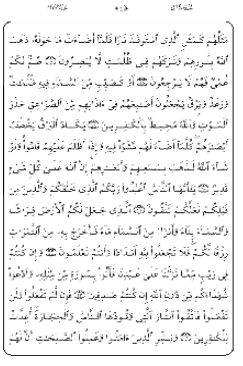


Fig. 16: Reconstruction of the distorted image

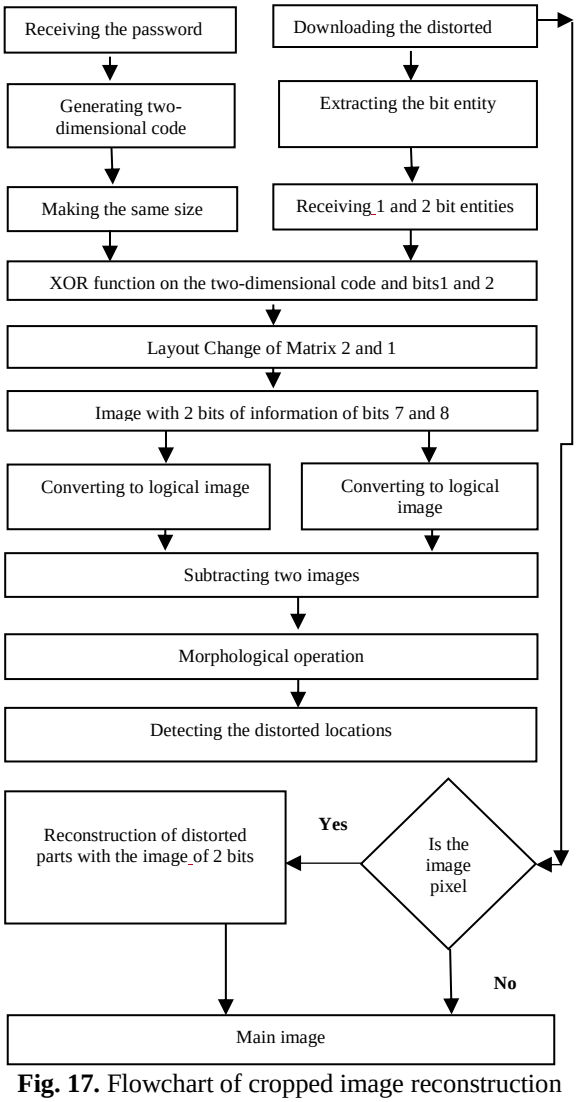


Fig. 17. Flowchart of cropped image reconstruction

Equations (1) and (2) are as follows:

Mean Square Error (MSE): MSE between original and watermarked image is measured by:

$$MSE = \frac{1}{MN}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}\left(I(i,j) - IW(i,j)\right)^2 \quad (1)$$

Peak-Signal-to-Noise Ratio (PSNR): The PSNR between the original and watermarked image is obtained by:

$$PSNR\,(I,I_w) = 10 \times log\,10\frac{MAX_I^2}{MSE} \quad (2)$$

The results of this test is included in Table 1.

Table 1: Results of the evaluation of the watermarked image with criteria

Evaluation Criteria	Criterion Result
Mean Square Error (MSE)	48
Peak-Signal-to-Noise (PSNR)	30.45

5. CONLUSION

Given that the proposed watermarking algorithm is fragile and its information can be destroyed with the slightest distortion, the recovery and reconstruction of distortions in the Quran pages are performed using two-dimensional barcodes and algebraic functions. In this way the algorithm not only detects the distortion but also detects its location as well. Then, the distortion is reconstructed and corrected. The difference between this method and previous ones is that previous methods only detected the distorted location. But in this method, the distorted location is detected and distortions are corrected. In addition, these pages are going to be safe against cutting attacks. If such a distortion occurs in Quran page, the cropped image can be retrieve using this algorithm. The significant advantage of the proposed method is that a two-dimensional code can be generated for each page of Quran, and it can be expanded and used to protect and the digital image texts that are very sensitive.

REFERENCES

[1] Dr. Omar Tayan, " The Role of Information Security in Digital Quran Multimedia Content." ,2014.

[2] S.M. Mousavi, A.Naghsh dnd S.A.R.Abu-Baker, "Techniques used in Medica Images a Survey. ", Journal of Digital Imaging The Journal of the Society for Applications in Radiology , pp. 714-729, 2014.

[3] A.SivaSankar,T.JayachandraPrasad,M.N.GiriPrasad,"LSBBasedLossless Digital Image Watermarking using Polynomials inSpatial Domain for DRM. ", 2011.

[4] S.Khurana, " Watermarking and Information-Hiding.", 2011.

[5] S. M. Mousavi , A . Naghsh , Azizah A . Manaf , " A robust medical image watermarking against salt and pepper noise for brain MRI images. " Springer Science Business Media New York,Article pp1-30,2016.

[6] M. S. Khalil, F. Kurniawan, M. Khurram Khan, Y. M. Alginahi, " Two-Layer Fragile Watermarking Method Secured with Chaotic Map for Authentication of Digital Holy Quran." The

Scientific World Journal Volume 2014 ,Article ID 803983, 29 pages, 2014.

[7] H. Amira, R. Rhouma, S.Belghith, "An eigen value based watermarking schem for tamper detection in gray level images. "International Multi-Conference On System,Signals and Devices, 27-30 ,2010.

[8] A. Gutub,L. Ghouti,A. Amin, "Utilizing Extension Character Watermarking. "International Conference on Security and Cryptography ,Barcelona, 2007.

[9] Aabed, Mohammed, Sameh M. Awaideh, Abdul-Rahman M. Elshafei,& Adnan Gutub,"Arabic Diacritics Based Steganography. " IEEE International Conference on Signal Processing and Cmmunications, pp 756-759, 2007.

[10] F.Kurniawan, M.S. Khalil1,M.Khurram Khan ,Y.M.Alginahi, "Exploiting Digital Watermarking to Preserve Integrity ofThe Digital Holy Quran Images. ", 2013.

[11] F. Kurniawan, M. S. Khalil, M. Khurram Khan,Y. M. Alginahi, "DWT+LSB-based Fragile Watermarking Method ForDigital Quran Images. ",2014.

[12] A. Farmani, H. Balazadeh Bahar, " Hardware Implementation of 128-Bit AES Image Encryption with Low Power Techniques on FPG. " Majlesi Journal of Electrical Engineering, Vol. 6, No. 4, December 2012.

[13] A. Farmani, M. Jafari and Seyed Sohrab Miremadi. "A high performance hardware implementation image encryption with AES algorithm." 3rd International Conference on Digital Image Processing. International Society for Optics and Photonics, 2011.