[1] Baraa Al Samarai

Developing a Blockchain-Enhanced System for Certificate Generation and QR Code Integration

Journal of Electrical Systems

Abstract: **-** Previously, certificates had to be manually distributed which not only is time-consuming and prone to mistakes.
As a result, there has been a rise in the issuance of fake certificates which has become a problem for those in search of jobs. To treat this problem, several certificate verification systems have been put forward by researchers. However, it is evident that since centralized systems are more mainframe, then most of them contain vices that include hacking and manipulation.
Such a system proposed in this dissertation is based on the concept of a certificate generation and verification system that uses blockchain and Quick Response (QR) codes. The system uses iteration and incremental models in system modeling and employs data flow diagrams and cases to illustrate the system's workings. The proposed algorithm is developed in the PHP front end and Spring Boot (a Java framework) for the back end.
The developed system optimizes the process of certificate generation and its dissemination as well as the issue of students' identity concerning protection. The use of the blockchain reduces weaknesses that are anchored on centralized servers since they are easier to hack and manipulate. Further, the incorporation of QR codes facilitates confirmation of certificates which offers the clients an anonymous confirmation option to protect the identity of learners.
Therefore, we can assert that the evaluation of the system proves its efficiency regarding the stereotypes resulting from certificate counterfeiting. The fact that the system is shielded, and the identity of the students is kept safe, makes it quite beneficial to institutions and employers. With the employment of this certificate generation and verification system, it makes the certificate to be genuine besides promoting an effective and efficient verification procedure.

Keywords: Blockchain; certificates generation; certificates verification; Quick Response Code.

I. INTRODUCTION

The World Wide Web has drastically changed the process of information sharing and transfer, however, the issue of security becomes the key point, particularly in the case of making important and confidential operations. Conventional methods of certificate authentication by universities and other institutions largely involve paper-based systems that are inherently defective and inefficient. Traditional approaches to manual verification procedures are costly and take a lot of time, and they do not fully solve the problem of fraudulent activities and forgery. The problem also evident in the current job market is that of fake certificates and as a result, the employers struggle to ascertain the validity of the certificates presented to them.

To tackle these problems, there is a real demand for a highly secure Web-based certificate generation and validation system, which would require identification of the minimum interference from people. An automated system in this regard would mean that the creation and validation of certificates is done by the system with the least likelihood of human error. Blockchain which is based on the distributed electronic record with high security is being introduced as a solution for multiple spheres. The system offers direct messaging and records sharing with no requirement of a middleman. On the same note and building on blockchain technology, a certificate generation and verification system can provide parties with verifiable tools coupled with timestamps that cannot in any way be altered.

The objective of this research is to propose a certificate generation and verification system that integrates blockchain and Quick Response (QR) codes. The system will enable institutions, organizations, and individuals to get authentic verification of educational certificates in a secure, anonymous, and user-friendly way. By this system, it is evident that issues in certificate authentication can readily be handled hence increasing the reliability of education certificates.

GOALS

[1] GULF UNIVERSITY – Bahrain, University Charles III of Madrid - Spain

Email: har@gulfuniversity.edu.bh

1. Streamlining the certificate distribution process: It means that the platform should be effective in simplifying and automating the process of certification distribution in order not to occupy too much time for the administrators.

2. Providing professional-looking certificates: The platform should enable the administrators to develop and print professional-looking certificates for issues corporate and in the organization's brand.

3. Increasing credibility: These measures include a QR code that when scanned will confirm the authenticity of the certificates to prevent acts of fake certificates.

4. Improving sustainability: It should be noted that the platform should be environmentally friendly and help minimize the use of beneficial resources in the organizational environment due to the absence of physical certificates.

II. LITERATURE SURVEY

To conduct an efficient verification of certificates, the following are some of the attempts researchers have made in handling the problem of certificate forgery. However, several approaches are still mainly based on manpower, or they pose some serious issues about scalability, security, and reliability.

Musee in his work Musee (2015), created a generic, cloud-based, Agile Methodology based, and process Unified Process modeled, certificate checker for certificate verification. However, the RDBMS used in the prototype does not support horizontal scalability, thus the built-in basic functions only let request and generate authenticated credentials.

