Jurnal Kejuruteraan 34(3) 2022: 485-493
https://doi.org/10.17576/jkukm-2022-34(3)-15

Image Watermarking Technique for Digital Al-Quran based on Fibonacci Transform via DWT

Nasharuddin Zainal, Seri Mastura Mustaza* & Wan Noormaheran Wan Hussin

Department of Electrical, Electronic & System Engineering (JKEES),
Faculty of Engineering & Built Environment, Universiti Kebangsaan Malaysia, Malaysia

*Corresponding author: seri.mastura@ukm.edu.my

Received 7 October 2020, Received in revised form 16 September 2021
Accepted 16 October 2021, Available online 30 May 2022

ABSTRACT

Advent growth in information and communication technologies has accelerated the needs to secure digital media. Demands for digital media when on the move urged Quran readers to install the Quran mobile apps on their device. However, there is no secure mechanism to legalize its content credential. On the other hand, mobile developer finds difficulty in getting access to readily authentic Quran database sources. Malaysia government has introduced Smart Quran mobile apps without any counterfeit protection. Correspondingly, the contents are vulnerable to hacking, falsification which consequently endangering Islamic institutional prestige. There is also a lack of credible authorization institutions to verify authenticity of the digital Quran that could possibly deviate the Muslim faith by reciting falsified content and meaning. To fill the void, this paper explores the utilization of an image watermarking to preserve the Quran digital image. The study presents new blind RGB image watermarking using Fibonacci Transform via Discrete Wavelet Transform (DWT) and manipulates the R component of the Al-Quran image. The second level of LL decomposition of the cover image will then be substituted by the Fibonacci-transformed watermarked version. DWT embedding is achieved through alpha blending technique. Final watermarked image is obtained once RGB conversion is performed. The efficiency of the method is assessed towards 10 samples. Verification is conducted via the extraction of the endorsed license image. The results demonstrate enhanced robustness and imperceptibility with average PSNR and SSIM of 92.13 dB and 0.99 respectively. Forgery cases of digital Quran applications are therefore tackled.

Keywords: Image Watermarking; Digital Al-Quran; Fibonacci Transform; Discrete Wavelet Transform (DWT)

INTRODUCTION

Massive evolution in digital technology nowadays is in tandem with the surge of prevailing digital media modification tools or software. Digital media such as image, video and audio are prone to various modification attacks with little to no quality affect (Said 2015). Current lifestyle trends introduced the tendency in frequently accessing information digitally. This includes the recitation of digital Quran. With more than 500 Al-Quran mobile version that is free to download on the Android platform (Zahari et al. 2017) and the widespread usage of the digital Quran across all platform via the internet, there is the need for tools or systems to verify the authenticity of the digital version of the Quran. The Quran is a sacred book, and that it is required to be read by all Muslims, and is the foundation of Islamic faith, ethics, and values. These days any website or mobile application developer can reproduce the holy Quran into digital version, makes it susceptible to manipulation and alteration. Hence, it is each Muslim obligation to preserve the holy Quran from dishonest manipulation. The findings in Talib et al. (2015) suggest the developers are required to provide assurance that the contents of their mobile Quran application are reliable, and that even when interacting with add-on functionality, the content validity will not be jeopardized. This study shows that addressing issues related to security threats and vulnerabilities will minimize changes and alterations that could occur in mobile Quran apps.

In 2018, McAfee Global Threat Intelligence has detected an almost 65,000 fake mobile apps (Kerner 2019). A control mechanism needs to be established to counterfeit this statistic. Fake mobile apps can be categorized as imitators or imposters. Tang et al. (2019) characterized imitators apps as those with almost similar names and functionalities to the original apps, while imposters refer to the apps that share the same metadata with the original apps. Fake mobile Quran may be categorized as both with manipulated content. As early as in 2006, an incident of fake Holy Quran being distributed over the Internet has been exposed by (Hakak et al. 2017; Hilmi et al. 2013). Then, a year later, King Saud University (KSU) has developed digital Al-Quran as Ayat Program where the digital images supplied by the scanned copy of the physical mushaf from the King Fahd Complex for The Printing of The Holy Quran (King Saud 2014). Later, Zakariah et al. (2017) urged the research community to accommodate technical solution to conserve the authenticity of Al-Quran and calls for the establishment of an enforcement agency to validate online Quran publications. Hakak et al. (2017) then describes main considerations while perusing the Quran are the credibility and purity of the Quran messages as well as to shield the verified content from inappropriate transformation or conversion. The authors outlined watermarking as one of the promising solutions to alleviate forgery risk in Quran.

