Graduation Certificate Verification Model: A Preliminary Study

Omar S. Saleh[1], Osman Ghazali[2], Qusay Al maatouk[3]
School of Computing, University Utara Malaysia (UUM), Kedah, Malaysia[1, 2]
Asia Pacific University of Technology and Innovation (A.P.U), Bukit Jalil, Kuala Lumpur[3]

***Abstract*—Graduation certificates issued by universities and other educational institutions are one of the most important documents for a graduate. It is a proof of graduate's qualifications and can be used to advance forward in one's career and life. However, due to advances in software, printing and photocopying technologies, forgery of those certificates is made easy and as good as the original, making them difficult to detect. Several universities and educational institutions as well as businesses started to dedicate resources for verifying certificates however that is usually a tedious and quite costly process and there isn't a clear model that can be adopted by those institutions that could minimize cost and speed up the process. There are many techniques proposed for paper based document verification and this paper analyzes and expatiate the issues on those techniques. Most of the verification techniques require change in the process of certificate generation either by changing template, changing paper, changing printers, adding hardware or even adding extra information. This change may mean that the university or verifier needs the proper knowledge to execute and run the proposed technique. This also means that older certificates may not work with the newly introduced techniques. To also add some proposed techniques require a change that is not always easy or cheap like in creating a third body to verify certificates.**

***Keywords*—Graduation certificate verification; graduation certificate authentication; graduation certificate forgery**

I. Introduction

Document verification is a vast field such that there is bank type of documents, governmental type of documents, transactions type of document, educational certificates type of document and many more other kinds. Each of the domain and types can be treated differently and the content vary tremendously. For example transactions can contain number in tabular form while educational certification may contain only textual information presented in paragraphs. Due to the vast differences in types of documents and how they are presented the research will focus on digital verification of paper-based graduation certificates. Verification is the process of determining or confirming that someone (or something) is original. Documents Verification on the other hands can be define in various ways such as the researchers [1] defines document verification as the process of proving the correctness or authenticity of a document by using a proven method or technique. While the researchers [2] defines it as the process of ensuring that documents received from holder are genuine and that the holder is the rightful owner. The problem is that the verification of certificates is costly and time consuming using the traditional methods in which the person to verify calls the issuing institute to make sure that said certificate is correct and that the information is real [2],[3],[4],[5]. For example, when a certificate holder applies for a position or a seat at some university the certificate holder either sends a copy by post or email or even faxes a copy to the place of interest. The place of interest accordingly verifies that the holder's certificate is real and not forged and that the information is real. And it is the dominant method. The traditional approach is time consuming and costly for both the place of interest as well as the issuer since resources would be allocated by both parties just to do one verification. It can grow exponentially costly if the process is repetitive. If the place of interest opted-for does not verify submitted certificates it can suffer great damages. Such that it will be more costly to recruit individuals especially in the long run because the company will have to suffer from the unqualified personnel and hence bad performance for the company which also means loss of money and reputation; this in turn will also mean higher employee turnover. Ultimately this will lead to loss of market value. That lead the researchers to investigate the techniques which can be used for document verification. The next sub-sections will dive in details of document verification such as its aim, its workflow and types of documents.

II. Document Verification

The main aim of document verification is the ability to trace the origins of a document to a specific person, the device that produced it or the place where it was produced [6]. Forgeries pose a huge threat to the integrity of documents, with significant dangers in terms of authentication and trust. It is therefore important to protect the integrity of a document in order to prevent problems arising from the modification of a document by intruders [6]. According to the research conducted by [4], all documents or credentials that are printed are potentially subject to counterfeiting and forgery. Forgery can cause a lot of damage when it comes to trust and authenticity [7].

There is a high market for forgery as well as opportunity with low cost, high quality results available [1]. Researchers have also found several significant problem areas when it comes to document verification. For instance, the technologies that are put forth to stop or prevent forgery do not seem to be moving as fast as the evolution of the forging techniques [8]. With respect to academic documents, further authentication problems include the variations from one school to the next, which causes consistency issues that can be taken advantage of, especially in international situations [9].

There are two basic document categories that are considered in document verification literature; digital based documents and the traditional paper or printed document. The research in this case deals with certificates. Almost all documents can be handled in a digital manner, except for the certificate. The reason for this exception is that all digital documents are easy to forge without leaving any clues [10]. Furthermore, the prevalence of forged certificates results from the increased global demand for higher education, which exceeds the university capacity of the world [9].