Osman and Umar (2016) developed a model that integrates cloud technology and cryptography to improve the figure of certificate authentication. Though this approach enhances confidentiality and security its implementation costs restrain it from being a third-party cloud service provider.

According to Zheng et al., (2017), blockchain technology and smart contracts can be used to guarantee the immutability of certificate authentication. Nonetheless, they need to implement the two and carry out more work on the framework to appreciate what they have in mind.

Singhal and Pavithr (2018) came up with a certificate verification system through the application of QR codes and an application in smartphones. While the system incorporated digital signatures together with QR codes for verification, issues arose concerning security since the records of QR codes were stored insecurely.

Yusuf et al. (2018) proposed an automated batch certification, which comprised of the certificate formats and templates. However, the system lacked efficiency because it involved user entry of inputs and was only partly automated.

Based on the above-discussed concept, Jiin-Chiou et al. (2018) introduced a solution that anticipates the use of blockchain in certificate verification among institutions, students, and service providers. Despite the goal of improving the system's security, its utilization of a single hash key made it publicly available once the key was revealed.

Neehu & Vani (2018) proposed a web certificate verification system that used login credentials just as the authentication technique for the generation of web certificates, and this proposed system has serious security vulnerabilities due to the absence of an extra layer of system security.

San et al. (2019) deployed a certificate verification system by applying trusted ledgers of blockchain. While those are beneficial to the users by offering them control over their data, the system's implementation was complex, requiring a good understanding of blockchain technology, and did not include data privacy preservation mechanisms Obilikwu, Usman, and Kwashay (2019) designed a Top-Down Iterative Model for a generic Certificate Verification System for Nigerian Universities. Although the system overcame the issues of horizontal scalability and sharing at certain levels, it had some drawbacks concerning memory usage and flexibility.

The measures formulated by Gaonkar et al. (2020) incorporated informing the members of the certificate-issuing system which had an online sign-up process. However, the system was not quite efficient because certificates could be either faked or replicated, the information was compiled in the central database which could easily be hacked.

Saleh et al. (2020) put forward an architecture of verification of educational certificates based on blockchain that centered on authorization, authentication, confidentiality, ownership, and privateness. However, due to the only framework having a narrow range of applications and limitations when being adopted in the business environment.

In a more recent work, Aniket, Sagar, and Shivraj (2020) have also highlighted the call to design a proper digital certificate system to counter the problem of forgery. They suggested a decentralized certificate verification system that utilized a blockchain signature and timestamp of certificates. However, the expenses of putting into operation were relatively high, and another problem connected with the forgery of the digital signatures occurred.

Summarizing it is possible to state that a lot of approaches have been suggested to solve the problem of certificate verification, however, there are a lot of needs in developing systems that will afford to be scalable, secure, safe, and flexible in the sphere of the checking of the educational certificates legitimacy. Previous approaches include disadvantages which are as follows: the method often depends on manual operation, some approaches may have a problem in database management systems scalability, have problems with security, and problems connected with reliability of some verifying procedures. Based on these challenges, this document seeks to discuss and examine various strategies and methods that are employed in certificate verification systems. The subsequent sections will describe the methodology applied in this research, and then give a literature review. Subsequently, the document will describe the outcomes and future work concerning the analysis of major whooshes from the literature review. In the last section, the conclusion will be made, and suggestions for other further research studies will be given.

III. METHODOLOGY

In this study, we use the theoretical-methodological approach where the verification of students' skills and courses is based on the software development life cycle use of the Iterative & Incremental development models. Such models provide a clear framework for dissecting the whole verification process into measurable components and allowing for the cyclical approach.

The incremental model on the other hand breaks the verification task into smaller units where each unit is incremental to the previous one. This allows for progressive breakdown in evaluating the students' skills as well as the courses making it easier to make changes and implement them as the verification goes on.

In the same manner, the iterative model presupposes the analytical repetition of the verification processes in several cycles called iterations. In each cycle, the data received is taken into consideration and improvements made for the next cycle result in the generation of the next version of the verified skills and courses. This process is a cycle and is repeated until the best verification result is obtained as the optimal outcome.

Using these two models, the present research would also like to avoid a poor definition of student skill demands and course validation criteria. Further, requested enhancements and consequent phases of development of new functionalities can be smoothly integrated, which in turn ensures the constant improvement and flexibility of the verification procedure.