Sharif (2019) agreed that it is vital to monitor digital al-Quran verses and chapters to certify the authenticity, and he also discloses that digital Quran has been popular among the senior citizens. For instance, an avid non-Arabic Quran reader finds pleasure to get to read or even memorize the Quran using mobile apps as it offers flexibility and convenience. With this widespread usage, there is the urgency to develop a method to preserve the originality of the content of digital Quran to ensure readers to engage with only an authenticated and endorsed content of the holy Quran. This is to avoid the misinterpreted meanings of the verses which can unintentionally drift Muslims' faith. Elobaid et al. (2014) finds developing the digital Quran is a tedious, error-prone and very time-consuming process without getting authentic sources in a form that can be readily inputted to their databases. Additionally, Alginahi et al. (2017) and Talib et al. (2015) supported the claim that developers shall provide a credible Quran mobile apps without endangering contents validity.

Top two Al-Quran mobile apps in Malaysia have been developed and available in Google Play Store with over 100,000 devices being downloaded (Jakim 2019; Tilawah.My 2019). The Smart Quran apps is an initiative by the Government of Malaysia to develop the first version of Quran mobile application that is endorsed by the Al-Quran Printing Control and Licensing Board, Ministry of Home Affairs, Malaysia (MOHA) and compliance with the Printing of the Quranic Text Act 1986 (Act 326). It is a collaboration project between Malaysian Communications and Multimedia Commission (MCMC), MOHA and the Department of Islamic Development Malaysia. However, the app is lacking in terms of security trait.

Digital watermarking is a technique used to add a covert media known as watermark media into the cover media, to form a watermarked media that can be used to protect images. The watermark media could be visible or invisible (blind) as long as its stick together with the cover media (Hai Tao et al. 2014; Hassanien 2006). The essential part in digital image watermarking is determining the region of interest (ROI) in which the watermark shall be embedded. This will specify the complexity to detect the watermark and the strength of the watermarked image to withstand various image processing attacks. For Al-Quran images, copyright protection is required to shield the Al-Quran contents from being changed from its original meaning and contents. Image watermark is preferred as its eliminate localized and dispersed in text watermarking attack (Kamaruddin et al. 2017; Wei Khang 2016).

A blind image watermarking in a frequency domain based on optimal blocks selection has been proposed by Tarhouni et al. (2018). The study presents a watermark insertion scheme utilizing Discrete Cosine Transform (DCT). Block based is preferred in DCT to ensure changes only happened in the transform coefficients of the selected block to avoid alteration towards the whole image (Kr Sinha et al. 2014). The study also applied Arnold's Transform to the installed watermark. Almost similar algorithm was utilized by Cedillo-Hernandez et al. (2015) except for the untouched Cb and Cr components. The researchers claimed assimilation of image normalization and convolutional encoding in DCT domain resulting 44.19 dB, 0.9559 and 0.9967 in PSNR, VIF and SSIM value respectively.

In comparison to the previous studies, Harith Raad (2014) utilized Cb and Cr components of the RGB cover image instead. The findings indicate the two-level sub-bands demonstrates sufficient imperceptibility, capacity, and security, albeit of the extracted watermark being modified entirely. To achieve higher capacity with an acceptable recovery quality, Chaughule (2017) presented a blind, non-blind and double or modified blind watermarking scheme which exploits DWT on RGB host image. the watermark image is mapped chaotically using Arnold's Transform. In the same way, Hasan (2018) has developed a simple partitioning of RGB host and watermark image in 3-levels DWT domain with an absence of Arnold's Transform. Tan et al. (2019) has put an extra mile from the preceding studies when acquaint with channel coding-based, 4-levels DWT, Arnold's Transform, YCbCr pattern and SVD. The paper discloses that channel-based scheme is able to retrieve precise watermark against all categories of attacks. A combination of DWT and LSB has been utilized by Kurniawan et al. (2014) to protect digital Quran images and improvised the watermarking integrity by applying parallel watermark in both wavelet and spatial domain.

DWT which manipulates Haar wavelet function inspired the study by Wang et al. (2019). The authors perform 3-levels DWT into the YIQ cover image, 1-level DWT into the YIQ watermark image and embedding occurred in low and mid band frequency wave range. The paper use DCT technique and recommends the middle band as the best region to introduce watermark. Having consensus agreement, T. Bhaskar et al. (2015) also utilizing DCT middle band frequency of the Y component extended to the video watermarking.

Exploiting block-based selection, Abraham et al. (2017) presents a 2×2 blocks of logo color image to be embedded into the host color image in the spatial domain and handle each color channel separately. The watermark bits are installed into all regions of the host image. The scheme introduces Simple Image Region Detector (SIRD) to each of the sub-block before implanting the watermark bits. Ghadirli et al. (2019) concludes an image encryption need to be integrated with other schemes to compensate their deficiencies. A hybrid between cryptography and watermarking methods has been constructed by S. Khalil et al. (2014) to authenticate and detect digital holy Quran image forgery. The article initiates two-layer of fragile watermarking coupled with a chaotic map. Embedding is performed in both wavelet and spatial domain towards both RGB and grayscale Quran images. The approach in this study manifests excellence tampering discovery up to the little tiny area. N. Jayashree et al. (2019) presents a chaotic hybrid watermark in DWT, Z-Transform and bidiagonal SVD. The host image is decomposed in 3-levels DWT and its HH3 and HL3 is then subjected to Z-transform. Arnold's Transform is applied into binarized watermark image and finally bidiagonal SVD is used to compute the area in which embedding will happen.