According to the research conducted by [10] there are two main types of forgery, type 1 and type 2. Type 1 forgery is when some part of the original document is changed in order to benefit someone who was not benefitted by the original document. In this case, the base substance, normally the paper or plastic card, remains legal and valid, but the information that is contained therein is forged. The second, type 2 forgery is when both the base substance and the information contained therein is fake. However, it is often very difficult to tell whether it is real or fake because the base substance and the style of the document normally look authentic [10]. The researchers of the research [10] outlined the characteristics of the classic unforgeable document. They also outlined three principles of the unforgeable document as follows;

1) The forged document normally has some difference from an authentic original document in some way

2) The detection of the forgery can happen without reference to the authentic original document

3) There is a concrete verification method that does not necessarily involve communication with an authentication bureau

III. Document Verification Workflow

There are three entities must be present to accomplish the process of document verification which are the issuer, the owner and the verifier. The issuer represents the entity that issues the document such as an educational institution or business organization or even a charity organization. The owner represents the person who owns the document. The verifier represents the employer/third parity that verifies the document. Based on that, the document verification workflow can be diagrammatically represented in Fig. 1

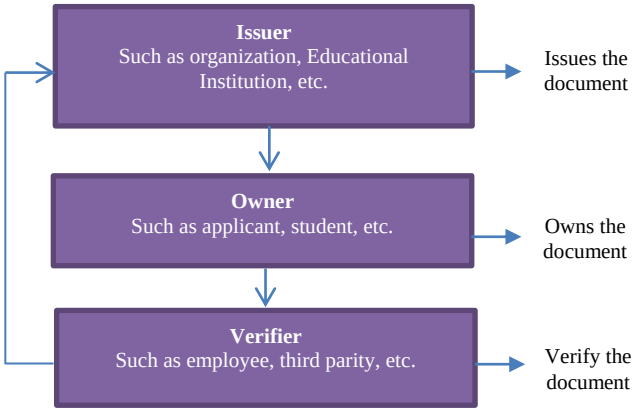

Fig. 1. Document Verification Workflow.

IV. Types of Documents

Documents can be categorized to two categories which are paper based documents and digital based document [10]. Paper based document contains characters, digits, tables, etc. Its digital version or digital document is a computer file. Digital document is designed to produce visual information on the computer monitor [10]. Forgery of documents has increased jeopardizing the integrity of both the document holder and the organization that issued the document [4-5]. The forgery of document is classified into two types which are 1) altering part of an authentic document that is original and 2) producing a new fake certificate with false information [10]. Forgery of document has become easier than the past mainly because of the technological advancements. For example scanning and printing hardware are much more advanced than they use to and are not as expensive add to that the editing software that are widely spread and constantly being updated and enhanced. Unfortunately as document forgery has become easier the increase of fake document has also increased. The latter is due to the lack in advancements in securing as well as verifying the paper-based documents [2],[6]. In other words documents securing and verification are not advancing as fast as the tools that enable forgery are. For that, the document verification became an important task; it is the process of ensuring that documents presented by prospective employees are genuine and that the holder is the rightful owner.

V. Paper based Document

This section will describe and detail on the first type of documents mentioned earlier and is the paper based documents. Its importance is described and also how they are verified.

A. Importance of Paper based Document Verification

The paper based documents are still widely used. There are many types of paper based document such as graduation certificates, birth certificates, etc. The information inside the paper based documents are subject to threats like forgery; despite measures taken to protect them attacks still happen. Author in [8] attributes that to the lack of verification. There are many cases where documents where forged throughout the globe. For example one that happened in New Delhi, where five people obtained loans and cheated the banks using fake documents [6]. Another example is one that happened in Bagdad, an investigation of 20,000 government employees by Iraqi's parliament showed that some employees have used forged educational certificates and fake diplomas to get their jobs. The issue extended in that those employees that used fake certificates became senior officials in the government [6]. Forgery of documents can happen in any discipline or line of work. In U.S. for example, The National Health Care Anti-Fraud Association projected that United States of America lost 3% to 10% of total healthcare cost to fraud [12]. Another example of forgery that happened in an area that involved the medical discipline is in Malaysia. The mainstream newspaper reported that a statement given by the Congress of Unions of Employees in the Public and Civil Services (CUEPACS) stated that more than 45,000 or 3% of 1.5 million government's staff in Malaysia forged medical certificate as a reason of absence from work to do part-time jobs. Another discipline that was impacted is Education. For example the prominent University

of Newcastle let out 50 students because they used forged certificates. The lecturers later on the course figured out that those students were unable to keep up with their studies and made them suspicious. That lead to a verification process, the university discovered that the English language certificate and degree certificate were forged.

