IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 28, 2016; accepted February 21, 2017, date of publication March 14, 2017, date of current version June 7, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2682109

Preserving Content Integrity of Digital Holy Quran: Survey and Open Challenges

SAQIB HAKAK[1], AMIRRUDIN KAMSIN[1], OMAR TAYAN[2], MOHD. YAMANI IDNA IDRIS[1], ABDULLAH GANI[1], AND SABER ZERDOUMI[1]

[1]Faculty of Computer Science and Information Technology Department of Computer System and Technology, University of Malaya, Kuala Lumpur, Malaysia
[2]Computer Engineering Department and NOOR Research Center, College of Computer Science and Engineering, Taibah University, Madinah, Saudi Arabia.

Corresponding author: Saqib Hakak (saqibhakak@gmail.com)

TThis work was supported by the University of Malaya through the Faculty of Computer Science and Information Technology under Grant RP003A 14HNE and Taibah University-NOOR Research IT Center Al-Madinah Al-Munawwarah, Saudi Arabia under Grant NRC1-126B, 2015-2016.

ABSTRACT In recent years, a new trend has come up, which is that of reading the digital Quran online. This text was revealed more than 1400 years ago in the Arabic language and has been protected from all possible ways of distortion until today. Unfortunately, driven by the desire to make profit or gain publicity, fraudsters have started modifying certain Quranic verses. These alterations are misleading many people who are thus deprived of the original and accurate message of the Holy Quran. This paper focuses on systematically analyzing and categorizing existing research related to preserving and verifying the content integrity of the Quran. This paper further assesses these existing studies in terms of their evaluation parameters and findings. We find that the existing studies can be classified according to their format and methods, i.e., the online formats in which the Quranic content is available, methods employed to protect the Quranic content from modification, and last methods of verification. This paper concludes with the issue of future challenges and their possible solutions.

INDEX TERMS Quran, content integrity, hadith validation, Quran verse authentication, tampering, authentication.

I. INTRODUCTION

The major challenge faced by researchers today is that the ever-growing range of digital media vastly exceeds the latter's ability to put proper authentication or integrity mechanisms in place. The past years have witnessed a, massive increase in the use of digital content accessible through the internet which has dramatically increased cases of copyright violations and this raised the issue of integrity, authenticity of digital content and data vulnerability [1], [2]. Due to the same reason, more and more research is being undertaken in the area of data integrity, authentication and security. The statistics are shown in Fig 1 taken from the web of a science database.

The excessive reliability on the internet and the increase in users has further exaggerated the problem of integrity and authenticity. According to World Internet statistics [3], the number of internet users is increasing fivefold as shown in Fig 2. With this trend of increase in internet users, the rate of publishing sensitive digital content online is also on the rise. There is lot of sensitive digital content available online which can be accessed and downloaded from different sources, such as religious websites, social media websites and other online blogs.

By sensitive content is meant here that the content constitutes material of utmost importance which requires protection of confidentiality, integrity or availability. This sensitive content may appear in the form of text, image, audio or video. As sensitive content is also considered the Holy Quran as the most authentic and unaltered religious text of all times. It constitutes the duty of every Muslim to protect its authenticity and integrity [4]. Furthermore, the majority of Muslims today use the internet for online education on religious precepts, Quran recitation and memorization, banking and socializing [5], [6]. The Quranic text or content is available in the form of simple text or images on numerous websites. However, there is no proper way or procedure to ascertain the authenticity or integrity of this sensitive published content. Besides, there is no converging trend where attempt has been made to unify various approaches for the purpose of authentication in the area of sensitive content like Digital

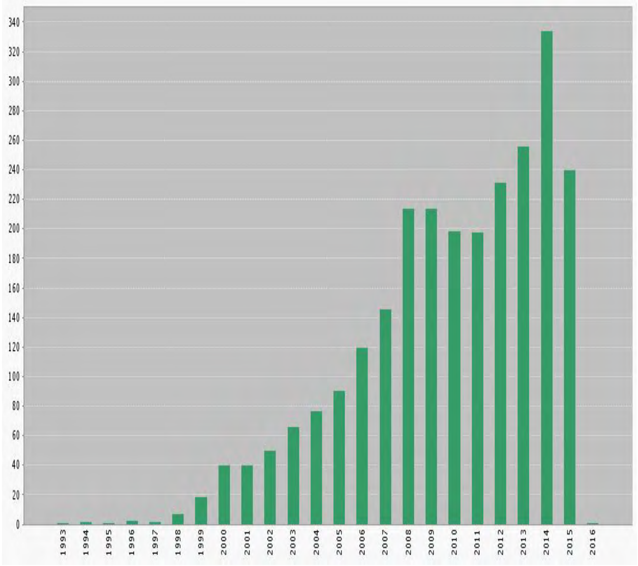

FIGURE 1. Research in the field of Authentication/Data Integrity of Online sensitive data (web of Science, 2015).

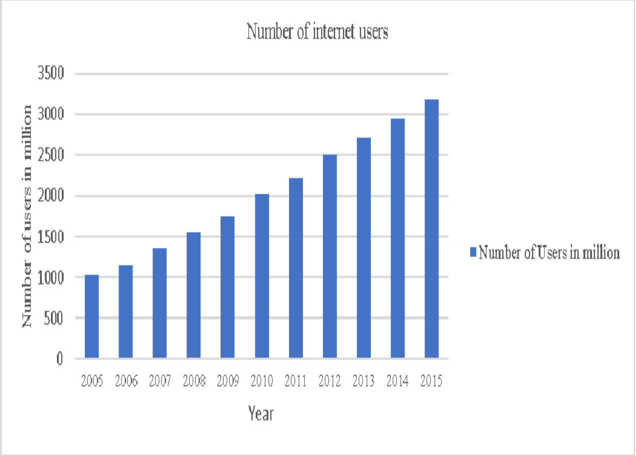

FIGURE 2. Number of Internet Users per Year [3].

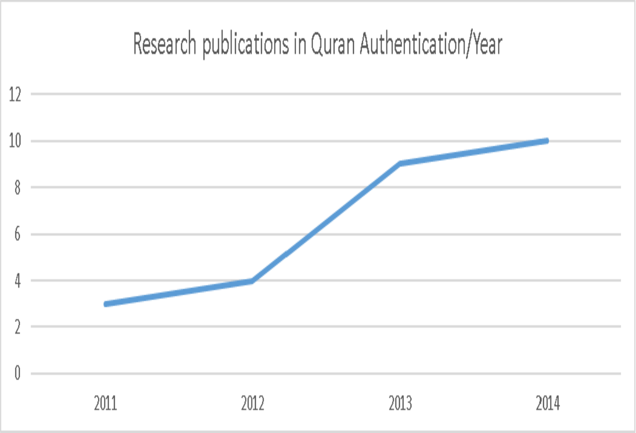

FIGURE 3. No. of Publications in the area of Quran Authentication (IEEE-Xplore, Elsevier Library).

Holy Quran. This is also one of the reason that this survey was carried out to give future researchers an overview of various approaches used in preserving the integrity of Digital Holy Quran and paving the way for unification of various approaches to achieve the goal of authentication. Thus, there is the need for a system that can monitor and endorse the digital copies or verses of the Holy Quran and hadith traditions (sayings of Prophet Mohammad (pbuh)) available in the various digital formats.

Some research work has already been started in this area as summarized in Fig 3. The focus of these studies is the verification of the Quranic content and its protection from tampering. The data presented in Fig 3 were taken from the IEEE explore library and Elsevier Scopus library. However, there still remains a lot to be done as this research field is quite new and still growing. For example, numerous symbols and diacritics are contained in the Quranic text, and the modification of just one symbol may change the meaning of a whole sentence or verse. If one single verse is misunderstood or misinterpreted, it creates lot of confusion in the minds of young Muslims who do not know it any better.

It is hoped that a better understanding of the processes involved in preserving and verifying the integrity of the Quranic content can enable us to devise a new and more efficient approach. The contributions of this paper can be summarized as follows:

1. To review the current research done in preserving the Digital Quranic content. This study constitutes the first survey carried out on the different approaches used for preserving the integrity of the Digital Quran.
2. To propose a new taxonomy based on the Quran integrity and authenticity approaches and techniques used for the same. A taxonomy based on possible attacks is also proposed.
3. To recommend future research in response to possible future challenges.

This paper is organized as follows: Section II presents the survey on the need of a system that can verify the integrity of the Quranic content, Section III contains brief summary related to ancient authentic copies of Holy Quran, Section IV reviews the preservation of the content integrity of the Quran, in Section V, a new taxonomy related to preserving the content integrity of the Quran is proposed, Section VI presents a classification of possible future attacks, and Section VII discusses open challenges and recommends future studies followed by the conclusion.

II. NEED OF QURAN INTEGRITY AND AUTHENTICATION APPROACHES

There has been one questionnaire based survey done by Khan and Alginahi [7] on Quran digitization challenges focusing on adaption of technologies used in reading Quran and other Islamic related material. The authors have tried to raise the awareness related to authentication of digital Holy Quran on internet and other related issues. The survey finally concludes that there is need of some monitoring body that can monitor each Islamic resource available online. In our case, also, a short survey was conducted in order to evaluate the need for such a system that could verify the integrity and authenticity of Quranic verses made available online. The purpose of this survey was to explore the public perception and gather feedback from the grass roots before carrying out our review work. A short questionnaire was created with experts from two public universities of Malaysia, i.e. University of Malaya and International Islamic University Malaysia. The questions were kept reasonably simple and easy to understand so that the users could easily answer those questions.

The number of expected participants was limited to 500 drawn from both the above-mentioned universities. The choice of conducting the survey in these universities was the level of diversity of the student population as both universities possess a considerable proportion of international students from different countries and cultural backgrounds. Some of the international students were Arabic native speakers while others were not. Out of 500 expected participants, we were able to obtain responses from a total of 376 participants who answered our questions and provided us with the expected feedback.

The first question related to the age of those who frequently read the Quran. The purpose was to find out whether young people familiar with the internet and all related technologies were really interested in reading their holy book in digital form. As shown in Fig. 4, 66.1 % of the participants within the age group of 18-30 read the Quran and 32 % who were above 30. The second question was to assess how often people read the Quran. The result showed that 43% of the participants read it every day while 34.9% read it whenever they felt like it as shown in Fig 5.

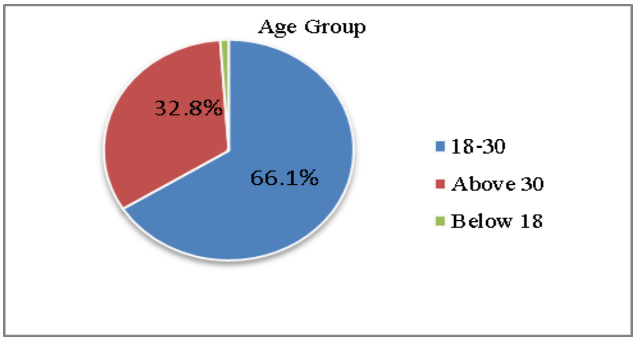

FIGURE 4. Age Group.

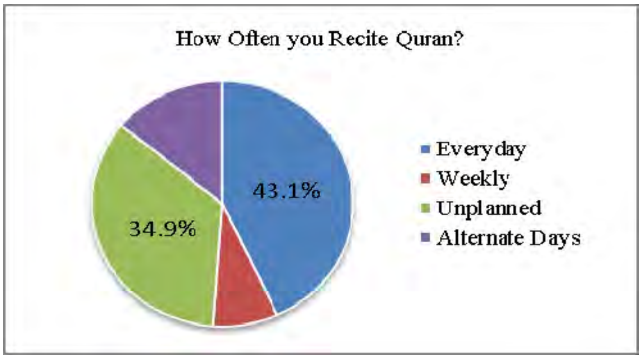

FIGURE 5. Quran Reading.