Figure 1 illustrates the diagram depicting the application of Iterative and Incremental development models.

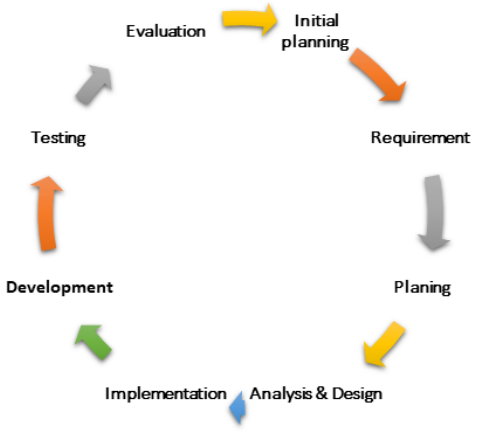

Figure 1. Active and Incremental Model

IV. PROPOSED SYSTEM FRAMEWORK

In this section, the features available to students, the verifiers, and universities making use of the structure of the proposed system as explained in section, Figure 2 are discussed.

To use the certificate creation, element of the given blockchain-based system, an institution must pass through the registration process initially. Once registered, the university gains system access and can generate certificates using two methods: creation of many records with a definition csv layout or unique record generation with probably the ability to control fields.

Finally, every generated certificate is stored in the form of an IPFS file for file safety. For each of the certificates the ID or hash, the system creates in addition to a two-dimensional bar code of a QR type that in addition has contents of an SHA-256 type. All these identifiers along with the details written in the certificate will be stored in the network of blockchains. Registered legit certificates are assigned the deserved hash IDs and the QR codes are provided to the student for online validation of the certificates.

Once again, all the certificates excluding duplicate ones can be verified by the hash or the QR code either by the verifiers or anyone. The copy of the certificate attached by the user that he or she uploads can also be verified with that of the certificate generated by the system. Among all these aspects, it is quite appreciable to mention that underneath the certificate, from any illegitimate interference and change it is saved safely.

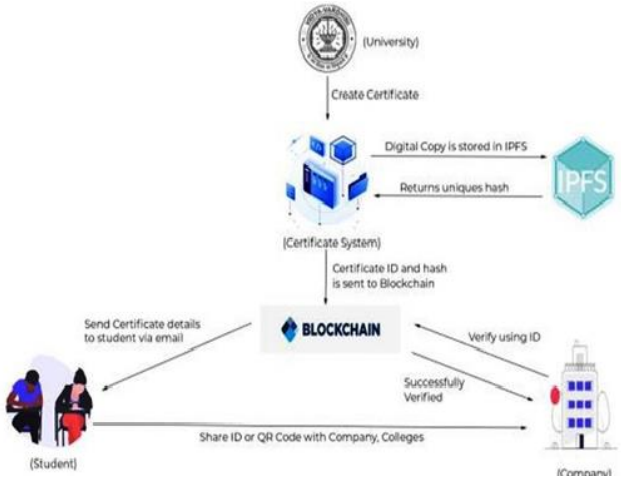

Figure 2. New System Framework (Ravi et al, 2021)

V. THE ARCHITECTURE OF THE NEW SYSTEM

Figure 3 illustrates the architectural design of the newly developed system for managing African locally incorporated banks.

It consists of four main components: It has clients, Interplanetary File System (IPFS), Database, and Blockchain.

Clients can be user administrators or institutes that are responsible for the validation of certificates. For every client who initiates a request in the system, the following happens to the request. Secondly, there is spring security as well as JWT (JSON Web Token) for user authentication and request validation. When the request is successfully approved by the security layer, it proceeds to the request processor unit. In the case of services architecture, services, and controllers have the request, deal with the needed operations, and supply a response that is provided to the client.

The IPFS is used concerning storage, being used to store certificate documents or other information. Meanwhile, the database contains different data and information characterizing the entities of a system such as user information as well as certificate information. The system also communicates with the blockchain network to create a hash code for every certificate. The same communication link is kept when there is a certification exercise, or when undertaking any similar processes.

Thus, it guarantees secure user authentication, effective request handling, precise data storage applying IPFS, and connection with the blockchain-based network to check certificates and hash.