With that has been mentioned document verification is important to overcome many issues that could even do with life and death. Imagine a doctor forging his way into a medical school. Or a politician forging his way to power. As a result, many could be harmed of such a behavior. Document verification of a paper based document has to be efficient to allow of seamless verification.

VI. The Graduation Certificate

A university is an example of an organization that creates so many documents for their students. It issues a certificate and academic transcript for each of its graduates. The certificate contains information that certifies a person has graduated from a certain specialization and obtained results as stipulated in the certificate. The certificate can then be used for job hunting or pursuing academics or any other purpose. The graduation certificate issued by the universities/institutions is one of the important documents for the graduate. It is a proof of graduate's qualification and can be used anywhere. Every year millions of students graduate from colleges and Universities, and their numbers are growing. Institutions issue certificates to those who have successfully completed the requirements of graduation. A graduation certificate is still in the form of a paper-based document because, as of yet, an electronic document cannot effectively replace a physical certificate [13]. With the rise of graduates and advancements in printing and photocopying technologies, came the rise of fake certificates as well threatening the integrity of both the certificate holder and the university that has issued the certificate [4-18]. This means that document validation and verification has become an important task The graduation certificate has to be verified to ensure that its content is true and also to ensure that the issued certificate comes from a real source [2]. Fake certificates can be created easily and the quality of a fake certificate can now be as good as the original. The certificates of many prominent universities have been forged and these forgeries are very difficult to detect. Educational establishments try to combat fraud and forgery in several ways [7]; however, most of the methods are time consuming because they are manual and involve human interaction. A lot of the time is spent in either reaching out to the university to verify a certificate or in awaiting a reply from the university that the certificate is valid and true. This process can be extremely laborious and expensive especially if a company needs to check the certificates of several hundreds of applicants. This adds to need of having a cost effective fast solution to verify certificates.

A. Importance of Graduate Certificate

Graduate certificates are of great importance to land a job or pursue further education they are the proof that the holder possesses the necessary knowledge to take a given position or pursue education. If these certificates are forged the whole foundation could collapse such that the employee would hold a position is not entitled to and could ruin or bring down the company. If it is in an educational institution it could mean many things of which a seat could be occupied by unworthy person instead of a worthy person. The graduate certificate as mentioned earlier can either be paper based or digital.

B. Paper-Based Certificate

Paper based certificates are still widely spread mostly because it is considered more secure than the digital certificate [6],[8]. Paper based certificate have stamps and signatures on them which can reflect originality [14]. Many entities require a stamp and a signature to accept a given document and graduation certificates are no different. However, the issue that arises is that the holder would be bound to providing the original copy every time the stamp and signatures are required. Another importance for paper based certificate is that they are easy to note from and on; Say the manuscript; modules can easily be highlighted and marked. Allowing multiple reviewers to go through it and do the same.

Paper based certificates despite being widely used they can be damaging. The most important disadvantages are:

- With paper based certificates is risk of loss and damage. Paper based certificates can easily be lost especially now as it is easy to relocate between different places and countries.
- Paper-based certificates is that they can be costly especially if changes are required on the document; for example a faulty name was printed, more papers would have to be used and that extra cost for the entity issuing the certificate; this indirectly also effects the environment.
- Paper based certificates can easily be damaged be it a wet hand or a fire in the building; Once the paper documents are damaged they are usually hard to recover. The holder either has to travel to source to generate the same or if the same is not regenerated it is a loss [15].
- Paper based certificates can eventually consume physical space.
- Paper based certificates can be slow to retrieve.

Despite these drawbacks with Paper based certificates entities still use it.

C. Digital based Certificate

The graduate digital certificate is the certificate that is issued in a digital form. It usually issued through a secure certification and verification method [16]. It is mostly adopted in order to solve the management problems of paper based certificate [15]. However one of the important reasons why digital certificates are widely adopted is that digital certificates provide a unique feature which is portability [17]; it is easy to transfer documents when they are digital.

Digital based certificates are considered environment friendly and can easily be organized without taking much space. The digital certificates in the simplest form is the easiest to forge without the need for special hardware [17]. Editing softwares are widely spread and changes to manuscripts and graduation certificates can easily be made. Digital certificates

are easily generated and can be amended with ease. Despite the advantages the digital based certificates they are not widely spread as the paper based certificates and are not the preferred method for many universities. Even if digital based certificates are issued paper based certificates are still required and needed.