Image watermarking that modelled geometry attacks such as cropping, scaling and rotation in image geometry changes has been proposed by Roy et al. (2018). The paper presents a scheme that assimilate key generation, detection of the geometry attacks, and watermark embedding and extraction phases. A scheme to detect, reconstruct and repair the distortion in Quran pages using Image Watermarking in spatial domain has been formulated by Arabzadeh et al. (2018). The paper displaced the 7th and 8th bits of the controlled, plain Quran page and into new matrix which segregated the page into 4 segments with 4 Quick Response (QR) codes. However, this method requires 604 of QR codes (watermark image) to protect one whole Al-Quran (rasm Uthmani) as it uses Quran page number to generate a unique 2D QR code for each page.

Combination between DWT and DCT including Arnold's Transform was utilized in Chaturvedi et al. (2019) and B. Jagadeesh et al. (2019) papers. The former interested in YCbCr while the latter uses existing RGB images. The successive paper uses dual watermark image to embed with additional SVD and the scheme looks alike as the third proposed scheme in Chaughule (2017). Both schemes shared embedding stages which includes single level DWT, DCT block-by-block and LL sub-band is chosen to encapsulate the watermark image. The successive works add HH sub-band to hide the second watermark image. Similarly, A. Alotaibi et al. (2019) considers Quran text-image by integrating integer wavelet transform (IWT) to the original image and DCT towards low frequency, LL sub-band. To compare imperceptibility and robustness criteria between DWT and DCT, Said (2015) has revealed that DWT has delivered slightly better value in PSNR and outweighed DCT in terms of NC.

In line with security enhanced of watermarking performance, Rakotomalala et al. (2018) compared the performance of image-based-permutation-transform scrambling technique and revealed that Fibonacci Transform outperformed Arnold Transform corresponds to PSNR, SSIM, NPCR UACI, correlation coefficients and response time. Image watermarking with Fibonacci Transform in 3-levels DWT of the host image is demonstrates by (P. Shanthi et al. 2016). The host image of LL3 is transformed using Fibonacci. The scrambling position utilizing Fibonacci Transform is opted to covert the place in which the embedding is occurred. The study concludes that this approach is robust, secured and increase invisibility. A combination of Arnold's Transform and Fibonacci Transform in DWT image watermarking has been accessed by Kr Sinha et al. (2014). The authors used random binary sequence from scrambled-binarized watermark image to encrypt and pseudo-random number generator to determine the pixel to be used on a given key. The host image experience three-level of DWT at LL sub-band region which then the watermark will be implanted into LL3. Meanwhile, Fibonacci Transform is opted because of it is a key dependent domain where the selected sub band is related to the selected Fibonacci. For a cover images with N×N size, p is chosen as a sub band size. The parameter p is secretly shared between the transmitter and receiver. The relationship of DWT sub-bands with Fibonacci sub-band size is illustrated in Table 1.

TABLE 1. Relationship of DWT and Fibonacci sub-bands

No	DWT sub-bands	Fibonacci sub-bands
1.	LL	$N_{n-1} \times N_{n-1}$
2.	LH	$N_{n-1} \times N_{n-p-1}$
3.	HL	$N_{n-p-1} \times N_{n-1}$
4.	HH	$N_{n-p-1} \times N_{n-p-1}$

There are several properties that defines image watermarking performance such as imperceptibility, robustness, security and capacity. An extracted watermark that is resilient to attacks is called robust while the one which damaged or destroyed once detected is catagorized as fragile. Imperceptibility means the watermark does not induce visual image distortion. The watermarked image must mimic the cover image. Thus, this paper aimed to secure an endorsed Quran mushaf by Ministry of Home Affairs (MOHA) with secure image watermarking and consequently, to be utilized by the Quran mobile apps developers or Quran publisher to offer a digital version of the physical mushaf to the consumer. Discrete Wavelet Transform (DWT) is proposed in this scheme, motivated by the theory from DWT multiresolution analysis that decomposes the image into recursive and band-limited component whereby the original image can be restored. DWT helps to transform the original Al-Quran image into low and high frequency denoted as LL, LH, HL and HH which corresponds to approximate, vertical, horizontal and diagonal part of an image information. DWT based image watermarking in lower frequency presents better composition when introduced to attack. This will ease the development stage of Quran mobile apps as the images are Printing of the Quranic Text Act 1986 (Act 326) compliance ready. The rest of the paper is organized as follows: Section 2 discusses the proposed method with its embedding and extraction processes and Section 3 reports the experimental results in terms of imperceptibility and robustness. Finally, Section 4 concludes the paper.

METHODOLOGY

DWT AND IDWT

In digital watermarking, the options for embedding a watermark hinge on either in a spatial domain or in a transform domain. Since the aim of this paper is to articulate robustness and imperceptibility in image watermarking, transform domain is favored due to the strength ability while dealing with myriad of morphing and signal processing technique. Furthermore, this domain considers Human Visual System (HVS) and more durable than spatial domain (Jabbar 2018). In this study, DWT is proposed motivated by the theory from DWT multiresolution analysis that decomposes the image into recursive and band-limited component whereby the original image can be restored.

