Eksplorium *p*-ISSN 0854-1418
Volume 47 No. 1, January 2026: 310–318 *e*-ISSN 2503-426X

Investigating the Application of Electronics and Quantum Coding in Identity Recognition

Hesam Addin Goliyzadeh

Electronic Engineering, Linear Integrated Circuits, Non-Profit Lamee University, Gorgan, Iran

Article Received: 01 December 2025, Revised: 16 January 2026, Accepted: 26 January 2026

ABSTRACT

One of the important issues in today's society that is a concern for many experts and users is the issue of security and identity recognition and verification. Today, in matters related to the security of places such as universities, airports, ministries and even computer networks, the use of biometric methods in identifying or verifying the identity of individuals has become very common. New information technology has become an important factor in the future development of the financial services industry, especially the banking industry. The growth of international trade and the difficulties in transferring money have given researchers the necessary motivation to introduce a new structure. Internet banking is the newest way to provide banking services. Internet banking, facilitated by electronic commerce technologies, has helped commercial banks to remain competitive by increasing profitability, reducing transaction costs and improving customer service.Security for online banking has changed dramatically over the relatively short period that online banking has been in use. In particular, authentication in early systems was vulnerable to a variety of attacks, such as phishing attacks, and in some cases still is. There is no doubt that quantum encryption protocols are capable of quickly detecting any attempt to attack the cipher and the authentication process. In this paper, we present a model for authentication in online banking using quantum encryption.

Keywords : Quantum encryption - Security – Authentication

INTRODUCTION

One of the important issues in today's society that is a concern for many experts and users is the issue of security and identity recognition and verification. Today, in matters related to the security of places such as universities, airports, ministries and even computer networks, the use of biometric methods in identifying or verifying the identity of individuals has become very common. Advanced office attendance systems, security systems for entering and exiting specific places, notebooks equipped with fingerprints, etc. use various biometric identification methods (Abbas Roustaei, 1404). Biometric technologies, including fingerprints, iris scanning and facial recognition, have become key tools for identifying identity in recent years. In the meantime, facial recognition plays a vital role in identity verification, especially in security centers, law enforcement agencies and public places.With the advancement of facial recognition technologies, criminals' attempts to conceal their identities through facial changes have become a security challenge. Despite the increasing need for this technology in Iran, the development of indigenous and efficient tools in this area is of particular importance (Mohammad Zolfaghari and Ehsan Ebrahimi, 2014). There are various definitions of Internet banking in the literature, which refers to conducting banking transactions via electronic devices over the Internet. Technological developments, especially in the fields of telecommunications and information technology, have transformed the banking industry, and the importance of Internet banking is increasing due to its wider reach and lower cost per transaction. Most banks use the Internet as a new distribution channel.Since the introduction of "home banking" services by the Big Four New York banks in 1981, Internet banking has brought about many changes in commercial banking practices. The past four years have witnessed dramatic technological changes, including the advancement of electronic commerce, or the exchange of goods (tangible or intangible) and payments over telecommunications systems. This includes various initiatives such as Internet banking, online payment systems, telephone banking, and mobile banking. The potential capabilities of this technology, especially in the banking industry, are significant.Many banks have

established a presence on the Internet, and others are doing the same using telecommunications technologies and systems. A bank can reach its customers and not only provide them with general information about its services, but also allow them to conduct interactive financial transactions.

By capitalizing on the potential of electronic commerce to generate profits, reduce transaction costs, improve customer service, and be flexible in meeting the changing needs and lifestyles of its customers, Internet banking has enabled banking institutions to compete more effectively in this global environment, developing products and services beyond the constraints of time and space.

Due to its interactive nature, the Internet as a service delivery channel is fundamentally different from other channels such as branch networks or telephone banking.Internet banking was initially introduced as a new solution using software and a private network. The Internet and the World Wide Web have now affected the way banks conduct business. Today, international trade has grown significantly. Recently, deregulation and globalization have led to a large growth in the value of non-trade-related financial transactions. The range of functions typically provided by Internet banking telecommunications systems includes displaying statements and balances, paying bills, transferring money between accounts, viewing regular payments and direct credits, viewing transactions with search and sorting capabilities, ordering checkbooks, and transferring information to other software such as a personal financial manager. Therefore, this article examines the application of electronics and quantum coding in identity verification.