VII. Related Work

There are several incidents where fake documents were discovered. As a result, many techniques arose like holograms, stamps and wet-signatures [2],[7]. However, these techniques can easily be replicated to create forged documents. Fortunately, there are continuous researches aiming to provide newer and better means to authenticate, validate, and verify the paper based documents. This made for several techniques to verify the paper based documents.

Signature extraction is a technique applied to verify bank cheques [18]. Signatures are of great importance in any paper based document. The availability of signature reflects the authenticity of document and level of authority that handled the document. For that in the conducted research [18], they focused on the signature verification only and they only targeted bank cheques. Their proposed system utilizes their signature database for verification. Given this research is focusing on graduate certificates this solution may not be the best solution to adopt for graduation certifications simply because 1) using the signature on its own would not ensure that the certificate is not forged and that the information is correct; the signature merely reflects that the document has been authorized by a specific person. This does not ensure in any way that the content is valid and is correct. Another issue with this approach is that 2) it still can be forged. Anyone can just copy the original signature and with the right tools a new certificate is created. Documents can be forged and the same signature used; the system will simply identify the signature and ensure that it exists in the database of signatures. The third issue with the proposed approach is that the technique was proposed with bank cheques in mind. Bank cheques have specific formats and templates than graduation certifications.

Print signature is another technique which is proposed to verify tickets [19]. Print signature has two procedures which are the 1) registration and 2) authentication. The registration procedure is given to the document to be protected; and the authentication procedure is to verify the authenticity and originality of the printed document. The verification process is made based on Optical character recognition (OCR) techniques. The OCR technique is made by fetching the features of document to be verified and then matched with saved features in database or somewhere else. The solution was made for tickets and tickets have different format and theme than graduation certification. The technique could be adopted to verify the graduation certification however the proposition as is would not work because 1) this may verify the content however it does not verify the source or where it was issued from. 2) saving the features to recognize later was made for tickets and not graduate certificates. 3) to save the features on a database may not be the safest approach. If the database is exposed the verification process will fail. The best approach is that if an algorithm verifies on the fly without the need to store the sensitive details needed to verify on the database.

The use of hash value for verification was proposed by the researchers [20]. The proposed method in the conducted research contains two stages which are document enrolment stage and authentication stage. They proposed to compute a hash value in the document enrolment stage and then store it in hash value database. The document is authenticated through computing the hash value again in the authentication stage and compared to the hash value in the database. If it matched, the document is authentic and if it not, the document is not authentic. The generation of hash value depends on the content in the certificate which will help in protecting the document from any changes. However, this approach does not consider securing the stored hashed value from leakage or being attacked.

Barcode is one of the most well-known approaches which can be used for document verification. Barcode technology is one of the most important parts of AIDC. The barcode can be analyzed to obtain the hided data. In term of encoding type, the barcode can be classified into two categories, namely, are 1D barcode and 2D barcode. The 1D barcode usually consists of varying of parallel lines different in both widths and space. Barcode offers several benefits such as High data capacity; error correction ability; and no additional storages [21]. 2D barcode can be used to hold information in both sides horizontally and vertically. Its content can be recovered reliably by scanning and decoding of the barcode. The main use of 2D barcode is to hold significant amount of data, typically of the order of 500 bytes per square inch. One of the main advantages of 2D barcode is that it can be printed on paper by normal printers and scanned by normal scanners [22].

2D barcode to verify the hardcopy of mark sheets [2]. The 2D barcode contains the encrypted data of the document. For document verification, they proposed an application which scans the 2D barcode and the document image to process it. The application reads the document image line by line utilizing OCR technique to recognize the text in the image of the document taken. Their proposed process to decrypt the information from the 2D barcode. The proposed method has advantage over the techniques which was proposed by [9],[16], as they proposed to encrypt the information however; the drawbacks of the proposed method is somewhat similar to the drawbacks in using the QR codes and are: 1) modifications has to be in the printed certificate; 2) availability of public key; 3) older documents without the 2d barcode cannot be verified.

The researchers [7] suggested somewhat similar verification approach to the researchers [2]. They proposed to embed the hashed unique key generated from the timestamp, track number and the content of document into 2D barcode. For document verification, they proposed to scan the document using OCR techniques. The text of the document along with the timestamp and the tracking number will be extracted from the 2d barcode. However the extracted data is hashed using hashing algorithm. The generated hash value is matching with the hash value stored in 2D barcode. If the hash values are same, the document is original else the document is fake. The proposed method is adopted within same organization.