The transformation of DWT is used in this work for the purpose to convert the original signal from spatial domain into frequency domain. Four non-overlapping multiresolution coefficient sets are achieved after DWT is applied to the Al-Quran image. The coefficients (LL, LH, HL, HH) are obtained from Equation (1) to (4).

$$Z_{LL}^{K}=\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}m(x)m(y)Z_{LL}^{K-1}\times(2u-x)(2v-y) \tag{1}$$

$$Z_{LH}^{K}=\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}m(x)n(y)Z_{LL}^{K-1}\times(2u-x)(2v-y) \tag{2}$$

$$Z_{HL}^{K}=\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}n(x)m(y)Z_{LL}^{K-1}\times(2u-x)(2v-y) \tag{3}$$

$$Z_{HH}^{K}=\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}n(x)n(y)Z_{LL}^{K-1}\times(2u-x)(2v-y) \tag{4}$$

where *K* defines the level of the decomposition. *m(x)* and *n(y)* are the impulsive responses. Inverse DWT or IDWT is obtained using Equation (5).

$$m(x,y)=\frac{1}{\sqrt{MN}}\sum_{m}\sum_{n}W_{\varphi}(j_0,m,n)\varphi_{j0,m,n}(x,y)+\frac{1}{\sqrt{MN}}\sum_{i=H,V,D}\sum_{j=j0}^{\propto}\sum_{m}\sum_{n}W_{\varphi}^{i}(j,m,n)\times\varphi_{j.m.n}^{i}(x,y) \tag{5}$$

FIBONACCI TRANSFORM

The aim of this paper is to enhance security level of the watermarked image. Thus, introducing encryption technique such as image scrambling using Fibonacci Transform is adapted. The matrix of Fibonacci series is as in Equation (6).

$$FT_1=\begin{pmatrix}F_1 & F_2\\ F_3 & F_4\end{pmatrix}=\begin{pmatrix}0 & 1\\ 1 & 2\end{pmatrix} \tag{6}$$

THE PROPOSED IMAGE WATERMARKING SCHEME

This study used a top bottom approach, and the algorithm was constructed using MATLAB software. The project design is described in Figure 1.

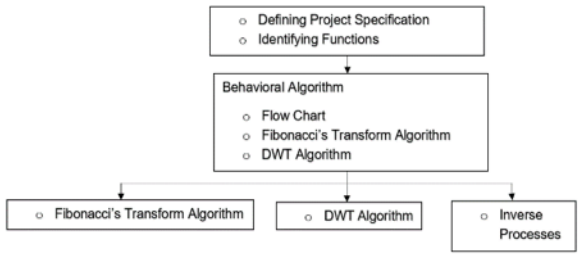


FIGURE 1. Top Bottom approach of the project design

The framework of the image watermarking scheme is described using a flowchart as in Figure 2.

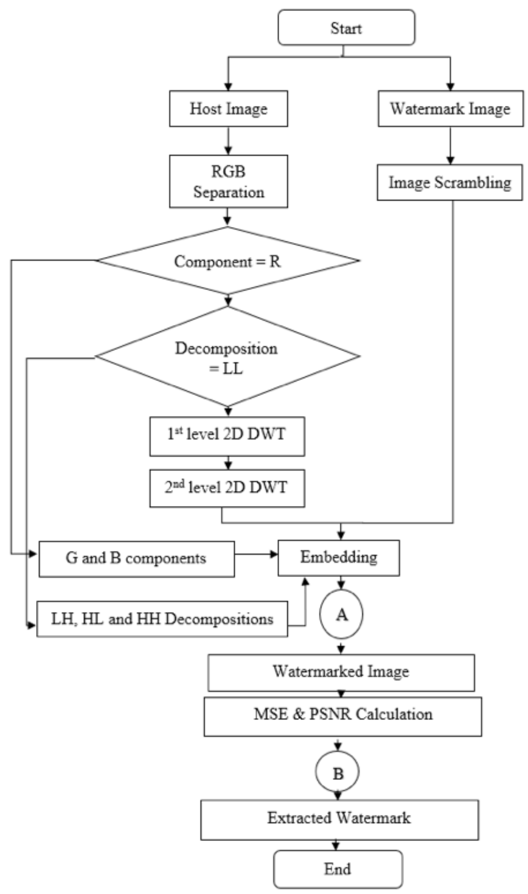


FIGURE 2. Framework Design Process Flow Chart

The process starts by reading the watermark image of MOHA stamp, transforming it into gray scale image and scrambled the image using Fibonacci transform twenty times. The scrambled watermark image is denoted as *WI*. Parallel to this step, the host Al-Quran image is also loaded in RGB form. The host image is decomposed into R, G and B color space, and the R plane of the host imaged is chosen. R component is chosen due to producing high PSNR in Koju et al. (2014) comparison works. 2-level DWT is then applied to obtain the sub-bands of R plane; LL2, LH2, HH2, HL2.