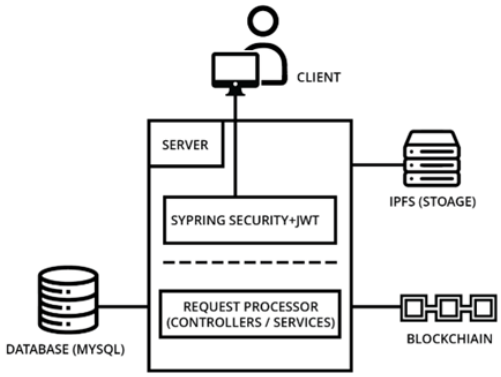

Figure 3. Architectural Diagram

In the system architecture overall, every process represented in Figure 3 occurs following a successful confrontation with the security layer. Nevertheless, not all requests are authenticated that is when dealing with certificates. Some users do not need to sign in for the certificate verification which in turn means that in cases where authentication might be required, it is not necessary. On the other hand, administrative requests such as the addition and modification of data do call for authentication.

The spring security component deals with sessions for the current users and their details and JWT is responsible for generating tokens for authentication. When a user logs in, it makes a token and to each request the user makes, the token is used to check the legitimacy and authorization level of the user. The JWT first occurs to the request, then it verifies the user and determines whether the token has expired. This way, irrespective of the token's validity or expiry status, the JWT informs the spring security component or subcomponent, which alone is charged with the verdict on whether to accept or deny the request.

If the JWT can authenticate the user, and the user has passed through an authentication process and has a valid token, then the spring security component passes the request to the request processor to process. The response is then passed and sent back to the user. On the other hand, when the user verification is unsuccessful the spring security component prevents the request from being executed. In this context, these functionalities that are referred to as the security layer belong to the server architecture while the request processor layer is also part of the server architecture that can support them.

VI. ALGORITHM OF THE SYSTEM

```
Begin
    Upload student records
    If records already exist, go to step 8
    Else, print "Upload successful"

    Create certificates
    Store certificates in IPFS (InterPlanetary File System)
    Generate a certificate with a unique hash code
    Generate a QR code for the certificate

    Preview the certificate

    Send the certificate details to the student via email or SMS

End
```

Figure 4. Algorithm of The System

This algorithm outlines the steps to be performed to upload student records, check if the records already exist, create certificates, store them in IPFS, generate a certificate with a unique hash code, generate a QR code for the certificate, preview the certificate, and send the certificate details to the student via email or SMS. The algorithm then ends.

VII. FLOWCHART OF THE SYSTEM

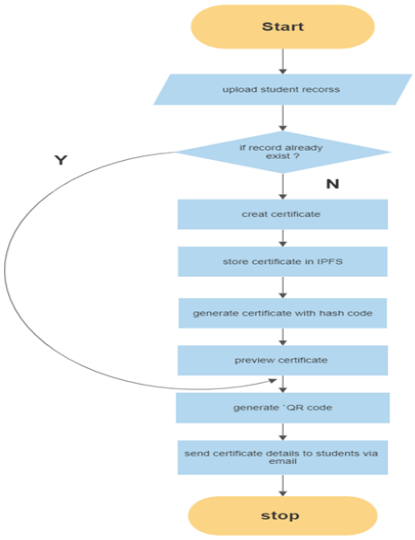

Figure 5. Flowchart of the System

VIII. CERTIFICATE GENERATION PROCESS

UI DESIGN

Certificate viewer for the user or receiver

Figure 6. UI DESIGN(STEP1)

See all your certificates in one place.

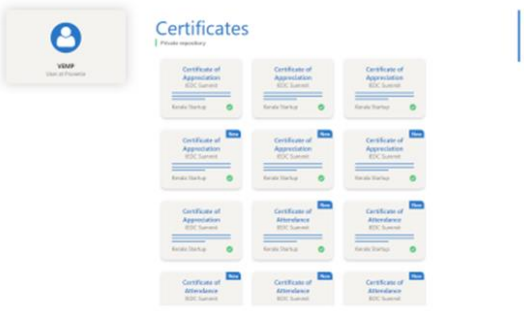

Figure 7. UI DESIGN(STEP2)

Directly share/post your achievements on social media.