Similar to the verification approach which was proposed by [7], the researchers [6] also proposed to use 2D barcode.

however their intention was to verify documents sent from point A to point B with a known sender and receiver. The verification method is proposed based on a scenario where user A wants to send document to user B and user B wants to verify the sent document sent by A. Hence, they proposed that the important parts of the document such as time stamp, issuing number, sender signature and hashing value of the content of the document be embedded in the 2D barcode. For document verification, the receiver decrypts the content through scanning the 2D barcode. This approach added extra details to the embedded data in the bar code however these details may not be needed in graduation certificate and it is suffer similar drawbacks to [2] mentioned earlier.

The QR code is one of 2D barcode types; it was first designed in Japan, and then later became more popular. QR code offers several benefits such as fast reading; high storage capacity, etc. It is was developed by Denso Corporation in 1994. QR code nowadays are adopted for different uses as well as different applications. It has been used in transport ticketing, commercial tracking, identity verification and website Uniform Resource Locator (URL) [14-18]. QR code comes in various sizes and versions. The smallest size is of 21x21 modules; it was the first version. The latest version is 40 which come in size of 177x177 (inch). QR codes have four levels of error correction which are, namely, L, M, Q, H; these levels are different in the rate of error correction like 7% is in the level L; 15% in M; 25% in Q and 30% in H [6-20]. However; the QR code capacity is based on its version and its level of error correction. QR code can hold up to 7089 characters of numerical data; 4296 characters of alphanumeric. QR code has several benefits like high capability of error correction; can be scanned from any direction; support different encoding types and versions, etc.

QR codes as a mean of paper based document authentication [23]. Their proposed method can only be applied between known sender and receiver. for each party there are set of procedures. They proposed to generate hash value from the message then the hash value is encrypted with the private key of the sender. This forms the digital signature. The message and the digital signature are then combined and compressed and embedded in the QR code. The QR code is printed on the paper and then sent to the receiver.

The QR code in the document is scanned first, the data of QR code is decrypted in order to obtain the embedded message and digital signature. The digital signature is decrypted using the sender's public key. Their proposed technique of document verification is similar to the proposed approach by [24],[25].

In the research conducted by [9] and [14], they proposed to keep the information in a database instead of a QR code. A QR code scanner must be used to scan the QR code.

QR code is another technique which proposed to be utilized for document verification. For example, in the research conducted by [3],[26] the researcher proposed to use of QR codes on degree certifications, they proposed a scheme to generate the QR code. The scheme is a set of procedures. The first being composing the student details; followed by generation of a hash value from the composed details; after that the digital signature is composed using the university's private key; the content along with digital signature are combined and embedded into the QR code and QR code is printed on the bottom of the certificate.

For degree certificate authentication, they proposed a scheme similar to the approach which proposed by [23] and is scanning the QR code from the certificate; decrypting the details off the QR code; generating new hash value from the content of certificate that at hand and then matching process is done to compare the hash value. If the hash values are same, it means the certificate is authentic. if not, it means the content is altered and the certificate is fake. It is clear from the creation and verification process of the proposed method is that it is similar to the method proposed by the researchers of [23] and [27]. However, their solution unfortunately is under a license, which means for any entity to adopt the said solution the license must be purchased.

In the research conducted by [28], they suggested leveling up document verification by adopting a two level QR code. The two level QR code means that the QR code has two levels of storage; the information is stored in the first level and the second level is created by replacing the black modules with specific textured patterns. The texture patterns are related to print and scan process and they are sensitive. For document verification, the 2LQR is scanned. This proposition is mostly useful to verify the documents within same organization. Also document content were not considered.

Watermarked QR code is also an approach which is proposed for document verification [1]. Watermarked QR code contains the QR barcode, validation link to a website where it will show result and logo image. The logo image is for identifying the owner who generated the QR code. In the research conducted by [1], they proposed a process to embed the validation link into the QR code and then generate the QR code. The watermark logo is embedded into QR code image. For document verification, they proposed scanning the watermarked QR code using QR reader. The proposed process is very simple; however they only focused on validating the institution that issued the document and not the content or whether the content is correct.

RFID is another technique used for document verification. RFID stands for Radio Frequency Identification; it uses the radio frequency waves to transfer data. The data is transferred between two entities which are the reader and moveable item. The moveable item is tagged to categorize, identify and track it [25],[29]. In the research conducted by [30], they developed smart degree system based on RFID.Their system utilized the fingerprint of graduates for the purpose of certificate verification. They proposed that the university issues the certificates with RFID tags; this tag contains the important information related to the graduate like name, graduation date, the program, the degree and biometrics (fingerprint) of the graduate. For certificate verification, an interrogator must be used to read the embedded data in the tag and also the verifier have to log into a website which is usually indicated in the back of the certificate, and download the required software to enable interpreting the tag. The issue with the proposed solution is that the process of authentication is time consuming, especially that the external entities that might verify the

certificate will have to download a software in order to read the encrypted data along with the need to have an RFID reader to read the tag and download its data. Another major problem associated with approach is that the certificates mailed or copies cannot be verified since they will lack the RFID in them. The original certificate has to be present and this is not a feasible solution making RFIDs useless for graduate certificates.