Next step of the proposed image watermarking steps involved two main stages, which are embedding and extraction, labeled as A and B, respectively in the flowchart of Figure 2. These two stages will be described in the following subsections.

DWT-FIBONACCI WATERMARK EMBEDDING ALGORITHM

The processes involved in the watermarking insertion or embedding is summarized through the flowchart illustrated in Figure 3 and each of the steps are explained below:

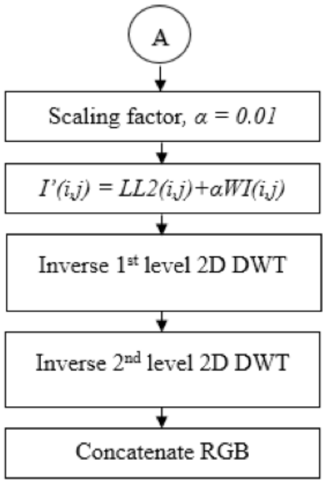


FIGURE 3. Flowchart for watermarking embedding

Step 1: Embed the scrambled watermark image to R plane's LL2 sub-band by using only optimized scaling factor or alpha, α = 0.01. *Haar* wavelet filter is used in this scheme due to operationally fast and easy to understand, memory efficient, provides high compression ratio and PSNR value including offering more significant details of the signal in contrary to other wavelet transforms in reversible process (Khan et al. 2019).

Step 2: Utilize Equation (7) to accomplish the embedding of the watermark image.

$$I'(i,j) = LL2(i,j) + \alpha WI(i,j) \tag{7}$$

The image obtained is the watermarked R plane which comprises the watermark image.

Step 3: Take the first level inverse of 2D DWT of watermarked R plane
Step 4: Take the second level inverse of 2D DWT of watermarked R plane
Step 5: Concatenated the watermarked R plane with the G and B plane to get the final watermarked image.

In this study, the lower band frequency coefficient (LL) is selected to embed the watermark, to achieve efficient computational time as watermark detection that occurred in lower resolution region contains fewer number of frequency bands that involved at every successive resolution level. LL sub-band watermark embedding will not alter the original host image information as it remains its optimum presence because it does not contain the fine information of the image (Singh 2018).

The watermarked image is then passed to the extraction phase.

DWT-FIBONACCI WATERMARK EXTRACTION ALGORITHM

The proposed watermarking scheme is a blind technique whereby the watermark extraction occurred without the existence of the original host image. The extraction process is represented through a flowchart in Figure 4 and the steps involved are explained below:

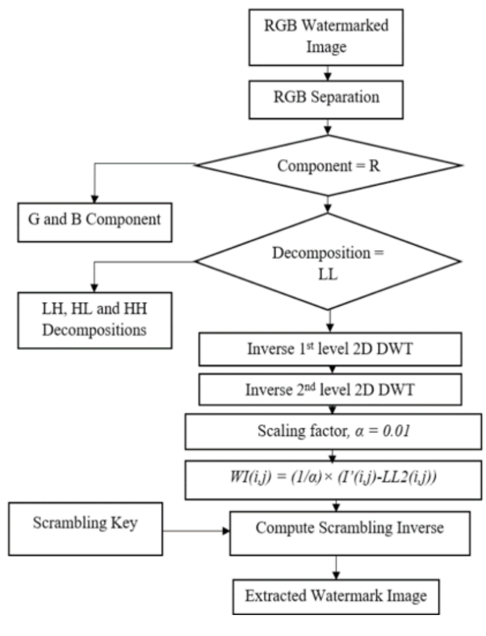


FIGURE 4. Flowchart for Watermarking Extracting

Step 1: Load the watermarked Al-Quran image in RGB form from the embedding phase.
Step 2: Decomposed the final watermarked image into RGB color space.

Step 3: Select the R plane of the final watermarked image to be manipulated.
Step 4: Apply the 2-Level DWT of R plane in watermarked image to get the sub-bands of R plane LL2, LH2, HH2, HL2.
Step 5: Extract the watermark image using Equation (8).

$$WI(i,j) = \frac{1}{\alpha}\, I'(i,j) - LL2(i,j) \tag{8}$$

Step 6: Apply the Fibonacci's descrambling method to obtain the original watermark image.

WATERMARKING PERFORMANCE

Watermarked image can be gauged using PSNR to assess its quality. The goal is to achieve as high as possible PSNR value as it specifies high security due to minimum gaps between the original and watermarked image. Therefore, hard to break the covert information. Basically, human perspective eyes can accept an image with PSNR > 30 dB (Kr Sinha et al. 2014). However, according to Agarwal et al. (2015), if the PSNR is 35 dB or higher, then both of the images are considered virtually indistinguishable by human viewers. The quality of an image is subjected to attacks, watermark capacity and size of image. PSNR formula used in this paper is defined in Equation (9).

$$PSNR = 10 \times \log \frac{MAX_i^2}{MSE} \tag{9}$$

where MAX_i is the maximum possible pixel value of the host image and MSE (Mean Square Error) is a cumulative squared error between the watermarked image and the original image. The mathematical formula for the MSE is defined in Equation (10).

$$MSE = \frac{1}{m \times n} \times \sum_{i=0}^{m-1} \sum_{i=0}^{n-1} [I(i,j) - K(i,j)]^2 \tag{10}$$

where *m* and *n* are the number of rows and columns in the original images, respectively and *I (i, j)* is the cover image, *K (i, j)* is the watermarked image.