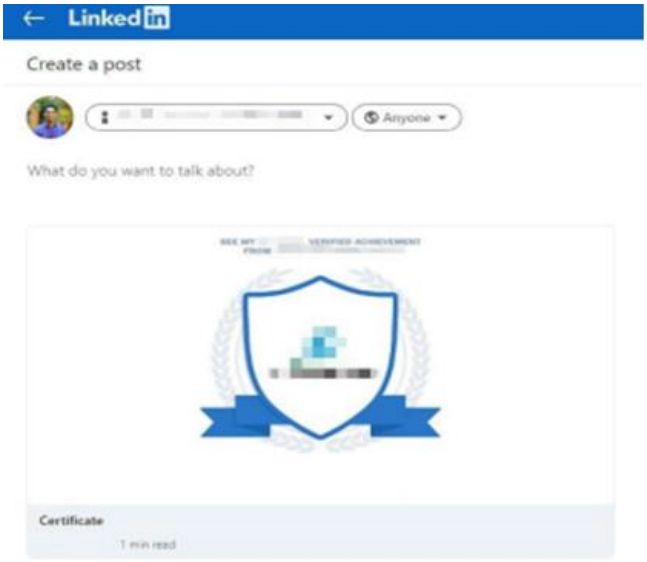

Figure 8. UI DESIGN(STEP3)

email notification to the receiver when they receive new certificates

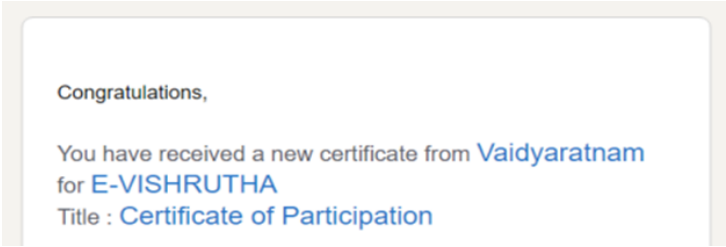

Figure 9. UI DESIGN(STEP4)

Choose from predesigned templates for easy certificate

creation.

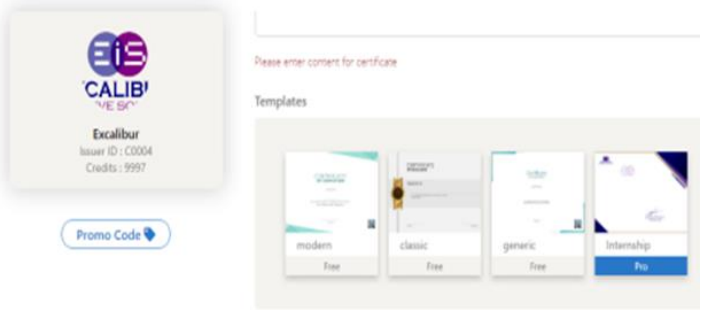

Figure 10. UI DESIGN(STEP5)

Enter all recipient’s email id’s at once and in one click issue all certificates.

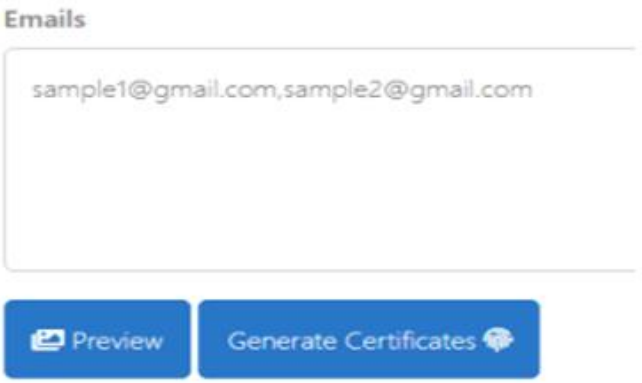

Figure 11. UI DESIGN(STEP6)

IX. VERIFICATION USING QR CODE

The validator has another way through which he can be certain of the scanned QR code. They can even bar code scan the code, and this is usually provided by the students or graduates during the application or entry as highlighted by the QR Figure. This verification procedure can be done using the QR Code Extension found in commonly used browsers such as Chrome, Firefox, and Internet Explorer. Likewise, the use of mobile devices can also successfully perform this procedure with the support of the QR code scanner applications.

Figure 12. QR Code

An invalid Certificate ID is being rejected.