The other dominant approach utilized in document verification is digital watermarking [31],[32]. It is a technique that can be utilized for protecting the copyrights or ownership; it also can be used to prevent forgery in printed documents. It is a method that can be used to embed some information in the cover image. This information can later be extracted and processed. The way watermarking works in the simplest form is through embedding the main information of document as a watermark in the same document. For document verification, the hidden information can be extracted using certain algorithms [33]. Usually it is very hard to notice the embedded watermark by the human naked eyes, hence if tools like OCR is used to read the contents the watermark would be lost [8]. The drawbacks of using watermarking is that it can easily be lost when transforming paper-baser to digital and vice-versa. Also to add it requires change in the type of paper used for certificates as well as the process of generating the certificate. As for digital watermarking generally graduate certificate are not all digital and still are being paper-based and so is most of real-life documents [34].

Based on what has been presented in the previous sections, there are many techniques proposed for paper based document verification. Most of these techniques require change in the process of certificate generation either by changing template, changing paper, changing printers, adding hardware or even adding extra information. This change may mean that the university or verifier need the proper knowledge to execute and run the proposed technique. This also mean that older certificates may not work with the new introduced techniques. To also add some proposed techniques require a change that is not always easy or cheap like in creating a third body to verify certificates.

As reflected some techniques are mostly suitable for specific domain and document like signature extraction for bank cheques. Others were proposed based on specific environments and conditions like environments that assumes both send and receive are known to each other [2],[35].

VIII. Discussion

With today's availability of low-cost scanning devices, high-quality printers and better color copy machines, the production and circulation of fake certificates became cheap and easy because a paper document can easily be forged [3],[11]; however, the forgery of important document like graduation certificate became a real issue. The 21th century has experience a lot of fraudulent activities and misconduct most especially in the practices of certificate forgery. The resultant effect of these habits in most cases normally reduces the integrity of institution concern [28]. Hence, anti-counterfeit method has becoming a worldwide research focus.

It is clearly shown in the previous sections that there are some proposed techniques that were made with graduation certificates in mind and there are other techniques made for other purposes that could be adopted to verify the graduate certificates such as QR code, 2D barcode, watermarked QR code and RFIDs. An RFID tag solution is very complex, costly process and the lifetimes of such devices are very limited [16]. A very popular approach, often used in practice, is watermark. It usually provide a good protection against forgery, but they are costly and often not included in real-life documents [34]. compared to computer chips and RFID tags, data hiding technologies like Quick Response (QR) code are much cheaper and do not require specialized hardware for retrieving data. QR codes are inexpensive, and they are passive read-only elements whose content cannot be altered. Decoding of the QR code can be done by many low-cost devices, including smart phones. As QR Code has high capacity, all the standardized features extracted from the fingerprints could be encoded in it. It can be read from any direction and standard encryption techniques can be applied to the QR code to make it even more secure [36]. With each of these techniques there are limitations as reflected earlier. Despite the scare resources in literature, the available literature that focuses on graduate certificate verification is very limited and also there is no clear model to graduate certificates verification that could be adopted by universities. Universities do not have a model to work with they simply execute different techniques which are not necessarily suitable and cost effective. The verification process can consume a lot of resources (time and money) for both entities the issuer and verifier. For example, the verifier would call the university and the university would interns consult its records and reply to the verifier. This process is tedious and resources hungry. That is why there ought to be a model that balances the cost effectiveness and efficiency. The verification process of paper based documents varies in three dimensions the first being the tools used. The second the scope and the third being the procedure of verification.

1) Procedure: The researchers of [4],[29] suggest scanning the document then verify.

2) Tools: In the research conducted by [20], they suggest OCR techniques for automatic verification. While in the research conducted by [6], [7], they suggest utilizes Smart phones with cameras. And there are other approaches that involves adoption of extra hardware such as RFIDs, such an approach requires an interrogator to read the embedded data in the tag and also the verifier has to log into a website which is indicated in the back of the certificate, and download the required softwares add to that the original certificate with the RFID has to be present. From the previously stated, it can be concluded that the verification process of paper based document requires either extra software, changes to the current certificates and also can require extra hardware. Paper based document verification still need to be further enhanced to increase of the verification speed and make it effective and reliable.