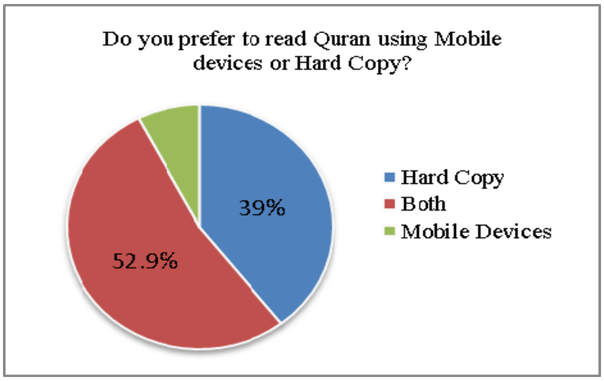

FIGURE 6. Preference of Reading Quran.

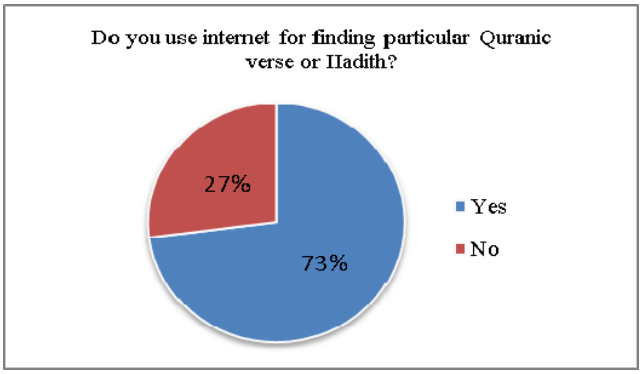

FIGURE 7. Use of Internet for reading Quran.

The next question was related to the preference of reading the Quran in a specific medium, i.e. hard copy or soft copy or both. Although 39.5 % of the participants preferred to read the Quran in hardcopy, another 7.6 % of the participants preferred reading softcopies and 52.9 % both. This question was followed by a question related to the use of the internet with respect to reading Quran or *hadith*. 73 % of the participants responded that they rely on the internet for finding a particular Quranic verse or *hadith*. Statistics of both these questions are shown in Fig 6 and 7 respectively.

Even though 73% of the participants confirmed that they used the internet for finding specific Quranic verses or *hadith*, it was surprising that they did not seem to be concerned about the authenticity or integrity of that content. The statistics with respect to this question are shown in Fig 8 where 29 % of the participants asserted that they could verify the authenticity of a particular verse or *hadith* and yet the majority of them (71%) could not. Altogether 69.6 % of the participants were not sure whether or not of any such verification system was available (Fig. 9) while approximately 10% simply did not know anything about it.

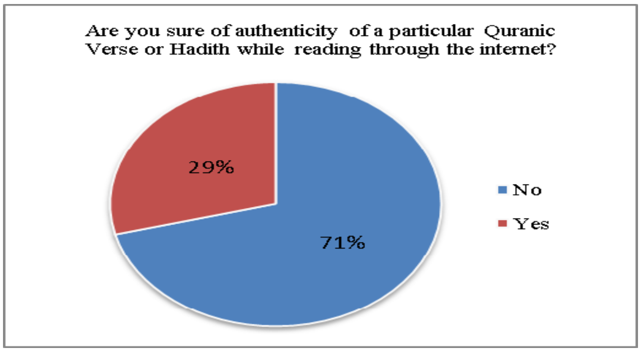

FIGURE 8. Authenticity while reading Online.

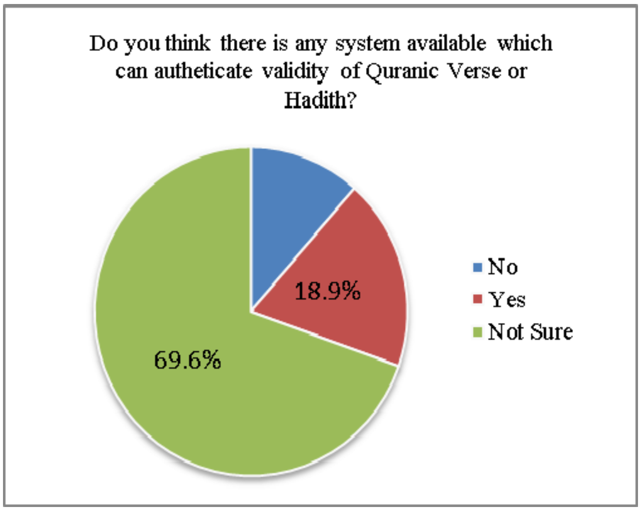

FIGURE 9. System available Online.

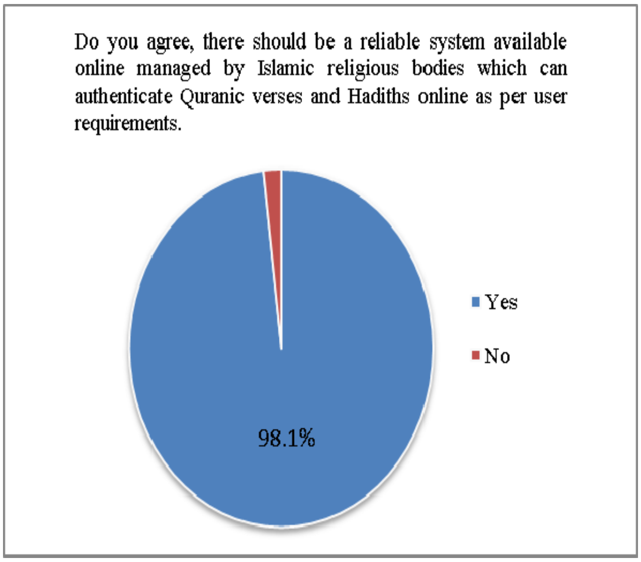

FIGURE 10. Need of reliable authentication system.

Although 18.9 % of the participants attested that such a system was available, a discrepancy in their answers to question 10 was found (Fig. 10). Almost 98.1 % of the participants concluded that there was a need for such a system. Thus, those 18.9 % who earlier claimed that there was such a system available online denied their previous statement by supporting the concept and need for such a system.

The last question was to find out whether native speakers of Arabic who could understand and read the Quran very well were able to identify erroneous Quranic verses or *hadith* available online. To our surprise, 27.6 % of the participants who were familiar with the Arabic language answered that they could not find any mistake in the Quranic verses they had come across online. 14.2 % admitted their helplessness in finding any mistake in the Quranic verses they had come across. The reason for this may lie in the complexity of the Arabic language which involves a lot of symbols and diacritical signs. 43.5 % of the participants admitted that they read only randomly. The statistics are shown is Fig. 11.

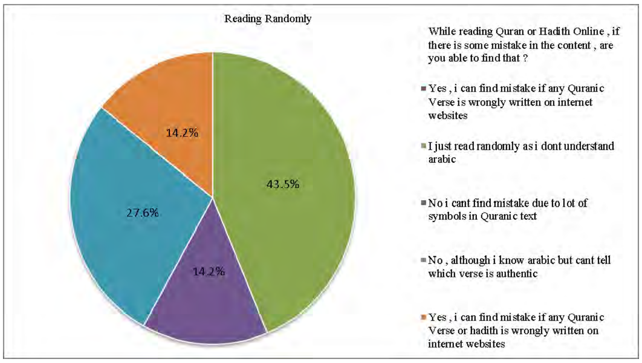

FIGURE 11. Ability to detect mistakes in the Holy Quran.

The above survey motivated us to carry out this research with respect to preserving the content integrity of the Holy Quran which constitutes a sacred Book of Revelation for 1.7 billion Muslims worldwide. Based on the feedback to this survey, a review was carried out to determine the state of the art of current online checking systems based on their different formats, i.e. image based and text based format.

III. IMPLICIT INTEGRITY OF HOLY QURAN

In order to review existing works related to authentication of Holy Quran, it is important to know its preservation from tampering since 14 centuries. Recently one of the oldest copy of Holy Quran in the form of Hijazi script was discovered using radioactive technique by Birmingham university [8]. Carbon dating technique is used to determine the age or date of organic matter from the relative proportions of the carbon isotopes i.e. carbon-12 and carbon-14 that it contains. From the research findings, it was observed that not a single Quranic verse has been tampered with compared to current version of Holy Quran. The reason of Holy Quran being preserved from tampering since 14 centuries is probably due to the fact that it was learnt by heart and memorized. After its revelation to Prophet Mohammad (pbuh), it was composed on parchments, leaves and other such materials by his trusted companions. However, to avoid any confusion in its writing,

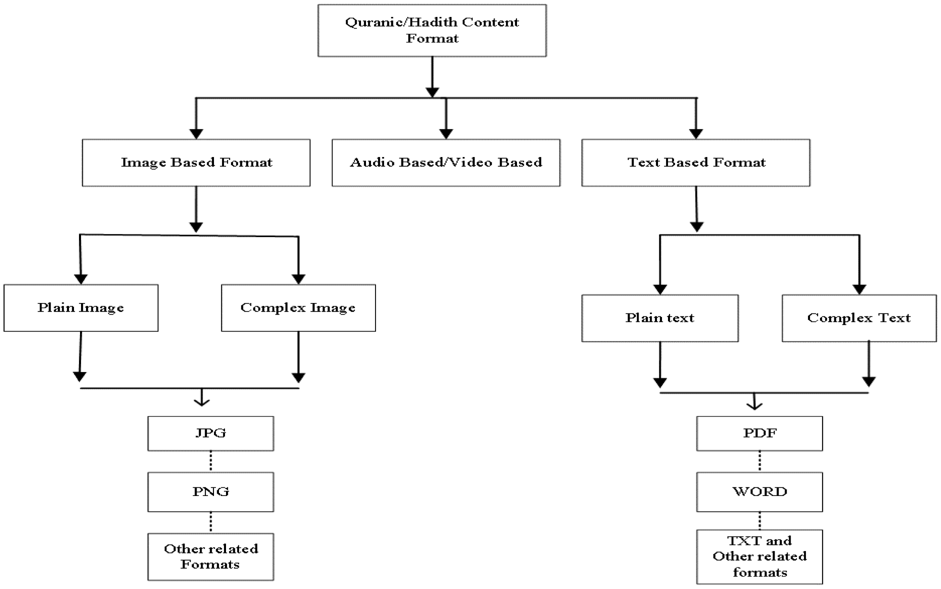

FIGURE 12. Classification Based on Format.

it was standardized and named as Uthman's codex which is considered as archetype of modern Quran used today [9]. Moreover, there are Several trustworthy organizations like King Fahd Complex for The Printing of The Holy Quran managed by Saudi Ministry of Religious Affairs, King Saud University and other related religious bodies that has authentic copies of Holy Quran for printing purposes [10]. Some other ancient copies of Holy Quran include Sana'a manuscripts using palimpsests (a manuscript page from which text has been washed for reusing the manuscript page) [11]. Hence, to preserve integrity of Digital Holy Quran, it is important to review existing works done to identify the weaknesses and strength of techniques used and propose future directions.