RESULTS AND DISCUSSIONS

For evaluation purpose, the experiments are tested on 1024×1024 Quranic images, available from (Jakim 2019). Figure 5 illustrates some of the Quranic sample images used in this study.

(a) 10.ppm

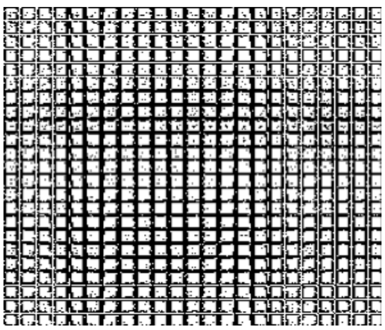
(b) 7.ppm

(c) 5.ppm

FIGURE 5. Samples of the Host Image

Figure 6 compares the original watermark image of the official MOHA stamp and the watermark image after Fibonacci Transform has been applied 20 times, scrambling the watermark image before embedding it to the Quran image.

(a) Original Watermark



(b) The watermark image after Fibonacci Transform

FIGURE 6. Watermark Images

IMPERCEPTIBILITY

In view of imperceptibility criteria, the study calculated the PSNR (refer to Equation (9)), which is dependent on MSE value. The PSNR value is used for evaluating the transparency of watermarking technique and, the larger PSNR is, the better the image quality. A watermarked image is considered acceptable by human perception if its PSNR value is above 30 dB (Kr Sinha et al. 2014). The results of the proposed scheme with top three outstanding PSNR values are shown in Figure 7. The results for all the samples used in this study are tabulated in Table 2. Since all the images have PSNR value greater than 30 dB, it is therefore concluded that the final watermarked images are good quality images.

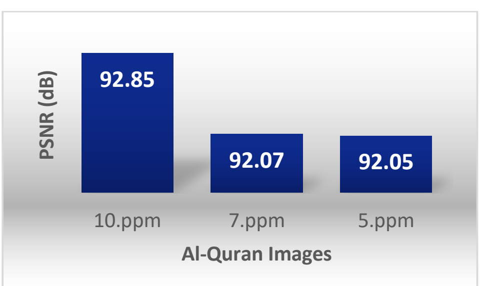


FIGURE 7. PSNR values for Al-Quran images

TABLE 2. MSE and PSNR value for the host images used to test the proposed scheme

No.	Host Image filename	MSE	PSNR (dB)
1	1.ppm	0	92.03
2	2.ppm	0	92.05
3	3.ppm	0	92.05
4	4.ppm	0	92.03
5	5.ppm	0	92.05
6	6.ppm	0	92.04
7	7.ppm	0	92.07
8	8.ppm	0	92.05
9	9.ppm	0	92.03
10	10.ppm	0	92.85

ROBUSTNESS

With regards to robustness, the paper leverages on the Structural Similarity Index Measure (SSIM) of the watermarked image. All the watermark image that has been applied to Quranic images ‘10’, ’7’ and ’5’ achieved the SSIM values of over 0.99. This indicates that even after the watermark has been added using the proposed scheme, the structural information is preserved, and the original and watermarked images is nearly identical. In this scheme, a gray scale watermark image is used and requires an 8 bits information per intensity. It is interesting to note that the grayscale watermark image sufficiently meet the requirement of minimizing the bit information of the watermark image, requiring $m \times n \times 8$ bits. This is the reason most of the existing approaches for robust watermarks are based on binary watermark images. This may raise concerns in producing robust watermarked image which was addressed by the usage of grayscale format in image scrambling method.

DISCUSSION

All of the PSNR values for the watermarked images processed using the proposed scheme showcased a good visual image, as all of the sample images recorded a PSNR value of above 30 dB. All of the images also achieved good SSIM value from introducing Fibonacci’s Transform in the proposed scheme, which complicate the attacker in finding the location of the watermark image and so fulfilling the robustness criteria of watermarked image as compared to Arnold’s Transform in controlled scheme by Verma et al. (2017). Fibonacci Transform features unique uniformity in which the adjacent pixels distance remains same in both original and scrambled image. Thus, the adjacent pixels able to spread further with less correlation between pixels leading to better SSIM value in the proposed scheme.

Since manipulating occurred in wavelet decomposition in which compatible to human eyes. Thus, the experimental scheme facilitates the imperceptibility requirement and so delivering enhanced SSIM value. While deploying LL sub-bands in DWT approach provides least of losses of image information which in turns giving better PSNR and SSIM value as opposed to the scheme that utilized DCT representation. This simulation result supports the theory of DWT outperform DCT in image watermarking as discovered in a thesis by Said (2015).