3) Scope: The other characteristic if verification is the scope. The verification process is proposed between sender and receiver [6],[7]. While the proposed process of document

verification is only carried out within their own organization [21],[37]. The verification process is only useful if the verifier is known for the issuer. However; the drawback with this process is that the third parity would have to manually communicate with the organization issuing to verify the document and this consumes a lot of time and hence becomes costly (cost of calling, assigning personal to call and of course allocating necessary resources to respond to the said request).

IX. Conclusion

With the rise of human population came the rise of educational institution to accommodate the population. However, this has introduced some problems to many organizations and to the educational institutions themselves. One of the most important problems is Verification. There are ways institutes try to combat frauds and forgeries however mostly are time consuming because they are manual and it involves human interaction. The time spent is either reaching out to the university to verify a given certificate or awaiting a reply from the university that issue the certificate. This latter can be extremely exhausting and expensive especially if a company does it for several hundreds of applicants. As presented in this study there isn't a clear model for verification. Even though there are researches taking place to enhance verification of documents; the graduation documents verification researches are very scarce. Little research is dedicated to graduation documents verification. Aside from that the techniques presented each has its flaws for seamless unified certification verification. In future work, authors will design and develop a clear model for graduation certificates verification.

Acknowledgment

Authors would like to sincerely thank Universiti Utara Malaysia (UUM), Asia Pacific University of Technology and Innovation (APU) and Ministry of Higher Education, Iraq for supporting this research.

References

[1] T. Mantoro, M. I. Wahyudi, M. A. Ayu, and W. Usino, "Real-time Printed Document Authentication Using Watermarked QR Code," pp. 68–72, 2015.

[2] S. Balsubramanian, R. Prashanth Iye, and S. Ravishankar, "Mark sheet verification," 2009 3rd Int. Conf. Anti-counterfeiting, Secur. Identif. Commun. ASID 2009, 2009.

[3] A. Singhal, "Degree Certificate Authentication using QR Code and Smartphone," vol. 120, no. 16, pp. 38–43, 2015.

[4] C. M. Li, P. Hu, and W. C. Lau, "AuthPaper: Protecting paper-based documents and credentials using Authenticated 2D barcodes," IEEE Int. Conf. Commun., vol. 2015-Septe, pp. 7400–7406, 2015.

[5] M. Al-gawda, Z. Beiji, and N. Mohammed, "Printed Document Authentication Using Two-Dimensional (2D) Barcodes and Image Processing Techniques," vol. 9, no. 8, pp. 347–366, 2015.

[6] M. H. Eldefrawy, K. Alghathbar, and M. K. Khan, "Hardcopy document authentication based on public key encryption and 2D barcodes," Proc. - 2012 Int. Symp. Biometrics Secur. Technol. ISBAST 2012, pp. 77–81, 2012.

[7] M. Salleh and T. C. Yew, "Application of 2D barcode in hardcopy document verification system," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 5576 LNCS, pp. 644–651, 2009.

[8] A. Husain, M. Bakhtiari, and A. Zainal, "Printed document integrity verification using barcode," J. Teknol. (Sciences Eng., vol. 70, no. 1, pp. 99–106, 2014.

[9] P. Documents, "Verification of the Integrity and Legitimacy of Academic Credential Documents in an International Setting," Coll. Univ., vol. 84, no. 4, 2009.

[10] K. Nozaki, H. Noda, E. Kawaguchi, and R. Eason, "A Model of Unforgeable Digital Certificate Document System."

[11] Z. Chen, "Anti-Counterfeit Authentication System of Printed Information Based on A Logic Signing Technique."

[12] D. W. Simborg, "Healthcare Fraud: Whose Problem is it Anyway?," J. Am. Med. Informatics Assoc., vol. 15, no. 3, pp. 278–280, 2008.

[13] M. Warasart and P. Kuacharoen, "Paper-based Document Authentication using Digital Signature and QR Code," no. Iccet, 2012.

[14] B. Micenková, J. van Beusekom, and F. Shafait, "Stamp verification for automated document authentication," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 8915, pp. 117–129, 2015.

[15] L. Chen-Wilson and D. Argles, "Towards a framework of a secure e-qualification certificate system," ICCMS 2010 - 2010 Int. Conf. Comput. Model. Simul., vol. 1, pp. 493–500, 2010.