IV. REVIEW OF QURAN AUTHENTICATION AND INTEGRITY VERIFICATION APPROACHES

There are different methods and approaches for solving specific problems. In certain cases, the type of format used is crucial. For example, the image format which consists of raw data depends on certain techniques whereas the text format which consists of binary data depends on its own set of techniques. The research review revealed the lack of proper direction as the researchers combined text format with image format and thus created considerable confusion. Also, the studies do not mention whether or not a particular approach works for different formats. Based on these observations, it is proposed to group the existing body of research on preserving and verifying the Quranic content into image based format, audio/video based format and text based format. However, this study's focus is on image and text based approaches due to the limited scope of this research. The purpose of this approach is to give proper direction to future researchers in terms of identifying specific format and working on that format using suitable methods for more efficient solutions. The classification based on format is given in Fig. 12. A brief description of each group along with the work done in these two formats is given below:

A. IMAGE BASED FORMAT

There is lot of Quran and *hadith* images available online. In order to simplify the classification, we divided the image content into two sub categories, i.e. plain image and complex image. A plain image constitutes a picture which is clear and without much color details whereas a complex image is a picture with more color details and a lot of symbols. The two types of images are shown in Fig. 13. This classification is done based on the fact that different techniques are used in image processing. Both plain images and complex images are available in different formats like JPEG, TIF, GIF, etc. This area falls under the image processing field, and there are different kinds of techniques used for checking the integrity of the images. In section V, these techniques are explained in order to provide future researchers with a useful overview.

Below is the review work which falls under the image based format category. All work done related to the protection and integrity verification of the Quran is discussed together with the approaches used and the limitations encountered.

Tayan et al. (2013): The authors claim that content protection and copyright protection constitute the two major challenges while dealing with online sensitive content. Zero watermarking is identified as the most promising approach for content verification and authentication. A document to be authenticated is embedded with a specific data sequence obtained from a watermark logo. Finally, logical XOR operation is done to generate a specific key. The word size limit

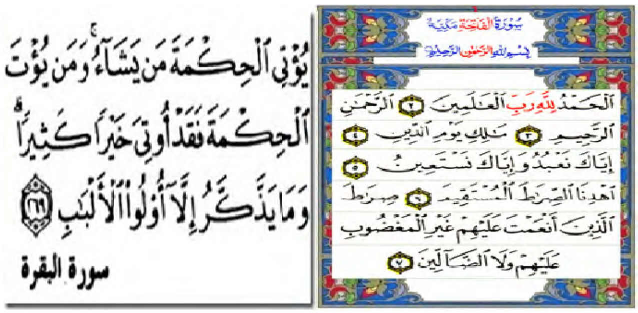
يؤتي الحكمة من يشاء ومن يؤت
الحكمة فقد أوتي خيرا كثيرا
وما يذكر إلا أولوا الألباب ٢٦٩
سورة البقرة
سورة الفاتحة مكية
بسم الله الرحمن الرحيم
الحمد لله رب العالمين ١ الرحمن
الرحيم ٢ مالك يوم الدين ٣
إياك نعبد وإياك نستعين ٤
اهدنا الصراط المستقيم ٥ صراط
الذين أنعمت عليهم غير المغضوب
عليهم ولا الضالين ٧

FIGURE 13. Quranic Images Plain and complex.

for which the key must be generated is not mentioned. In our opinion, the author is calculating the key for the whole document together which is similar to the hashing process. This key is used by certifying authority (CA) for authentication purposes during the decoding phase. The authors' claim regarding novelty of this approach seems rather unsupported. According to the algorithm, Unicode values of all characters are calculated and added to produce a sum. Then the parity bit is added to this sum and the key is generated. Hence, the difference between hashing and zero-watermarking remains unclear [12].

Tayan et al. (2014): This work focuses on the verification of digital text document integrity. This work is similar to the work published by Tayan et al. (2013) in terms of methodology. However, in the previous study, word size related to the generation of the key has not been mentioned. Also, the word limit size has been fixed at two [4].

AlAhmad et al. (2013): This study focuses on protecting the text of the Holy Quran from being tampered with. The authors have combined the two well-known approaches of AES and RSA resulting in a hybrid approach. The authors claim that many attempts have been made to distort the original text of the Holy Quran, for example by using the Galan application. However, there is no proper methodology mentioned regarding the protection of the text. There is no proposed algorithm mentioned nor are there any evaluation experimental results shown in order to evaluate this work [13].

AlAhmad et al. (2013): In this study, the authentication of holy Quranic text images is achieved by an invisible watermarking technique based on LSB. In order to generate the watermark for the pdf file, a DCT algorithm is used to reduce the time of extracting. For tamper detection, the hashing approach is used [14].

Abuhaija et al. (2013): This work centers on the authentication of web-based content. The framework, ITRUST is proposed for website authentication without providing the reader with any implementation details. There is no proper methodology mentioned as to how exactly the web content is authenticated. The general idea seems to be that the Registration authority (RA) is responsible for authenticating the content on websites. However, the role of the watermarking logo provider remains unclear [15].

Izhar et al. (2013): The authors identify the fragile watermarking technique as most suitable for authenticating of Quranic images. The image is divided into blocks, and each block is numbered in a spiral manner starting from the center like a ring form. The numbering is done so that watermarked blocks are relocated a minimum distance away from the original blocks. All blocks are then mapped using the equation (1):

$$B = [(k * s) \bmod Nb] + 1 \tag{1}$$

B is the watermarked block, s is the spiral, Nb is the block numbers, and k is the secret key which is the highest prime number from the result of block numbers divided by 2. In the second phase, the average intensity of each block is calculated by setting LSB of each pixel within the block zero [16].

Sabbah and Selamat (2014): This study classifies Quranic and non-Quranic words available online from Quranic image data sets. A classification model is developed based on the Support Vector Machine (SVM) approach. Based on the SVM classification model, words are extracted from online sources. However, before extracting the words, all symbols, diacritics, non-Arabic letters are removed via a filter. For evaluation purposes, the three parameters accuracy, precision and F-measure are taken. However, it is not mentioned how the algorithm extracts the features [17].

Kurniawan et al. (2013): This study focuses on protecting the Quranic image and authenticating the watermarked Quranic image. The original Quranic image is hashed to obtain the initial authentication code. This authentication code is then encrypted using a private key to obtain a secured authenticated code. This secured code (L) is used to tackle local attacks and is stored in a binary format. Wavelet domain is used to embed this secure code with the host image using DWT transformation. Embedding is done into coefficient wavelet (Ch) at resolution level 1-L. For authentication purposes, the inversion of the whole process is repeated. The authors evaluate the proposed approach on four digital images of the Holy Quran. The tests are performed to evaluate the localization capability of image tampering, fragility to JPEG compression under various quality factors (QF) and the quality of the image after the watermarking process. The proposed technique maintains fine image quality [18].

Kurniawan et al. (2014): The authors use a fragile watermarking approach to protect Quranic images based on wavelet and spatial domain. The same approach they have proposed in their study in the previous year, and we could not find any major differences. In the first phase, authentication bits are embedded into the host image, the output being the watermark image. In the second phase, the watermarked image is authenticated by hashing the whole image. By using a secret key, a secured authentication code is produced to detect any tampering [19].

Kurniawan et al. (2014): This work is similar to the previous work published by the same author except that here a different evaluation parameter is taken. The image is transformed into wavelet domain using DWT. By way of using a block-wise based approach, the image is then divided into several blocks and each block embedded with watermark bits for the authentication purpose. The three parameters PSNR, Pearson Correlation Coefficient (PCC) and Normalized Hamming Distance(NHD) are taken for evaluation purposes [20].

Laouamer and Tayan (2013): The authors propose a watermarking approach based on the SVD technique to authenticate Quranic images available online. The SVD technique involves transforming the image into different matrices and processing each matrix. The advantage of this technique lies in its robustness and security against geometrical attack [21].

Kamsin et al. (2014): This study discusses the need for authentication of the Holy Quran in all formats. The authors explain that with the digitization and increased internet use, there is an acute need to develop a reliable Quran authentication system to detect falsified verses [22].

Gutub et al. (2010): The author claims that due to ease and availability of digital text formats on the internet in the form of websites, articles and e-books, copying and altering texts has become very easy. Digital watermarking is branch of steganography whose main objective is to provide copyright protection and prevent illegal copying and diffusing. Here steganography is used to protect the text of the Quran from tampering. The secret bits are embedded in extensible characters of the Arabic text. The drawback in this kashida based approach is the elongation of characters which takes more space, requires more bytes and occupies more memory [23].

Gutub et al. (2010): The author proposes the kashida based approach to protect the text of the Holy Quran from tampering. The authors use the feature coding technique of watermarking where the security code is embedded with kashida to watermark the image. Kashida is a form of Arabic script with elongated characters. The proposed method serves as good candidate for copy right issues [24].

B. AUDIO/VIDEO BASED FORMAT

There is a considerable amount of Quranic and *hadith* content available online in the form of audio and video recordings such as mp3, mk3, mpeg and mp4. There are many different techniques which can be used for integrity checks. Due to the vast scope of the research, we have not discussed techniques used for this format in detail. However, brief description of some basic techniques is given as follows: In works of Subramanyam and Emmanuel [25] & Wang and Farid [26], different algorithms were proposed to detect temporal and spatial tampering attacks. The parameters used to detect forgery were compression parameters i.e. size, bitrate and frame type. The work of Lin and Delp [27] included the algorithm to detect compression and temporal attacks. Similarly, Cross and Mobasseri [28] proposed algorithm to detect tampering for MPEG-2 format. Some of the recent works in the area of video forgery includes the work of Wang *et al.* [29], that detected forgery in video based on discontinuity points to the optical flow that arises due to forgery. Alshareef and Saddik [34] introduced video forgery method based on detection of frame insertion and deletion. Similarly, rigoni et al. proposed tamper detection method for videos and audio based on extracting the marks that were embedded to host video or audio during protection phase [30]. All these mentioned approaches can be used to preserve content integrity of Digital Holy Quran too with suitable enhancements.

C. TEXT BASED FORMAT

Most internet users prefer to copy Quranic text from a specific source and paste it either on social media websites or other online blogs. This approach can be called binary approach and is one of the easiest and user-friendly approaches. Given the complexity of the Arabic scripts, the text content is divided into the sub-categories plain text and complex text. By plain text is meant simple Arabic script input without any symbols. By complex text is meant the Arabic scripts with added diacritic signs and symbols as shown in Fig. 14. The different formats available are word format, pdf format, etc. In order to provide more overview related to preserving the integrity of Quran and *hadith* texts, the various possible approaches and methods are discussed in section V.

ٱلْحَمْدُ لِلَّهِ رَبِّ ٱلْعَٰلَمِينَ   ٱلحمد لله رب ٱلعلمين

FIGURE 14. Plain and Complex Arabic Text.

As compared to the image based format, less research has been done on text based work. This may be due to the complexity of text based input. Below is given a brief overview of text based approaches:

Alginahi et al. (2013): In this work, an algorithm is proposed for the verification of Arabic verses along with diacritics and all symbols involved. The author claims that the proposed algorithm can detect whole and partial Arabic verses. For evaluation, the two parameters ''verified and authenticated'' and ''tampered with'' are taken. However, the algorithm itself is not mentioned except on the flow chart. From the given flowchart, it seems that this method involves a simple SQL approach using select query which is not the most efficient approach as it needs a particular location to be specified first. Moreover, it is evident from the flow chart that the algorithm removes all symbols and diacritics before converting the text into Unicode format [31].

Alsmadi and Zarour (2015): Here, a model is proposed for the authentication of Quranic verses. According to the author, document control and digital signature are the two mostly widely used approaches. Document control gives permission before and after publishing a document online. Digital signature means that documents should be verified by the person who signed them. The focus is on integrity checking whose challenge lies in the correct reading of the Arabic diacritics. Hashing is used in this research whereby the hash of the particular verse is calculated and the hash value compared with the hash value in the database. The major drawback of this approach is that only single complete verse can be

TABLE 1. Summarised version of research work carried out in image based format.