CONCLUSION

This paper focused on image watermarking for copyright protection, applicable to digital Al-Quran images. A DWT-based blind and robust image watermarking, manipulating 2 level DWT was described. The Fibonacci Transform was utilized to scramble the watermark image creating confusion in the extraction or detection. This scheme exploited R component of the original Al-Quran images to be replaced with the scrambled watermark image bits.

The evaluation of image watermarking in this paper emphasized on two main indicators which are the PSNR and SSIM, which represents robustness and imperceptibility criteria, respectively. The results agreed that with the manipulation of Fibonacci's Transform enhances the durability and performance of the experimental scheme. While combination of DWT image watermarking and Fibonacci's Transform presents excellent image property with respect to robustness and imperceptibility rather than in DCT. In addition, constructing hybrid approach between image watermarking and image encryption further elevates security characteristic in digital image protection.

ACKNOWLEDGEMENT

The authors would like to thank the Government of Malaysia for their financial support under the Hadiah Latihan Persekutuan (HLP) Scheme.

DECLARATION OF COMPETING INTEREST

None

REFERENCES

A. Alotaibi, R. & A. Elrefaei, L. 2019. Text-Image Watermarking Based on Integer Wavelet Transform (Iwt) and Discrete Cosine Transform (Dct). *Applied Computing and Informatics* 15(2019): 191-202.

Abraham, J. & Pau, V. 2017. An imperceptible spatial domain color image watermarking scheme. *Journal of King Saud University – Computer and Information Sciences* 1-10.

Agarwal, D. S.et al. 2015. Different types of attack in image watermarking including 2d, 3d images. *International Journal of Scientific & Engineering Research* 6(1): 841-845.

Alginahi, Y. et al. 2017. Digital holy Quran authentication, certification and standardization: A survey. *International Journal of Computer Science and Information Security (IJCSIS)* 15(12): 98-117.

Arabzadeh, A. & Naghsh, A. 2018. Detection, reconstruction, and repairing the distrortion in quran pages based on watermarking. *Majlesi Journal of Electrical Engineering* 12(3): 85-91.

B. Jagadeesh & Reddy, K. L. S. P. 2019. Visual Cryptography based on dual image watermarking for copyright protection and security using various transforms. *International Journal of Engineering and Advanced Technology (IJEAT)* 8(6): 4154-4160.

Cedillo-Hernandez , M.et al. 2015. Copyright protection of color imaging using robust-encoded watermarking. *RADIOENGINEERING* 24(1): 240-251.

Chaturvedi, R.et al. 2019. Dwt-Dct based copyright protection in YCBCR color space. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)* 8(10): 675-679.

Chaughule, S. S. 2017. A New Robust, Secure and High Capacity Watermarking Schemes for Image Authentication and Recovery Via the Discrete Wavelet and Arnold's Tranforms. Master Thesis, Department Of Electrical And Computer Engineering, University Of Massachusetts Lowell.

Elobaid, M. & Eldow, M. E. Y. 2014. Toward designing and modeling of Quran learning applications for android devices. *Life Science Journal 2014* 11(1): 160-171.

Ghadirli, H. M.et al. 2019. An overview of encryption algorithms in color images. *Signal Processing* 164(2019): 163-185.

Hai Taoet al. 2014. Robust image watermarking theories and techniques: A review. *Journal of Applied Research and Technology* 12(1): 122-138.

Hakak, S.et al. 2017. Preserving content integrity of digital holy Quran: Survey and open challenges. *IEEE Access* 5(2017): 7305-7325.

Harith Raad, H. 2014. Blind Colour Image Watermarking Techniques in Hybrid Domain Using Least Significant Bit and Slantlet Transform. PhD. Thesis, Faculty of Computing Universiti Teknologi Malaysia.

Hasan, H. R. 2018. Copyright protection for digital certificate using blind watermarking technique. *Kurdistan Journal of Applied Research (KJAR)* 3(1): 75-79.

Hassanien, A. E. 2006. A copyright protection using watermarking algorithm. *Institute of Mathematics and Informatics, Vilnius* 17(2): 187-198.

Hilmi, M. F.et al. 2013. Authentication of Electronic Version of the Holy Quran: An Information Security Perspective. International Conference on Advances in Information Technology for the Holy Quran and Its Sciences. Anjuran IT Research Center for the Holy Quran and Its Sciences (NOOR), Taibah University, . AlMadinah Al-Munawwarah, Kingdom of Saudi Arabia., 22-25 December 2013.

Jabbar, K. K. 2018. Image authentication subject review. *International Journal of Engineering Research and Advanced Technology (IJERAT)* 4(12): 13-18.

Jakim, D. O. I. D. M. 2019. Smart Quran's Apps. https://play.google.com/store/apps/details?id=com.madcatworld.qurantestbed&hl=ms [28 Oct 2019].