[16] L. Chen-Wilson et al., "Secure certification for ePortfolios," Proc. - 8th IEEE Int. Conf. Adv. Learn. Technol. ICALT 2008, pp. 744–745, 2008.

[17] R. Vartak and S. Deshmukh, "Survey of Digital Image Authentication Techniques," vol. 2, no. 7, pp. 176–179, 2014.

[18] V. K. Madasu, M. Hafizuddin, M. Yusof, and M. Hanmandlu, "Automatic Extraction of Signatures from Bank Cheques and other Documents," Techniques, pp. 10–12, 2003.

[19] B. Zhu, J. Wu, and M. S. Kankanhalli, "Print signatures for document authentication," Acm Ccs 03, pp. 145–154, 2003.

[20] S. Voloshynovskiy et al., "Information-Theoretic Analysis of Electronic and Printed Document Authentication," Electron. Imaging 2006, pp. 60721D-60721D–20, 2006.

[21] J. A. Lin and C. S. Fuh, "2D barcode image decoding," Math. Probl. Eng., vol. 2013, no. 3, 2013.

[22] J. K. Adjei et al., "Document Authentication System Preventing and Detecting Fraud of Paper Documents," ProQuest Diss. Theses, vol. 5, no. 2, pp. 58–63, 2014.

[23] M. Warasart and P. Kuacharoen, "Paper-based Document Authentication using Digital Signature and QR Code," 202.21.149.33, no. Iccet, 2012.

[24] A. K. Mikkilineni, G. N. Ali, P.-J. Chiang, G. T. C. Chiu, J. P. Allebach, and E. J. Delp, "Signature-embedding in printed documents for security and forensic applications," Proc., no. 0219893, pp. 455–466, 2004.

[25] A. K. Mikkilineni, P.-J. Chiang, G. N. Ali, G. T.-C. Chiu, J. P. Allebach, and E. J. Delp, "Printer Identification Based on Graylevel Co-occurence Features for Security and Forensic Applications," SPIE Int. Conf. Secur. Steganography, Watermarking Multimed. Contents, no. 0219893, pp. 430–440, 2005.

[26] H. A. Ahmed and J. W. Jang, "Higher educational certificate authentication system using QR code tag," Int. J. Appl. Eng. Res., vol. 12, no. 20, pp. 9728–9734, 2017.

[27] C. M. Borota, "Printing Techniques used to Secure Border Crossing Documents," vol. 2, no. 1, pp. 31–40, 2005.

[28] S. Ibrahim, M. Afrakhteh, and M. Salleh, "Adaptive watermarking for printed document authentication," Proceeding - 5th Int. Conf. Comput. Sci. Converg. Inf. Technol. ICCIT 2010, pp. 611–614, 2010.

[29] S. Voloshynovskiy et al., "Information-Theoretic Analysis of Electronic and Printed Document Authentication," Electron. Imaging 2006, vol. 6072, pp. 60721D-60721D–20, 2006.

[30] C. Mudraganam, "SmartDEGREE from TCS to combat Certificate Malpractices," 2009.

[31] U. Garain and B. Halder, "On automatic authenticity verification of printed security documents," Proc. - 6th Indian Conf. Comput. Vision, Graph. Image Process. ICVGIP 2008, pp. 706–713, 2008.

[32] S. Sheng and X. Wu, "A new digital anti-counterfeiting scheme based on chaotic cryptography," Int. Conf. ICT Converg., pp. 687–691, 2012.

[33] M. Afrakhteh, S. Ibrahim, and M. Salleh, "Printed document authentication using watermarking technique," Proc. - 2nd Int. Conf. Comput. Intell. Model. Simulation, CIMSim 2010, pp. 367–370, 2010.

[34] J. Gebhardt, M. Goldstein, F. Shafait, and A. Dengel, "Document authentication using printing technique features and unsupervised anomaly detection," Proc. Int. Conf. Doc. Anal. Recognition, ICDAR, pp. 479–483, 2013.

[35] G. Gupta, S. K. Saha, S. Chakraborty, and C. Mazumdar, "Document frauds: Identification and linking fake document to scanners and printers," Proc. - Int. Conf. Comput. Theory Appl. ICCTA 2007, pp. 497–501, 2007.

[36] S. Ambadiyil, K. S. Soorej, and V. P. Mahadevan Pillai, "Biometric based unique ID generation and one to one verification for security documents," Procedia Comput. Sci., vol. 46, no. Icict 2014, pp. 507–516, 2015.

[37] S. Liu, "Anti-counterfeit system based on mobile phone QR code and fingerprint," pp. 250–254, 2010.