Authors	Approach Used	Findings	Limitations	Evaluation sources
[12]	Zero -watermarking	Zero-watermarking approach has been identified as effective technique to authenticate image based document	Limited to Image format only. Whole document is hashed similar to hashing	Not any evaluation parameter taken. Only encoding time and decoding time mentioned.
[4]	Hybrid approach of watermarking and digital signature	Zero-watermarking approach has been used to authenticate image based document	Limited to Image format. This approach is prone to fail when text input will be given. Overhead of storing keys	Not any evaluation parameter taken. Only encoding time and decoding time mentioned.
[13]	Cryptography and Hashing.	Hybrid approach of AES and RSA is proposed to protect text document from tampering	1. Lack of proper methodology. 2. No pseudo code of hybrid algorithm mentioned.	No experimental results shown
[14]	Invisible watermarking and hashing	Invisible watermarking approach based on LSB is proposed.	1. Not valid results due to lack of experiments. 2. Limited to Pdf format only	No Experiments done and discussed.
[15]	Watermarking	A general framework regarding authentication of web-site content is proposed.	2. Based on manual authentication mechanism where RA is assigned to authenticate web-sites.	Not experimental. General architecture proposed.
[16]	Fragile Watermarking	Image based authentication of Quranic images based on fragile watermarking is proposed and proposed algorithm shows significant improvement.	Limited to image only.	Top four Quran applications from android have been taken for experimental purposes. Four evaluation parameters i.e. Average processing time, Average PSNR value, detection and recovery are taken.
[17]	Machine Learning Approach	Machine learning approach has been proposed for classifying Quranic words from Non-Quranic words.	Limited to Image format only.	Three parameters i.e. accuracy, precision and F- measure have been taken for evaluation purposes on 4 different data sets.
[18]	Fragile Watermarking	Fragile water marking approach has been proposed to protect quran from tampering.	Limited to Image for mat only	Two metrics i.e. Bit Error rate and PSNR are taken for evaluation purposes.
[19]	Fragile Watermarking	Fragile water marking approach has been proposed to protect quran from tampering.	We could not find any major difference between the two approaches proposed by same author.	Two metrics i.e. Bit Error rate and PSNR are taken for evaluation purposes.
[20]	Fragile Watermarking	Fragile water marking approach has been proposed to protect quran from tampering.	Limited to Image format only. Not any major difference between the previous approaches proposed by same author.	Three parameters i.e. PSNR, Pearson Correlation Coefficient (PCC) and Normalized Hamming Distance(NHD) are taken for evaluation

TABLE 1. ***Continued.*** **Summarised version of research work carried out in image based format.**

				purposes
[22]	Not mentioned	Quran authentication system has been proposed.	This work is just an idea towards developing Quran authentication system.	Simple prototype has been shown, how future Quran authentication system will work.
[23]	steganography	A technique based on steganography has proposed to protect the Quranic document.	Limit to Image only. Needs. There is no experimental evidence to prove this technique is prone to various tampering attacks.	There is no specific metric taken for evaluation purposes.
[24]	Feature code watermarking	A method based on embedding security bits in kashida is proposed.	1. Limited to Image only. 2. Need to test the proposed approach using different kind of attacks.	There is no specific metric taken for evaluation purposes.
[21]	Watermarking	An enhanced approach based on singular value decomposition (SVD) for watermarking the data is proposed	Limited to Image. There are no benchmark results shown from previous work.	For evaluation purposes 5 parameters have been taken: Peak Signal-to-Noise-Ratio (PSNR), Structural Similarity Index (SSIM), Visual Information Fidelity (VIF), the Universal Quality Index, Noise Quality Measure (NQM)

checked at a time. Different verses are tested using different hashing approaches [32].

Sabbah and Selamat (2013): A framework is introduced to detect and authenticate Quranic verses in a text extracted from online sources, especially forum posts. The main purpose is to increase the detection accuracy of the diacritic text. The achieved accuracy on average is 62% and precision and recall 75 % and 78 % respectively. The framework involves extracting three lists from the Quranic script, distinctive Quranic diacritical words, distinctive letters, diacritic signs and symbols. Each letter, diacritic and symbol is given a distinctive weight. After assigning weights to the words, they are grouped into two sets, one with characters and the other with diacritics. However, this algorithm does not work on non-diacritical texts and there is too much overhead associated with calculating weights and dividing verses into two groups. The complexity of the algorithm increases with highly diacritical texts. Five tests are carried out altogether [33], [34].

Alshareef and Saddik (2012): This work proposes a framework for Quranic verse detection. The Quranic verse text is taken as input and the result is displayed as authentic or not. The two major components are Quranic quote filtering and verification. In Quranic quote filtering, all Arabic diacritics and special symbols are removed as they limit the traditional search engines to provide acceptable and accurate results to the users without any valid proof or justification. After removing all symbols and diacritics, the Quranic verification mechanism is used which uses regular expression SQL query to verify the text. The authors use single verses to evaluate their authenticity. Single Arabic words are also used and their results are compared with three Quranic search engines i.e. Muslim-Web, Ketaballah and HolyQuran. The proposed algorithm achieves 89 % accuracy. However, it can be assumed that, this accuracy decreases if the algorithm is used on large Arabic data sets due to the fact that regular expressions use the prefix-suffix approach for searching [34].

Nisha et al (2014): This study discusses the different search engines available online and assesses their limitations. A new search engine with the name of ''Truth-search-now'' is proposed. Five search engines with respect to Islamic content are chosen, TheIslamic search, IntoIslam, Search-truth, IslamiCity, and Allah.pk and evaluated based on the time taken by each search engine to conclude a particular query. No experimental proof is given or any algorithm mentioned. Moreover, the proposed site (www.truth-search-now.com) cannot be located online [35].

Given the existing research, it can be concluded that numerous issues have remained unsolved, such as accuracy and, precision related to detection and authentication of Quranic verses. More efforts are needed to address these problems. Besides, the availability of so many different techniques has resulted in confusion rather than clarity. In order

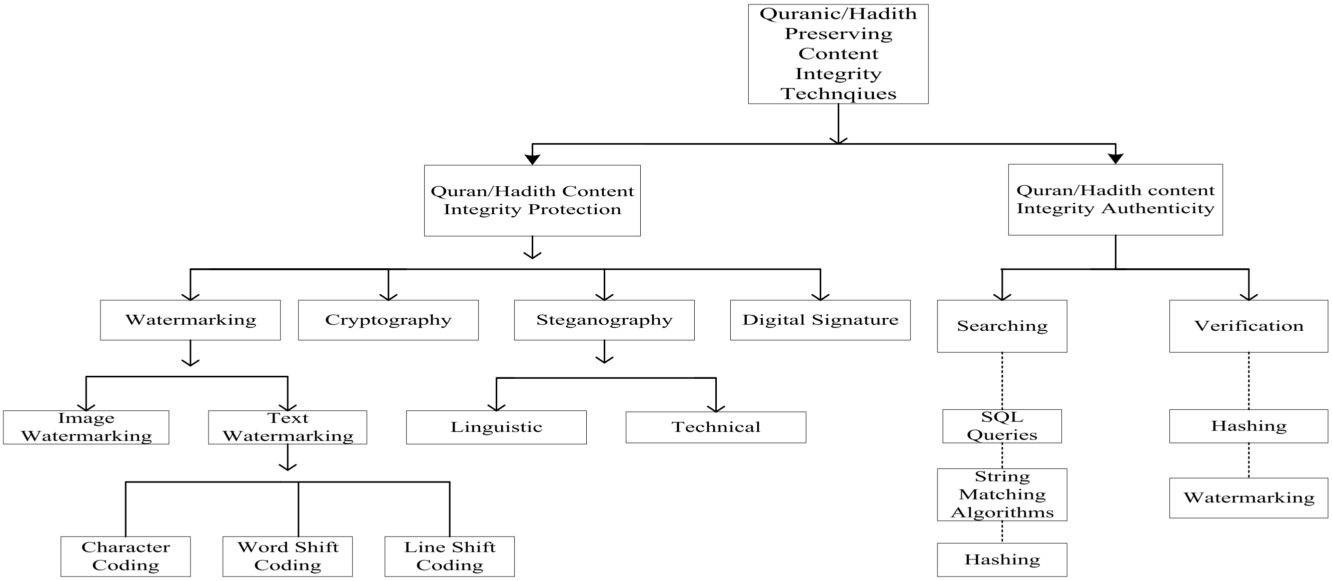

FIGURE 15. Taxonomy Based on Preserving Content Integrity.

to address this problem, the next section presents a summarized view of the methodologies underlying these possible techniques used in the protection and verification of excerpts of the Holy Quran. Other possible techniques are also addressed.

V. SUMMARY OF TECHNIQUES USED FOR PRESERVING THE INTEGRITY OF THE QURAN

We find that the above reviewed techniques need to be properly classified and their scope narrowed down. Such a classification can assist future researchers in selecting the most appropriate technique for the specific problem they study. Generally, a user has two concerns while reading the Quran or hadith online. The first and foremost concern is that of authenticity or integrity meaning, how to verify whether or not a particular hadith or verse is accurate and correct. The second concern is that of protection meaning how to protect the verified content data from undue alteration or other modification. Keeping these two concerns in mind, a new taxonomy based on content integrity approaches is proposed and classified into content integrity protection and content integrity authenticity as shown in Fig.15.

Content integrity protection can be defined as the approach which focuses on protection from possible tampering or modification. It is subdivided into the well-known approaches of watermarking, cryptography, steganography and digital signature. On the other hand, content integrity authentication which means to verify a content based on a verified source is categorized into searching phase and verification phase. In data integrity authenticity, a user wants to check whether or not a particular verse or *hadith* is correct. In order to do so, the required source has to be searched. Once the required source is located, verification can be done to check accurateness. The main factors that any content integrity protection and verification mechanism must have are as follows [36]–[38]:

1. Imperceptibility: It means the property of being invisible. The document to be protected from tampering much have security feature embedded within it such that it is not noticeable to audience [39], [40].
2. Robustness: The secured approach must be robust enough to tolerate any kind of attacks [39]–[41].
3. Security: The approach used for preserving content integrity must be secure enough to satisfy the condition of robustness [39].
4. Computational cost: The approach used to preserve content integrity of documents must be scalable in future on future computers with less computational overhead [39].

Based on these factors, different techniques can be used for data integrity protection. A brief description of each technique is given below under respective sections.

A. QURANIC/HADITH CONTENT INTEGRITY PROTECTION

As mentioned above, content integrity protection is the approach where all possible techniques which are being employed for protection of a particular content or can be used for protection are put together. Below follows the brief description of each approach:

Watermarking: Watermarking is one of the most widely used techniques for protecting digital media from possible modification or tampering. There are two types of watermarking: text watermarking and image watermarking. In image watermarking, a piece of information like a company logo or text is added to digital media like image and video for securing the content and owner identification [42]. Similarly, in text watermarking, a text is modified by way of line coding, word-shift coding and character

TABLE 2. Summarised version of research work carried out in text based format.