RESEARCH BACKGROUND

Seyed Mohsen Mousavi Khvansari conducted a study in 2025 entitled Simulation and Capacity Estimation of the Four-Qubit GHZ Mode Ultra-Compressive Coding Protocol on the IBM Quantum Computer. In this paper, an innovative protocol for quantum ultra-compressive coding based on the four-qubit GHZ mode has been developed. This new protocol has been designed with the aim of utilizing the maximum capacity of quantum systems and has been comprehensively investigated from a theoretical perspective. In this regard, the coding capacity of the protocol has been compared with the Holevo bound, which specifies the maximum information that can be extracted from a quantum system. To validate this protocol, simulations have been performed using quantum computing software. For practical verification, the protocol has been implemented on the IBM quantum computer. These steps allow researchers to compare theoretical and practical results.The experimental results showed differences from the theoretical predictions; in the theoretical results, each state had a 50% probability of occurrence, but in practical conditions, these values changed to 50.19531% and 49.80469%. The mentioned difference is caused by environmental noise and qubit-environment interactions; an issue that is considered one of the fundamental challenges in the field of quantum computing. This research not only examines these challenges, but also emphasizes the importance of finding solutions to reduce noise and improve the accuracy of measurements. To display the results, bar graphs are used, which are an effective tool for presenting data visually and facilitating more detailed analysis. Using these graphs makes it easier to understand patterns and inconsistencies in the data and allows researchers to identify and analyze more details.Overall, this research contributes significantly to the development of knowledge in the field of quantum computing by providing a new protocol and carefully examining the challenges and capabilities of quantum technologies. These achievements can pave the way for further advances in this emerging technology (Seyed Mohsen Mousavi Khansari, 2025).

Hamed Taghvai and Masroor Hassan in 2025 published a study titled Computational Complexity Analysis of Classical to Quantum Data Coding Methods: A Systematic Review. This paper provides a comparative analysis of data coding techniques in QML algorithms. We consider methods such as basis coding, domain coding, angle coding, and quantum coding based on 2QRAM. It also analyzes their efficiency in representing classical data in the quantum framework, considering factors such as suitability for different data types, efficiency in leveraging quantum properties such as superposition, and the impact on algorithm complexity. The strengths and weaknesses of each approach are compared, and a unique analysis of the asymptotic computational complexity of these algorithms is also presented.This comparison will guide the selection of the optimal encoding method for different

QML applications and ultimately pave the way for more efficient and powerful quantum machine learning models (Hamed Taghvaei and Masroor Hassan, 2025).

Seyyed Mohsen Mousavi Khansari and Mehdi Sadeghi conducted a study in 2023 entitled Quantum Ultracompact Coding Using Multipartite States. The aim of this research is to build a quantum ultracompact coding protocol that can transmit four bits of classical information by sending only two qubits using a four-partite quantum channel.Alice and Bob initially have a shared maximally entangled state of four qubits. Alice can create sixteen orthogonal maximally entangled states by locally manipulating her two qubits, which are used to encrypt the message sent to Bob. Bob decodes the four-bit message by measuring the generalized Bell state (Seyed Mohsen Mousavi Khvansari and Mehdi Sadeghi, 2023).

Omid Rahmani et al. conducted a study in 2025 entitled Intrusion Detection in IoT Networks Based on Flow Analysis and Behavioral Aggregation at the Execution Level. In this study, a network intrusion detection framework without packet content analysis is presented, which is based on aggregation of traffic information at the execution level. The traffic of an ESP32-based IoT network is modeled using the ns-3 simulator, and more than 480 independent executions including four traffic scenarios, normal, denial of service, rebroadcast, and impersonation, are analyzed. The results show that execution-level analysis, in the best configuration, achieves an accuracy of about 78% and a Macro-F1 of close to 0.77 in distinguishing four traffic classes, while the mere use of minimal QoS-based features reduces the accuracy to about 42%.These results show that the proposed framework, while maintaining its lightweight nature and without analyzing packet content, is a suitable option for deployment in real Internet of Things environments with limited resources (Omid Rahmani et al., 2025).

In 2024, Sajjad Ali Mohammadi and Mohammad Ghasemi Tadvani conducted a study entitled Presenting a Cyber Attack Detection System in the Industrial Internet of Things Using a Neural Network in Combination with the Gray Wolf Metaheuristic Algorithm and the Refrigeration Tree. In this paper, an attempt has been made to present a model to increase the accuracy of the Industrial Internet of Things intrusion detection system against cyber attacks, a combined method based on the Gray Wolf Metaheuristic Algorithm and Refrigeration Simulation with the Neural Network algorithm. First, the data was preprocessed and normalized, then in the next stage, the data was tested and evaluated using the Gray Wolf Metaheuristic Algorithm and Refrigeration Tree Simulation and their combination with the Neural Network algorithm. Based on the results obtained, the use of the SA-ANN hybrid algorithm has an accuracy of 88.4091 percent and the GWO-KNN has an accuracy of 93.2273 in detecting cyber attacks.It was found that using the combined GWO-KNN algorithm with an accuracy of 93.2273% performed better in terms of accuracy in feature selection and attack detection rate (Sajjad Ali Mohammadi and Mohammad Ghasemi Tadvani, 2024).