Kamaruddin, N. S.et al. 2017. A review of text watermarking: Theory, methods and applications. *IEEE Access*

Kerner, S. M. 2019. Fake Mobile Apps Are an Increasing Risk, Mcafee Reports. https://www.eweek.com/security/fake-mobile-apps-are-an-increasing-risk-mcafee-reports [20th Oct 2019].

Khan, S. et al. 2019. An efficient jpeg image compression based on haar wavelet transform, discrete cosine transform, and run length encoding techniques for advanced manufacturing processes. *Measurement and Control* 52(9-10): 1532-1544.

King Saud, U. 2014. Ayat Program. http://quran.ksu.edu.sa [22 Mac 2020].

Koju, R. & Joshi, S. R. 2014. Comparative analysis of color image watermarking technique in rgb, yuv, and ycbcr color channels. *Nepal Journal of Science and Technology* 15(2): 133-140.

Kr Sinha, M. et al. 2014. Digital Image Watermarking Using Fibonacci Transform in Yiq Color Space. *International Journal of Computer Applications* 104(15): 28-35.

Kurniawan, F.et al. 2014. Dwt+Lsb-Based Fragile Watermarking Method for Digital Quran Images. *2014 International Symposium on Biometrics and Security Technologies (ISBAST)*, hlm. 290-297.

N. Jayashree & Bhuvaneswaran, R. S. 2019. A robust image watermarking scheme using z-transform, discrete wavelet transform and bidiagonal singular value decomposition. *Computers, Materials and Continua* 58(1): 263-285.

P. Shanthi & Bhuvaneswaran, R. S. 2016. Image watermarking using fibonacci transform. *Asian Journal of Information Technology* 15(9): 1431-1436.

Rakotomalala, M. A.et al. 2018. Performances of image scrambling techniques based on the permutation transform. *IOSR Journal of Computer Engineering (IOSR-JCE)* 20(4): 55-70.

Roy, R.et al. 2018. Watermarking through image geometry change tracking. *Visual Informatics* 2(2018): 125-135.

S. Khalil, M.et al. 2014. Two-layer fragile watermarking method secured with chaotic map for authentication of digital holy Quran. *The Scientific World Journal* 2014(0): 1-30.

Said, M. A. 2015. A Comparison of Discrete Cosine Transform and Discrete Wavelet Transform Algorithm in Watermarking against Common Attacks. Master Thesis, Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia (UTHM).

Sharif, E. 2019. E Talaqqi: An analysis on the understanding of digital quran usage and implications among senior citizens in Malaysia. *Journal of Islamic, Social, Economics and Development (JISED)* 4(16): 66-81.

Singh, A. 2018. Block-Based Discrete Wavelet Transform Singular Value Decomposition Image Watermarking Scheme Using Human Visual System Characteristics and Firefly Algorithm. Master Thesis, Department Of Electronics And Communication Delhi Technological University.

T. Bhaskar & Vasumathi, D. 2015. Dct based watermark embedding into mid frequency of Dct coefficients using luminance component. *International Research Journal of Engineering and Technology (IRJET)* 2(3): 738-741.

Talib, S.et al. 2015. Mobile Quran App Security Vulnerabilities. *Proceedings of the 5th International Conference on Computing and Informatics, ICOCI 2015*, hlm. 447-455.

Tan, Y.et al. 2019. A Robust Watermarking Scheme in Ycbcr Color Space Based on Channel Coding. *IEEE Access* 7(2019): 25026-25036.

Tang, C.et al. 2019. A Large-Scale Empirical Study on Industrial Fake Apps. *ICSE-SEIP '19: Proceedings of the 41st International Conference on Software Engineering: Software Engineering in Practice*, hlm. 183-192.

Tarhouni, N.et al. 2018. A New Robust and Blind Image Watermarking Scheme in Frequency Domain Based on Optimal Blocks Selection. *International Conferences in Central Europe on Computer Graphics, Visualization and Computer Vision*, hlm. 78-86.

Tilawah.My. 2019. Tilawah Malaysia's Apps. https://play.google.com/store/apps/details?id=my.tilawah&hl=ms [28 Oct 2019].

Verma, P.et al. 2017. Comparative Analysis of Conventional 2-Level Dwt and Color Plane Watermarking for Telemedicine Applications. 2nd International Conference on Telecommunication and Networks. Anjuran IEEE Noida, Uttar Pradesh, India,

Wang, J. & Du, Z. 2019. A method of processing color image watermarking based on the haar wavelet. *Journal Visual Communications Image Representation* 64(0): 1-8.

Wei Khang, L. 2016. A Dual-Watermarking with Qr Code against Cropping and Resizing Attack. Masters, Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia.

Zahari, N. H. a. H.et al. 2017. Development of Al-Quran Android application from year 2013 to 2016: The highlight. *International Journal of Academic Research in Business and Social Sciences* 7(6): 183-195.

Zakariah, M.et al. 2017. Digital Quran computing: Review, classification, and trend analysis. *Arab J Sci Eng*