Authors	Approach Used	Findings	Limitations	Evaluation sources
[31]	SQL Query Approach	Algorithm has been proposed for detection of particular Arabic verse.	1. Not efficient enough as Major user need to know the particular verse to be verified is from which chapter. The approach is prone to fail if user don't know the surah name. 2. The algorithm will fail if there is last verse of one surah and first verse of consecutive surah.	Two parameters i.e. "verified and authenticated" and "tampered with" are taken.
[32]	Hashing	A method based on hashing to authenticate and verify Quranic verse.	1. Suitable for single verse only. 2. Hash Collision can occur. 3. Diacritic and non-diacritic Arabic verse will give different hash values.	No performance metric evaluated. Evaluation done based on comparing hash values of different text.
[33]	SQL Query approach	A Framework has been proposed to detect and authenticate Quranic text.	1. Not suitable for non-diacritical text. 2. Complexity of the algorithm will increase with more complex diacritical verse.	Accuracy, Precision and recall have been taken as evaluation parameters
[34]	Regular Expression approach using SQL queries.	A Framework is proposed which can authenticate Quranic verses.	For finding a particular verse, user need to enter surah-name also which is one of the major limitation of this approach.	For Evaluation purposes, accuracy metric has been taken and benchmarked with Ketaballah.net, Muslim-web.com, Holyquran.net
[35]:	ASP.dot Net platform has been used to develop the system	A new search engine "truth-search-now" has been proposed.	1. Could not locate the proposed engine online.	Performance of 5 search engines with respect to Islamic content have been evaluated by measuring search time.

coding. In line coding, the text is altered by inserting the watermark [43]–[45]. In word shifting, the location of the word is altered for the purpose of watermarking. The unmoved words serve as reference locations during the decoding process [43]. In character or feature based coding, coding is related to features of character. The feature of a character is changed to embed a security code for verification purposes. The height of an individual character can be altered or its position with respect to other characters. For the decoding process, some characters are left unchanged [43]. The watermark can be fragile, semi-fragile or robust depending on the application to be applied upon. Fragile and Semi-fragile watermarking is generally used for content authentication that can tolerate attacks such as compression and noise. Robust watermarking on the other hand embeds watermark tightly within the host document so that removal of watermark is difficult and is used mostly for copy-right protection. Robust watermark is generally detectable compared to fragile and semi-fragile watermarking approaches [46].

Cryptography: In terms of security, cryptography constitutes the standard technique. Its many applications include credit cards and banking transactions. In cryptography, the text easily readable by the human eye is converted into an unreadable text or cipher text to make it inaccessible to any third or unauthorized person. Encryption, generation of keys and decryption are the three most important phases in cryptography. Encryption is the process of converting plain text into cipher text. Decryption is the reverse of encryption. Keys are used to unlock the encryption phase [47], [48]. The main advantages of cryptography are securing confidential information between sender and receiver, authentication for

TABLE 3. Advantages/drawbacks of standard approaches.

Image based Approaches	Advantages	Drawbacks
Watermarking	Has the additional requirement of robustness against possible attack [61]	Lot of attacks possible in the form of geometric, noise and other related attacks
Cryptography	Main task is to ensure users able to communicate securely over an insecure channel [62]	More suitable for network related attacks as compared to digital documents[63]
Steganography	Message can be sent without any suspicion. Suitable for securing transmitted messages involving encoding and decoding process	Less secure. Not suitable for preserving integrity of sensitive documents like image or text [64]
Digital signature	very efficient in legally binding documents	Both senders and recipients need to buy digital certificates from trusted certification authorities

proof of identity, integrity check to make sure the message is not tampered with and non-repudiation, which does not allow the sender to claim that he or she did not send any message [49]–[51].

Steganography: Steganography is an information hiding technique where data are hidden in a cover media to make that information inaccessible to others [52]. The difference between cryptography and steganography lies in the fact that the former deal with the protection of content of message while the latter conceals the existence of the original message [53]. The idea is to embed the original message in a cover and send it secretly to the destination. The Stego key is used to restrict detection or recovery of the original message [53]–[56]. It can be further sub-divided into:

- Linguistic Steganography: Linguistic steganography entails data hiding in which information is embedded in a cover text in a way that is invisible to the outside observer [54].
- Technical Steganography: In technical steganography, a carrier is used to hide the actual message like ink dots. In ink dots, there is a specific letter in each drop specifying certain information [57].

Digital Signature: Digital signature constitutes a mathematical technique used to authenticate and validate the integrity of any particular message or digital document [58]. This technique is useful to detect any kind of tampering or impersonation in digital communications. Although this technique comes under the category of cryptography based on its asymmetric approach, we prefer not to include this technique under cryptography due to lot of possible future directions in the field of digital signature. One way hash of electronic data to be signed is created. For encrypting this hash, a private key is used. Thus, the combination of hashing and encrypting using a private key makes digital signature [59], [60].

The main advantages and drawbacks of all the standard approaches mentioned above is listed in Table 3.

Among all these approaches, we find watermarking as the potential approach that can be used to develop complete protection and authentication system for Quranic materials. Thus, based on review of related works presented in Table 1, research works involving watermarking for content integrity protection of Holy Quran are explored based on important factors of imperceptibility, robustness, security and computational cost in Table 4.

From the above analysis, it can be observed that all related work has certain limitations in terms of security, robustness to different kinds of attack and other related issues. Fragile/Semi-Fragile methods are more prone to geometrical attacks compared to robust based methods. Similarly, robust based methods are more detectable compared to Fragile/Semi-Fragile methods. Hence, there is need of an efficient water-marking approach that can achieve better results compared to existing methods irrespective of being fragile/ semi-fragile or robust.

B. QURANIC CONTENT INTEGRITY AUTHENTICITY

Content integrity constitutes one of the key issues of reading a particular Quranic Verse or *hadith*. Based on the mode of operation, content integrity authenticity can be divided into the two sub-categories of searching and verification. For both of these phases, the two important factors are accuracy and time complexity.

1) SEARCHING

Quran or *hadith* both are originally recorded in the Arabic language. Many Muslims know how to read Arabic but are not able to detect any undue modification. In order to check the authenticity of a specific verse or *hadith*, the first step is to search that specific verse or *hadith* and match the same

TABLE 4. Summary of watermarking approaches used for preserving content integrity of digital Quran.

Watermarking approaches	[12]	[4]	[16]	[18]	[19]	[20]	[24]	[21]
Imperceptibility	×	✓	×	✓	✓	×	×	×
Robustness	×	×	×	×	✓	✓	×	✓
Security	×	×	×	Malicious and non-malicious attacks are difficult to be distinguished among each other [41]	×	Malicious and non-malicious attacks are difficult to be distinguished among each other [41]	×	×
Computational cost	✓	✓	✓	×	×	×	×	×

TABLE 5. Drawbacks of content integrity authenticity approaches.

Phases	*Approaches*	*Drawbacks*	*Recommendation*
Searching	SQL query	Linear time complexity if Index not provided. In case Index is provided, user need to make sure the input verse belongs to which chapter. Prone to SQL injection attacks	Not Suitable for Quranic Databases.
	String Matching	Results in slower performance with respect to processing time for Non-ASCII based texts.	Potential approach to search and verify Quranic verses.
	Hashing	Might result in hash collision. Overhead associated in case many single Quranic verses need authentication.	Not recommended for authenticating single Quranic quotes. Recommended for whole/multiple pages.
Verification	Hashing	Hash collision and overhead in computing hash values for multiple single Quranic quotes.	Not recommended.
	Brute force	Linear time complexity (more processing time).	Efficient approach for verifying Quranic verses provided time complexity can be reduced.
	Watermarking	Prone to many attacks like geometric, noise if Image logo embedded in plain text. In case of bits embedded in plain text, overhead associated in making it secure.	Not recommended based on number of possible attacks and overhead associated with watermarking for plain text.

with a verifiable source. In the matching and searching phase, one of the fundamental requirements is the availability of the verified content, i.e. an authentic database. If there is no verified content, the data integrity check is bound to fail. It is proposed to classify search phase in the following three subcategories:

- *SQL queries:* SQL constitutes a standard database [65]. SQL is a query based scripting language, and the queries available in SQL are used for searching particular content. Some of the powerful search operators in SQL are SELECT and LIKE. However, the use of regular expressions which includes prefixes and suffixes is also used in the searching phase [34], [65].
- *String Matching algorithms:* String matching algorithms are classified into exact matching algorithms and approximate matching algorithms. There are many algorithms which can be used to search a particular query, such as Boyer-Moore, Rabin Karp and KMP algorithms which are considered as the standard string matching algorithms [66], [67].
- *Hashing:* Hashing or Message Digest (MDs) both mean the same, namely a one-way process where strings of characters are converted into a key or a value of fixed length. It is considered as a fast process to retrieve items from the data base [68]. These techniques are more concerned with accuracy rather than performance overhead. Hashing approaches have the problem of exchanging public-keys between many communicating parties. Some of the most commonly used hash approaches are Message digest 2 (MD2) (RFC 1319), MD 4 (RFC 1320), MD 5 (1321), Secure Hash (SHA) and keyed Hash Message authentication code (HMAC). MD 2, MD 4 and MD 5 are also known as message digests suitable for hashing digital signatures into shorter values. Similarly, the SHA family is suitable for making larger message digests [68].

2) VERIFICATION

The verification phase constitutes the next stage in the content integrity process. Although both searching and verifying are interrelated processes, sequence wise verification is the final phase. There may be other verification mechanisms but we propose the following three verification approaches:

- *Hashing Process:* In hashing, strings of characters are transformed into a specific key representing the original string. To check the integrity of that same string, the hash value is calculated and compared. If the hash values are the same for both the documents, the data are correct and accurate. In case the hash values do not meet the signified string, they have been modified and are not authentic.
- *Brute Force Process:* In the brute force approach, each character is checked one by one to be sure of data correctness and accurateness. Although this approach is quite simple and secure, it can take lot of time and space to process long files. However, this approach is efficient for short strings and produces accurate results.
- *Watermarking:* Watermarking can also be used for data integrity checking. A watermark or any logo can be used to authenticate a particular document or image.

The main drawbacks of all the standard approaches mentioned above is listed in Table 5.

After analyzing all the standard approaches that has been used for determining authenticity of text based Quranic verses, we find SQL approach promising approach to achieve the desired task. Based on review of related works presented in Table 2, research works involving SQL based approaches were explored based on important factors of accuracy and time complexity are presented in Table 6.

From Table 6, it can be observed existing works using SQL approaches have several drawbacks for authenticating Quranic content. Firstly, one of the important performance measure i.e. time complexity has not been taken into consideration. Secondly, two popular algorithms used in MYSQL i.e. linear search and binary search [69] have been used for searching and verifying the verse. Linear algorithm increases search time while as binary search algorithms need index approach with efficient queries which limits the capability of searching to specific index only. Hence, an alternative approach is needed to enhance the search and verification phase for searching and authenticating Quranic texts.

Efforts have been made to keep all basic concepts simple and lucid so that beginners can grasp the concepts quickly and easily. The last and final taxonomy is related to the possible attacks which can be directed against Quran and *hadith* content. This final taxonomy is presented in section VI.

VI. POSSIBLE ATTACKS ON THE INTEGRITY OF QURAN AND HADITH CONTENT

Since as lot of Quran and *hadith* content is retrievable in image or text format, any possible attacks can be classified as image and text related attacks as shown in Fig. 16.

A. IMAGE RELATED ATTACKS

There are measures to be taken to protect verified and authentic images. A number of approaches has been used to tamper with the content of images. The most common attacks are as follows:

- Removal attacks: These attacks consist of removing or destroying the watermark in the form of remodulating, collusion, denoising and quantization.
- Cryptographic attacks: These attacks consist of finding vulnerabilities in the algorithm which embeds the watermark unto the host data. Examples are oracle and brute force.
- Geometric attacks: In these attacks, operations on pixel level like scaling of image, rotation and pixel shifting are carried out which degrade the quality of the watermark.
- Protocol attacks: Here ownership information is destroyed or the watermarked image is changed.
- Forgery attack: The image is changed by deleting some part or inserting something new. Even the background can be changed.

Some of the attacks available in Matlab include Gaussain noise, Peeper salt noise, Speckle noise, Intensity

TABLE 6. Summary of watermarking approaches used for preserving content integrity of digital Quran.