Figure 13. Rejection Message

If the QR code scanned matches the code registered in the system, they will be brought to the preview of the certificate as shown in the figure below: Successful Verification of the Document generates a preview and prints the data. On the other hand, if the QR code scanned does not match the one in the system an error message is

displayed, informing the user that verification has been unsuccessful; an invalid Certificate ID for instance would look like this (Figure13).

X. CONCLUSION

This paper specifically concentrated on generating and verifying certificates and in doing so, intended to reduce the limitation in the current systems by integrating blockchain and QR codes. The formulated system enables only the university administrator to create as well as upload certificates and the records cannot be tampered with. The disruption of manual work in generating the certificates can be eliminated with the help of automation and the chances of losing the certificates whose generation lies with the students are also decreased. Integration of QR code helps in sustaining a clean and genuine record and thus helps in the prevention of tempering. The hash of the certificate is archived in the blockchain while the full document to the Inter Planetary File System (IPFS) to avoid document loss and corruption.

In terms of future work, several areas can be explored for further research: In terms of future work, several areas can be explored for further research:

- Access control system: Speaking of the security of the system, an access control mechanism to the admin application will limit the access point to only the authorized university authorities.

- Session management: The server can leverage sessions to make sure that all the actions towards the system are made through the client application boosting the level of security.

Biometric authentication: The use of fingerprints and facial recognition are methods that can add to the security and versatility of the system.

These areas can be considered the directions for future research and development of the enhancement in the functionality and security of the certificate generation and verification system.

REFERENCES

[1] Fedorova, E.P. and Skobleva, E.I., 2020. Application of blockchain technology in higher education. European Journal of Contemporary Education, 9(3), pp.552-571.

[2] Fernández-Caramés, T.M. and Fraga-Lamas, P., 2019. Towards next generation teaching, learning, and context-aware applications for higher education: A review on blockchain, IoT, fog and edge computing enabled smart campuses and universities. Applied Sciences, 9(21), p.4479.

[3] Fulmer, N., 2018. Exploring the legal issues of blockchain applications. Akron L. Rev., 52, p.161.

[4] Funk, E., Riddell, J., Ankel, F. and Cabrera, D., 2018. Blockchain technology: a data framework to improve validity, trust, and accountability of information exchange in health professions education. Academic Medicine, 93(12), pp.1791-1794.

[5] Ghazali, O. and Saleh, O.S., 2018. A graduation certificate verification model via utilization of the blockchain technology. Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 10(3-2), pp.29-34.

[6] Gilda, S. and Mehrotra, M., 2018, January. Blockchain for student data privacy and consent. In 2018 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-5). IEEE.

[7] Guo, J., Li, C., Zhang, G., Sun, Y. and Bie, R., 2020. Blockchain-enabled digital rights management for multimedia resources of online education. Multimedia Tools and Applications, 79(15), pp.9735-9755.

[8] Hameed, B., Khan, M.M., Noman, A., Ahmad, M.J., Talib, M.R., Ashfaq, F., Usman, H. and Yousaf, M., 2019. A review of Blockchain based educational projects. International Journal of Advanced Computer Science and Applications, 10(10).

[9] Han, M., Li, Z., He, J., Wu, D., Xie, Y. and Baba, A., 2018, September. A novel blockchain-based education records verification solution. In Proceedings of the 19th annual SIG conference on information technology education (pp. 178-183).

[10] Hardini, M., Aini, Q., Rahardja, U., Izzaty, R.D. and Faturahman, A., 2020, October. Ontology of Education Using Blockchain: Time Based Protocol. In 2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS) (pp. 1-5). IEEE.

[11] Haugsbakken, H. and Langseth, I., 2019. The blockchain challenge for higher education institutions. Eur. J. Educ, 2(3), p.41.

[12] Holotescu, C., 2018. Understanding Blockchain Opportunities and Challenges. eLearning & Software for Education, 4.

[13] Hughes, L., Dwivedi, Y.K., Misra, S.K., Rana, N.P., Raghavan, V. and Akella, V., 2019. Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. International Journal of Information Management, 49, pp.114-129.C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, and M. Miller, "Rotation, scale, and translation resilient public watermarking for images," IEEE Trans. Image Process., vol. 10, no. 5, pp. 767-782, May 2001.