SQL based approaches	[31]	[33]	[34]
Accuracy	×	✓	✓
Time Complexity	×	×	×

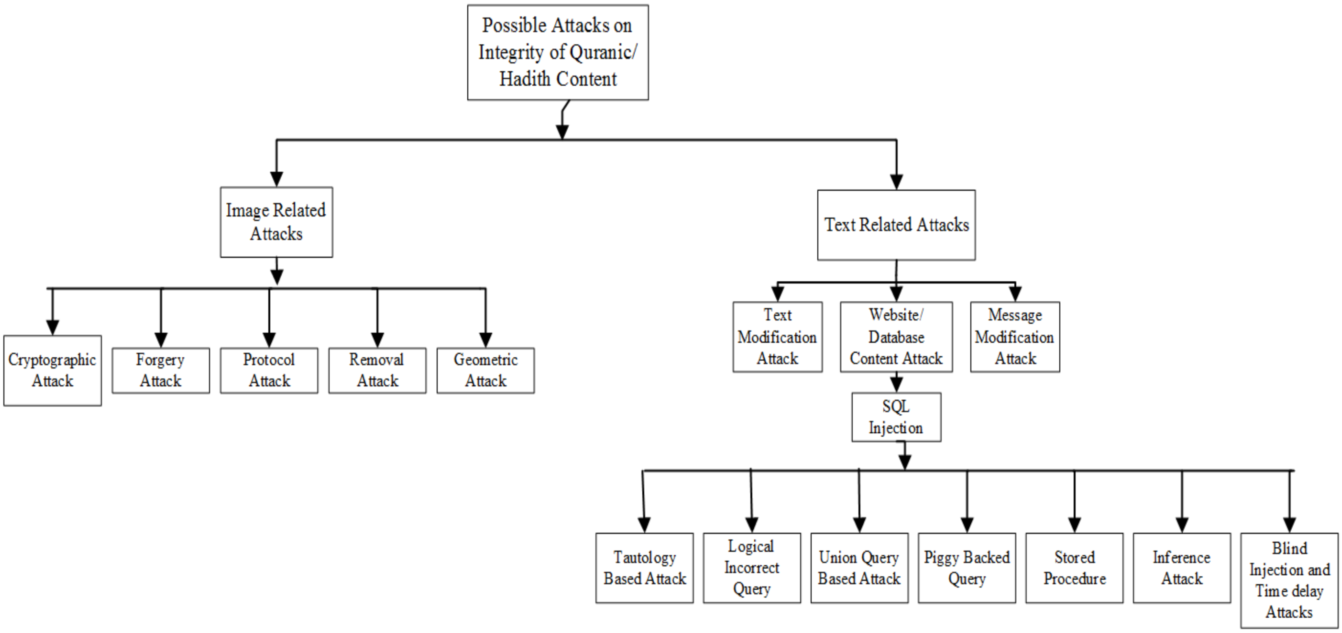

FIGURE 16. Possible Attacks on Integrity of Quran/Hadith.

transformation and Blurred Image [70], [71]. The above mentioned attacks were classified further based on the works of [40], [72], and [73] and state of art presented in Table 4 were explored based on their strength and drawbacks as shown in Table 7.

It can be observed from Table 7, most of the watermarking approaches proposed for preserving the content integrity of Holy Quran have not been tested against the attacks. Few works like [19] and [21] has tested their respective approaches against geometric and noise attacks. Thus, there is need to evaluate the strength of all these approaches against all kind of attacks presented in Table 7 to protect the sacredness of Holy Quran due to its sensitive nature.

B. TEXT RELATED ATTACKS

It is easier to tamper with a text than with an image. There are a lot of ways in which a text can be edited or modified [74], [75].

i) Text Modification Attack: In a text modification attack, the aim is to modify the text. The three operations commonly used include deletion, insertion and substitution. By deletion is meant that attacker deletes lines in a text or a symbol in a sensitive text which can change whole meaning of the sentence. Using insertion operation, the attacker inserts content which can change the theme of the original message. Substitution occurs when key words are replaced with other words in order to alter the original message [74], [75].

ii) Website Content Attack: **E**ach website possesses an authentic database at the back end of the system. This database is of critical importance for the host as well as attacker. If the attacker gains access to this database, he or she can modify the content accordingly. For this very purpose, the most widely approach is SQL injection whereby attackers provide data through SQL queries in such a way that the host database accepts those queries as its own. By taking advantages of this vulnerability, an attacker can modify the host database [76]. The SQL query is modified by using new keywords or operators. The various mechanisms of SQL injection include: (i) Injection through user input through HTTP Post and Get sessions; (ii) injection through cookies where a malicious user can make use of client cookies to build SQL queries and attack; (iii) injection through server variables which include HTTP headers; (iv) and finally second order injection attack where malicious inputs are

TABLE 7. Evaluation of attacks on watermarking based approaches presented in Table 4.

Related works		[10]	[18]	[19]	[20]	[21]
Performance Metric taken		processing time, PSNR, detection and recovery	BER, PSNR	BER, PSNR	PSNR, PCC and NHD	PSNR, SSIM, VIF, Universal Quality Index, NQM
Compression		✗	✓	✗	✗	✓
Noise Attack	Pepper & salt noise	✗	✗	✗	✗	✗
	Speckle noise	✗	✗	✗	✗	✗
	Gaussian noise	✗	✗	✗	✗	✓
Histogram equalization Attack		✗	✗	✗	✗	✗
Filtering Attack	Median filtering	✗	✗	✗	✗	✓
	Gaussian filtering	✗	✗	✗	✗	✗
	Wiener filtering	✗	✗	✗	✗	✗
	Sharpening	✗	✗	✓	✗	✗
Geometric Attack	Scaling	✗	✗	✗	✗	✗
	Rotation	✗	✗	✓	✗	✓
	Shift	✗	✗	✗	✗	✗
	Cut	✗	✗	✗	✗	✗
	Shearing	✗	✗	✗	✗	✗
	Translate	✗	✗	✗	✗	✗
	Collage/replacement✓	✗	✓	✗	✓	✗

used to trigger SQL injection indirectly. The possible intent of attacks may be identification of the injectable parameter, finger-printing database, extracting sensitive data, tampering of data, denial of service and bypassing authentication [43].

iii) Message Modification Attack: In this type of attack, the attackers replace the whole content with their own. For example, Bob sends a message A to Jack who receives message B instead of A. Although, there are ways to prevent message modification, hackers have the tools which allow them to change the whole message. It is recommended that future research would survey all the different techniques available today in order to devise mechanisms to prevent such message modification attacks.

Based on above mentioned attacks, work done to authenticate and verify Quranic texts presented in Table 2 were explored to look for limitations and other performance metrics. Weaknesses of existing works related to text format are listed in Table 8.

From the Table 8, it can be observed, no existing works have evaluated their respective approaches against these possible attacks. Thus, there is immense scope of future work in the area of security too with respect to text based formats.

In the above discussion, three possible attacks with respect to data integrity have been discussed with the aim to provide a brief yet comprehensive overview. There is lot of research yet to be done in this area, and the taxonomy presented can be refined further in future.

VII. OPEN ISSUES, CHALLENGES AND POSSIBLE SOLUTIONS

A. NEED OF AN APPROPRIATE AUTHENTICATION APPROACH

From the above discussion, it can be observed that there are different approaches that can be used to preserve and authenticate digital Holy Quran on internet. Watermarking, SQL and String matching techniques seem to be promising approaches that can be used to develop complete Quran authentication system. However, keeping the sensitivity of Holy Quran into consideration, developing of such an approach that can perform better in terms of security, robustness, computational costs, imperceptibility and other related parameters compared to existing methods is still an open issue and need more research efforts. In this case, watermarking, string matching and SQL approaches can be explored further for more efficient solutions.

B. RELIABLE DATABASE FOR AUTHENTIC AND VERIFIED QURAN AND HADITH CONTENT

When carrying out research and checking of the validity of different approaches, knowledge of a reliable and authentic database is of utmost importance. Although there

TABLE 8. Evaluation of attacks on text based approaches presented in Table 2.

Related Works	[31]	[32]	[33]	[34]	[35]:
Performance metrics	Verified and tampered with	No specified metric taken	Accuracy, precision and recall	Accuracy	Search time
Text modification attack	Deletion	×	×	×	×
	Insertion	×	×	×	×
	Substitution	×	×	×	×
	Reordering	×	×	×	×
SQL – injection attack	Tautology based attack	×	×	×	×
	Logical Incorrect Query	×	×	×	×
	Union Query based attack	×	×	×	×
	Piggy backed query	×	×	×	×
	Stored Procedures	×	×	×	×
	Web-Site based/Inference Attack	×	×	×	×
	Blind Injection and Time delay attacks	×	×	×	×
Message Modification attack		×	×	×	×

are reliable databases available such as tanzil.net, one can never be sure whether or not each piece of information displayed on the website is reliable. A possible solution for this problem is to develop an authentic database and have the content verified by an authorized Islamic religious body. The first challenge, however, would be to make all *hadith* collections available when creating such a database.

C. AVAILABILITY OF QURAN AND HADITH APPS IN MOBILE PLATFORM OPERATING SYSTEMS

The number of mobile users is continuously increasing as shown in Fig. 17 based on data made available by Comscore. In fact, the number of mobile users has already crossed the number of desktop users since 2014. The popularity and use of mobile platforms like android, IOS and Symbian is rapidly increasing.

The easy access to Quran and *hadith* applications on these platforms is one of the most challenging issues. The majority of Muslims around the world are downloading and following these applications blindly. There is no proper mechanism which can verify the reliability of these applications. This trend is worrisome and calls for proper measures to be taken. One possible solution is to identify all Quranic applications and then manually evaluate each application, although this approach is admittedly very tedious and cumbersome. Another approach is to develop a system, which can access all the content of an application automatically and verify it. Also, signature verification may be followed by collaboration with a Google team to help in verifying authentic applications. This issue constitutes indeed a major challenge and calls for more rigorous analysis and research.

D. IDENTIFICATION AND BLACKLISTING OF FAKE ISLAMIC WEBSITES

Lot of websites claim to be managed by Islamic scholars or other Islamic religious bodies. However, in actual practice, these websites have been created for the sole purpose of misguiding Muslims and non- Muslims alike by offering false information through fabricated *hadiths* and misinterpreted Quranic verses. This issue is again a very challenging problem. These websites are developed by unknown individuals or parties who quote Quranic verses out of context and mislead those users who are still unfamiliar with the Quranic message. The following website is one example of such abuse. (http://www.thereligionofpeace.com/quran/023-violence.htm). On this website, all Quranic quotes have been quoted out of context and have been developed to give the impression that Islam promotes violence. There are hundreds of such websites. One way of addressing this grave problem is to blacklist these kinds of websites after proper identification using suitable key words or develop an automatic system based on key-word search which can help in identifying those websites so that proper action can be taken.

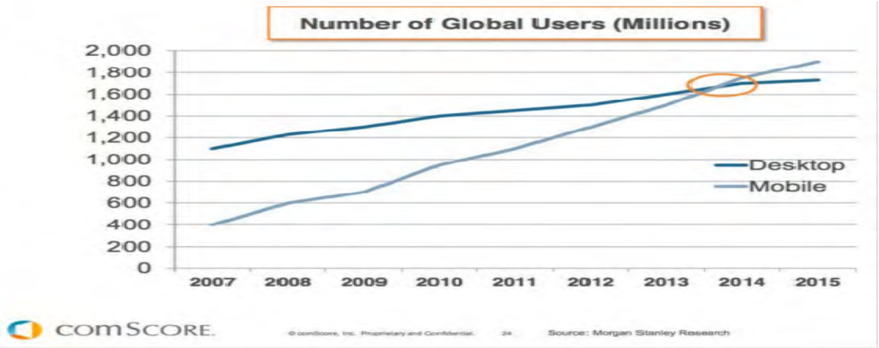

FIGURE 17. No of Mobile Users [77].

E. FABRICATED HADITH DETECTION SYSTEM

Hadiths are sayings and reported actions of Prophet Mohammad (PBUH) and constitute the second most valuable reference after the Holy Quran. There are lot of *hadith* collections containing thousands of traditions made available online which makes it nearly impossible for the average Muslim to distinguish between authentic and fabricated ones. Thus, lot of fabricated *hadiths* are readily accessible online with no proper way to immediately verify the authenticity of the same. These fabricated *hadiths* can be found on social media websites, online blogs and on regular websites. Again, this problem is too complex and challenging as it is not possible to stop people from posting fabricated *hadiths*. A possible solution would be to develop authentic databases of all *Sahih* collections certified by an established religious body. This database can then be used to develop an authentic *hadith* based website where users can check whether a particular *hadith* they have come across on the internet is authentic or fake. Since the Muslim community is a global community, such a system would have to be multilingual.

F. ONLINE LIBRARY

There is a dire need for an online library where all proposed algorithms with respect to preserving data integrity of the Quran and *hadith* can be made readily available to the researchers. Such a reliable online library can be of great assistance to future researchers who wish to test those algorithms and propose more efficient approaches with high accuracy and precision. GitHub is one of the most useful and efficient databases in this respect.

G. MESSAGE OF PEACE SYSTEM

Islam is the religion of peace. Given the negative and misleading associations of Islam with violence, terrorism and aggression which dominate all public media today, the original message of Islam as espoused in the Holy Quran must be made available to all people around the world. Although there are already numerous social media websites available which are trying to accomplish just that, their scope remains limited. A separate system needs to be put into place such as online teaching sites, where all basics of the Quran along with important moral and ethical guidelines can be taught to non-Muslims and Muslim alike.

H. PILGRIMAGE TEACHING SYSTEM

Islamic practice consists of several rituals which require proper instruction and allow Muslims to observe them correctly. The Hajj constitutes one of the most important obligations and memorable events in a Muslim's life for which Muslims need to save up a lot of money and wait many years before they are able to execute it. Therefore, a very efficient approach would be to merge this system with a Quran and *hadith* detection system. This would enable users not only to learn about this specific ritual but also access authentic Islamic sources at the same time.

I. ARABIC TEXT PATTERN RECOGNITION USING IMAGES

Pattern recognition constitutes highly researched area of study. The process of verifying content in the form of images, particularly in Arabic, remains a challenging and open issue. There are lot of minor problems in this area, such as the extraction of overlapping Arabic characters in an image and text retrieval from images using different writing styles. This area needs further research in order to identify further issues. Possible solutions may lie in the use of segmentation techniques and machine learning approaches.

J. NUMERICAL STRUCTURE OF HOLY QURAN

There have been some observations that Holy Quran is numerically structured based on number 19. The opening verse of Holy Quran i.e. "In the Name of God, Most Gracious, Most Merciful" (بسم الله الرحمن الرحيم), is of 19 Arabic letters. Similarly, the first chapter of Holy Quran revealed to Prophet Mohammad (Pbuh) i.e. Chapter 96 (Embryo) also contains 19 verses. There are many such examples in Holy Quran related to number 19. Hence, it will be interesting research work to authenticate Holy Quran based on numerical analysis.

K. EXPERT REAL TIME QURANIC VERSE DETECTION SYSTEM

The ready availability of Quranic content on the internet has made it very convenient for Muslims and non-Muslims to read up on any issue online. However, this convenience comes at a cost. Since the original Quran was revealed in Arabic and the majority of Muslims are not Arabs, and often only know how to recite selected verses from memory, they are dependent on translations. The reader unfamiliar with the Arabic language will need the help of diacritic signs and symbols to read the script correctly. Thus, there is the need to develop an efficient system that can detect and inform users of possible changes in a specific verse. In recent years, some efforts have been made in respect to verse verification but they are not efficient enough in terms of accuracy and precision.A possible solution is to identify suitable encoding techniques and identify weaknesses in the present string matching approaches. For evaluation purposes, the two parameters to be taken are accuracy and precision.

The above-mentioned points constitute a selection of the major challenges and open issues together with possible solutions and recommendations for future research. It is ceded that there are many other issues which only the future will reveal and only future research can address.

VIII. CONCLUSION

This paper reviews recent studies on Digital Holy Quran authentication, protection and integrity authenticity. There are numerous issues in this area which call for a resolute and timely response in the form of intensified research efforts. Quran authentication and protection faces many challenges, foremost improving the accuracy and precision of text detection. In this article, the most common challenges are pointed out and solutions are proposed. A brief overview of the existing research in this field is given, the possible limitations assessed and their findings evaluated. The promising directions which future research should take as discussed in section VII include the call for a reliable universal database of authentic and verified Digital Quran and hadith content, another major task for future researchers is to develop the Expert Real Time Quranic Verse Detection System with improved accuracy and precision.

REFERENCES

[1] J.-S. Pan, H.-C. Huang, and L. C. Jain, *Intelligent Watermarking Techniques*, vol. 7. Singapore: World scientific, 2004.

[2] R. Chamlawi and A. Khan, "Digital image authentication and recovery: Employing integer transform based information embedding and extraction," *Inf. Sci.*, vol. 180, no. 24, pp. 4909–4928, Dec. 2010.

[3] (May 1, 2016). [Online]. Available: http://www.internetworldstats.com/stats.htm

[4] O. Tayan, M. N. Kabir, and Y. M. Alginahi, "A hybrid digital-signature and zero-watermarking approach for authentication and protection of sensitive electronic documents," *Sci. World J.*, vol. 2014, 2014, Art. no. 514652.

[5] Y. O. M. Elhadj, "E-halagat: An E-learning system for teaching the Holy Quran," *Turkish Online J. Educ. Technol.*, vol. 9, pp. 54–61, Jan. 2010.

[6] A. Muhammad, Z. ul Qayyum, W. M. Muhammad, S. Tanveer, A. M. Martinez-Enriquez, and A. Z. Syed, "E-Hafiz: Intelligent system to help muslims in recitation and memorization of Quran," *Life Sci. J.*, vol. 9, no. 1, pp. 534–541, 2012.

[7] M. K. Khan and Y. M. Alginahi, "The holy Quran digitization: Challenges and concerns," *Life Sci. J.*, vol. 10, no. 2, pp. 156–164, 2013.

[8] *Qur'an Manuscript Public Display*, Bharathiar Univ., Coimbatore, India, Dec. 2015.

[9] J. D. McAuliffe, *The Cambridge Companion to the Qur'ān*. Cambridge, U.K.: Cambridge Univ. Press, 2006.

[10] M. F. Hilmi, M. F. Haron, O. Majid, and Y. Mustapha, "Authentication of electronic version of the Holy Quran: An information security perspective," in *Proc. Taibah Univ. Int. Conf. Adv. Inf. Technol. Holy Quran Sci.*, Dec. 2013, pp. 61–65.

[11] B. Sadeghi and U. Bergmann, "The codex of a companion of the prophet and the Qur'ān of the prophet," *Arabica*, vol. 57, no. 4, pp. 343–436, Jan. 2010.

[12] O. Tayan, Y. M. Alginahi, and M. N. Kabir, "An adaptive zero-watermarking approach for text documents protection," presented at the Int. Conf. Adv. Comput. Inf. Technol., 2013.

[13] M. A. AlAhmad, I. Alshaikhli, and B. Jumaah, "Protection of the digital Holy Quran hash digest by using cryptography algorithms," in *Proc. Int. Conf. Adv. Comput. Sci. Appl. Technol. (ACSAT)*, Dec. 2013, pp. 244–249.

[14] M. A. AlAhmad, I. Alshaikhli, and A. E. Alduwaikh, "A new fragile digital watermarking technique for a PDF digital Holy Quran," in *Proc. Int. Conf. Adv. Comput. Sci. Appl. Technol. (ACSAT)*, Dec.'2013, pp. 250–253.

[15] B. Abuhaija, N. Shilbayeh, and M. Alwakeel, "Security protocol architecture for website authentications and content integrity," in *Proc. World Congr. Comput. Inf. Technol. (WCCIT)*, Jun. 2013, pp. 1–6.

[16] S. I. Hisham, A. N. Muhammad, J. M. Zain, and G. Badshah, "Localization watermarking for authentication of text images in Quran with spiral manner numbering," in *Proc. Taibah Univ. Int. Conf. Adv. Inf. Technol. Holy Quran Sci.*, Dec. 2013, pp. 24–29.

[17] T. Sabbah and A. Selamat, "Support vector machine based approach for quranic words detection in online textual content," in *Proc. 8th Malaysian Softw. Eng. Conf. (MySEC)*, Sep. 2014, pp. 325–330.

[18] F. Kurniawan, M. S. Khalil, M. K. Khan, and Y. M. Alginahi, "Authentication and tamper detection of digital Holy Quran images," in *Proc. Int. Symp. Biometrics Secur. Technol. (ISBAST)*, Jul. 2013, pp. 291–296.

[19] F. Kurniawan, M. S. Khalil, M. K. Khan, and Y. M. Alginahi, "DWT+LSB-based fragile watermarking method for digital Quran images," in *Proc. Int. Symp. Biometrics Secur. Technol. (ISBAST)*, Aug. 2014, pp. 290–297.

[20] F. Kurniawan, M. S. Khalil, M. K. Khan, and Y. M. Alginahi, "Exploiting digital watermarking to preserve integrity of the digital Holy Quran images," in *Proc. Taibah Univ. Int. Conf. Adv. Inf. Technol. Holy Quran Sci.*, Dec. 2013, pp. 30–36.

[21] 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," *Life Sci. J.*, vol. 10, no. 2, pp. 2591–2597, 2013

[22] A. Kamsin *et al.*, "Developing the novel Quran and Hadith authentication system," in *Proc. 5th Int. Conf. Inf. Commun. Technol. Muslim World (ICT4M)*, Nov. 2014, pp. 1–5.

[23] A. A.-A. Gutub, W. Al-Alwani, and A. B. Mahfoodh, "Improved method of arabic text steganography using the extension 'Kashida' character," *Bahria Univ. J. Inf. Commun. Technol.*, vol. 3, no. 1, pp. 68–72, Dec. 2010.

[24] A. A.-A. Gutub, F. Al-Haidari, K. M. Al-Kahsah, and J. Hamodi, "e-Text watermarking: Utilizing 'Kashida' extensions in arabic language electronic writing," *J. Emerg. Technol. Web Intell.*, vol. 2, no. 1, pp. 48–55, Feb. 2010.

[25] A. V. Subramanyam and S. Emmanuel, "Video forgery detection using HOG features and compression properties," in *Proc. IEEE 14th Int. Workshop Multimedia Signal Process. (MMSP)*, Sep. 2012, pp. 89–94.

[26] W. Wang and H. Farid, "Exposing digital forgeries in video by detecting duplication," in *Proc. 9th Workshop Multimedia Secur.*, 2007, pp. 35–42.

[27] E. Ted, "Video and image watermark synchronization," Ph.D. dissertation, Purdue Univ. West Lafayette, West Lafayette, IN, USA, 2005.

[28] D. Cross and B. G. Mobasseri, "Watermarking for self-authentication of compressed video," in *Proc. Int. Conf. Image Process.*, vol. 2. Sep. 2002, pp. II-913–II-916.

[29] W. Wang, X. Jiang, S. Wang, M. Wan, and T. Sun, "Identifying video forgery process using optical flow," in *Proc. Int. Workshop Digit. Watermarking*, 2013, pp. 244–257.

[30] R. Rigoni, P. G. Freitas, and M. C. Q. Farias, "Detecting tampering in audio-visual content using QIM watermarking," *Inf. Sci.*, vol. 328, pp. 127–143, Jan. 2016.

[31] Y. M. Alginahi, O. Tayan, and M. N. Kabir, "Verification of Qur'anic Quotations Embedded in Online Arabic and Islamic Websites," *Int. J. Islamic Appl. Comput. Sci. Technol.*, vol. 1, no. 2, pp. 41–47, 2013.

[32] I. Alsmadi and M. Zarour, "Online integrity and authentication checking for Quran electronic versions," *Appl. Comput. Informat.*, vol. 13, no. 1, pp. 38–46, Jan. 2015.

[33] T. Sabbah and A. Selamat, "A framework for Quranic verses authenticity detection in online forum," in *Proc. Taibah Univ. Int. Conf. Adv. Inf. Technol. Holy Quran Sci.*, Dec. 2013, pp. 6–11.

[34] A. Alshareef and A. El Saddik, "A Quranic quote verification algorithm for verses authentication," in *Proc. Int. Conf. Innov. Inf. Technol. (IIT)*, Mar. 2012, pp. 339–343.

[35] S. Nisha, N. Ali, and A. B. M. S. Ali, "Searching quranic verses: A keyword based query solution using .net platform," in *Proc. 5th Int. Conf. Inf. Commun. Technol. Muslim World (ICT4M)*, Nov. 2014, pp. 1–5.

[36] A. Haouzia and R. Noumeir, "Methods for image authentication: A survey," *Multimedia Tools Appl.*, vol. 39, no. 1, pp. 1–46, Aug. 2008.

[37] F. Daraee and S. Mozaffari, "Watermarking in binary document images using fractal codes," *Pattern Recognit. Lett.*, vol. 35, pp. 120–129, Jan. 2014.

[38] H. Tao, L. Chongmin, J. M. Zain, and A. N. Abdalla, "Robust image watermarking theories and techniques: A review," *J. Appl. Res. Technol.*, vol. 12, no. 1, pp. 122–138, 2014.

[39] M. Arnold, M. Schmucker, and S. D. Wolthusen, *Techniques and Applications of Digital Watermarking and Content Protection*. Norwood, MA, USA: Artech House, 2002.

[40] N. M. Makbol, B. E. Khoo, and T. H. Rassem, "Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics," *IET Image Process.*, vol. 10, no. 1, pp. 34–52, 2016.

[41] J. Nin and S. Ricciardi, "Digital watermarking techniques and security issues in the information and communication society," in *Proc. 27th Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, Mar. 2013, pp. 1553–1558.

[42] P. Singh and R. S. Chadha, "A survey of digital watermarking techniques, applications and attacks," *Int. J. Eng. Innov. Technol.*, vol. 2, no. 9, pp. 165–175, 2013.

[43] J. T. Brassil, S. Low, and N. F. Maxemchuk, "Copyright protection for the electronic distribution of text documents," *Proc. IEEE*, vol. 87, no. 7, pp. 1181–1196, Jul. 1999.

[44] T. Zong, Y. Xiang, S. Guo, and Y. Rong, "Rank-based image watermarking method with high embedding capacity and robustness," *IEEE Access*, vol. 4, pp. 1689–1699, 2016.

[45] P.-H. Hsu and C.-C. Chen, "A robust digital watermarking algorithm for copyright protection of aerial photogrammetric images," *Photogramm. Rec.*, vol. 31, no. 153, pp. 51–70, 2016.

[46] F. Y. Shih, *Digital Watermarking and Steganography: Fundamentals and Techniques*. Boca Raton, FL, USA: CRC Press, 2007.

[47] V. K. Mitali and A. Sharma, "A survey on various cryptography techniques," *Int. J. Emerg. Trends Technol. Comput. Sci.*, vol. 3, no. 4, pp. 307–312, 2014.

[48] A. Kumar and A. Kumar, "A cell-array-based multibiometric cryptosystem," *IEEE Access*, vol. 4, pp. 15–25, 2016.

[49] W. Stallings, *Cryptography and Network Security: Principles and Practices*. Upper Saddle River, NJ, USA: Pearson Education, 2006.

[50] D. R. Stinson, *Cryptography: Theory and Practice*. Boca Raton, FL, USA: CRC Press, 2005.

[51] O. Goldreich, *Foundations of Cryptography*, vol. 2. Cambridge, U.K.: Cambridge Univ. Press, 2009.

[52] C. P. Sumathi, T. Santanam, and G. Umamaheswari. (Jan. 2014). "A study of various steganographic techniques used for information hiding." [Online]. Available: https://arxiv.org/abs/1401.5561

[53] S. Katzenbeisser and F. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*. Norwood, MA, USA: Artech House, 2000.

[54] K. Bennett, "Linguistic steganography: Survey, analysis, and robustness concerns for hiding information in text," CERIAS Tech. Rep. Center Edu. Res. Inf. Assurance Secur., Purdue Univ., West Lafayette, Lafayette, IN, USA, pp. 1–30, 2004.

[55] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*. San Mateo, CA, USA: Morgan Kaufmann, 2007.

[56] T. D. Denemark, M. Boroumand, and J. Fridrich, "Steganalysis features for content-adaptive JPEG steganography," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1736–1746, Aug. 2016.

[57] L. Por, B. Delina, Q. Li, S. Chen, and A. Xu, "Information hiding: A new approach in text steganography," in *Proc. Math. Comput. Sci. Eng. Int. Conf. (WSEAS)*, 2008, pp. 689–695.

[58] (2015). *Digital-Signature*. [Online]. Available: http://searchsecurity.techtarget.com/definition/digital-signature

[59] R. Bausys and A. Kriukovas, "Digital signature approach for image authentication," *Elektron. Elektrotech.*, vol. 86, no. 6, pp. 65–68, 2015.

[60] C.-S. Lu, "Multimedia security: Steganography and digital watermarking techniques for protection of intellectual property," in *Institute of Information Science Academia Sinica*. Taiwan, China: IGI Global Publishers, Jul. 2004, p. 268,

[61] J. Xuehua, "Digital watermarking and its application in image copyright protection," in *Proc. Int. Conf. Intell. Comput. Technol. Autom. (ICICTA)*, May 2010, pp. 114–117.

[62] J.-S. Coron, "What is cryptography?" *IEEE Security Privacy*, vol. 4, no. 1, pp. 70–73, Jan. 2006.

[63] H. Delfs and H. Knebl, "Symmetric-Key Cryptography," in *Introduction to Cryptography*. Berlin, Germany: Springer, 2015, pp. 11–31.

[64] E. Cole, "Hiding in plain sight," in *Steganography and the Art of Covert Communication*. Hoboken, NJ, USA: Wiley, 2003.

[65] C. J. Date and H. Darwen, *A Guide To SQL Standard*, vol. 3. Reading, MA, USA: Addison-Wesley, 1997.

[66] A. V. Aho and M. J. Corasick, "Efficient string matching: An aid to bibliographic search," *Commun. ACM*, vol. 18, no. 6, pp. 333–340, Jun. 1975.

[67] G. Navarro, "A guided tour to approximate string matching," *ACM Comput. Surv.*, vol. 33, no. 1, pp. 31–88, 2001.

[68] (2015). *SearchSQL*. [Online]. Available: http://searchsqlserver.techtarget.com/definition/hashing

[69] L. Welling and L. Thomson, *PHP and MySQL Web Development*. Indianapolis, IN, USA: Sams, 2003.

[70] L. K. Saini and V. Shrivastava. (Jul. 2014). "Analysis of attacks on hybrid DWT-DCT algorithm for digital image watermarking with MATLAB." [Online]. Available: https://arxiv.org/abs/1407.4738

[71] (2015). *MATLAB*. [Online]. Availablke: http://www.mathworks.in/help/images/ref/imcontrast.html

[72] C.-C. Lai and C.-C. Tsai, "Digital image watermarking using discrete wavelet transform and singular value decomposition," *IEEE Trans. Instrum. Meas.*, vol. 59, no. 11, pp. 3060–3063, Nov. 2010.

[73] S. Rastegar, F. Namazi, K. Yaghmaie, and A. Aliabadian, "Hybrid watermarking algorithm based on singular value decomposition and radon transform," *AEU-Int. J. Electron. Commun.*, vol. 65, no. 7, pp. 658–663, Jul. 2011.

[74] Z. Jalil and A. M. Mirza, "A review of digital watermarking techniques for text documents," in *Proc. Int. Conf. Inf. Multimedia Technol. (ICIMT)*, Dec. 2009, pp. 230–234.

[75] Z. Jalil, H. Aziz, S. B. Shahid, M. Arif, and A. M. Mirza, "A zero text watermarking algorithm based on non-vowel ASCII characters," in *Proc. Int. Conf. Edu. Inf. Technol. (ICEIT)*, Sep. 2010, pp. V2-503–V2-507.

[76] W. Halfond, J. Viegas, and A. Orso, "A classification of SQL-injection attacks and countermeasures," in *Proc. IEEE Int. Symp. Secure Softw. Eng.*, 2006, pp. 13–15.

[77] (2015). *Comscore*. [Online]. Available: http://www.smartinsights.com/mobilemarketing/mobile-marketing-analytics/mobile-marketing-statistics/

SAQIB HAKAK was born in Srinagar in 1986. He received the B.E. degree in computer science from the University of Kashmir, India, in 2010, and the M.Sc. degree in computer and information engineering from IIUM, Malaysia, in 2014. He was with the Telecom Sector and the Software Sector. He is currently a Research Scholar with the Computer Science and IT Department, University of Malaya. He has authored numerous several conference papers and journals under his name. His research interest includes: information security, affective computing, cloud computing, and wireless networks.

AMIRRUDIN KAMSIN received the BIT (Management) degree from the University of Malaya in 2001, the M.Sc. degree in computer animation Bournemouth University, U.K., in 2002, the Ph.D. degree from the University College of London in 2014. He is currently a Senior Lecturer with the Faculty of Computer Science and Information Technology, University of Malaya, Malaysia. His research areas include human–computer interaction, authentication systems, e-learning, mobile applications, serious game, augmented reality, and mobile health services.

OMAR TAYAN received the B.Eng. degree and the Ph.D. degree in computer networks from the University of Strathclyde, Glasgow, U.K. He is currently an Associate Professor with the College of Computer Science and Engineering and the NOOR Research Center, Taibah University, Saudi Arabia. He was a consultant to the Strategic and Advanced Research and Technology Innovation Unit, Taibah University, and is one of the founding members of the NOOR Research Center, Taibah University. He currently has about 50 journals, conference papers, technical reports, and invited talks to his credit, as well as a book publication in computer networks. He has successfully completed about 10 research and development projects as a Principle Investigator and a Co-Investigator in projects funded by King AbdulAziz City for Science and Technology, the Ministry of Higher Education, and the Deanship of Research, Taibah University. His research interests include information security, e-Learning and multimedia technologies, quranic computing, image processing, modeling and simulation, computer networks and Networks-on-Chip, and wireless sensor networks for intelligent transportation systems including Hajj transportation systems and crowd management.

MOHD. YAMANI IDNA IDRIS is currently a Senior Lecturer with the Faculty of Computer Science and Information Technology, University of Malaya. His research interest is in the area of information security, image and signal processing, and Internet of Things.

ABDULLAH GANI received the bachelor's and master's degrees from the University of Hull, U.K., and the Ph.D. degree from the University of Sheffield, U.K. He is currently a Professor with the Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, Malaysia. He has vast teaching experience due to having worked in various educational institutions locally and abroad—schools, teaching college, ministry of education, and universities.

SABER ZERDOUMI received the M. Tech. degree in France. He is currently pursuing the Ph.D. degree with the Faculty of Computer Science and IT, University of Malaya.