In 2024, Mohammad Zolfaghari and Ehsan Ebrahimi conducted a study entitled Presenting a Hybrid Method for Detecting Facial Change Using Image Processing: A Machine Learning Approach. This research aimed to identify and analyze features related to facial change in facial recognition methods based on image processing and machine learning. The results of this study show that the Naive Bayes algorithm with an accuracy of 93.30% and the K-nearest neighbor algorithm with an accuracy of 86.30% performed significantly in detecting facial changes; also, the hybrid method with an accuracy of 96.67% performed better. The findings of this study can lead to improving the accuracy and efficiency of surveillance and security systems. Emphasis on privacy aspects is necessary along with the development of these systems.It is hoped that the results of this research will pave the way for the development of more advanced algorithms and the implementation of more efficient systems in the field of facial change detection (Mohammad Zolfaghari and Ehsan Ebrahimi, 2024).

Seyyed Hossein Jafarzadeh and Ghazaleh Mohammad Hosseini conducted a study in 2025 entitled Automatic Evaluation and Recognition of Facial Features with Convolutional Neural Networks in the Problem of Identity and Emotion Recognition. In this study, the performance of convolutional neural networks (CNN) for the separate recognition of facial expressions and identities was investigated. For this purpose, four basic experiments were designed in which single-task networks were trained separately to recognize emotional expressions and identities of individuals. In the first stage, the limited CK dataset consisting of 281 images with 3 emotional expressions and 10 identities was used. After that, to evaluate the effect of increasing the data volume, the same networks were

p-ISSN 0854-1418
e-ISSN 2503-426X

tested on a larger version of this dataset (including 2816 images with 7 emotional expressions and 96 identities).The results show that the increase in data and the design used in optimizing the network in line with the changes in parameters had a significant impact on improving the performance of the models; so that the accuracy of recognizing emotional states increased to 80.96% and the accuracy of identifying identity increased to 42.96%. These findings clearly demonstrate the effective role of CNN architectures in extracting features related to identity and facial emotions, even in limited data conditions. The present study can be used as an effective step for developing more accurate facial recognition systems in areas such as intelligent interaction and behavioral analysis (Seyed Hossein Jafarzadeh and Ghazaleh Mohammad Hosseini, 2025).

In 2025, Zahra Saeedi conducted a study entitled Investigating New Methods and Artificial Intelligence in Identity Recognition from the Perspective of Scientific Police. Therefore, the purpose of this study is to investigate new methods and artificial intelligence in identity recognition from the perspective of scientific police.This research was completed in a descriptive and applied manner based on external internet and library resources. The results obtained indicate new methods of identification, including identification through tooth patterns, palm vein patterns, identification of earlobe patterns, gait patterns, voice recognition technology, iris and retina ophthalmography, automatic fingerprint recognition, facial recognition systems, rapid DNA analysis and analysis, examination and analysis of heat patterns emitted from the face or body, and also the role of artificial intelligence in increasing the ability to identify and recognize identities in the field of scientific police (Zahra Saeedi, 2025).

Mohammad Zolfaghari in 2025 AH conducted a study titled Presenting a Hybrid Method for Detecting Face Change Using Image Processing: A Machine Learning Approach. This research was conducted with the aim of identifying and analyzing features related to face change in face recognition methods based on image processing and machine learning. The results of this research show that the Naive Bayes algorithm with an accuracy of 93.30% and the K-nearest neighbor algorithm with an accuracy of 86.30% performed significantly in detecting face changes; also, the hybrid method with an accuracy of 96.67% provided better performance. The findings of this study can lead to improving the accuracy and efficiency of surveillance and security systems. Emphasis on privacy aspects is necessary along with the development of these systems.It is hoped that the results of this research will pave the way for the development of more advanced algorithms and the implementation of more efficient systems in the field of facial change detection (Mohammad Zolfaghari, 2025).

AUTHENTICATION IN INTERNET BANKING SYSTEM

In Internet banking systems, banks must ensure that users feel secure when using Internet banking services. They can control the level of authentication they undergo to log in to the site. They can identify and limit attackers by making it difficult for fraudsters to access customer accounts.

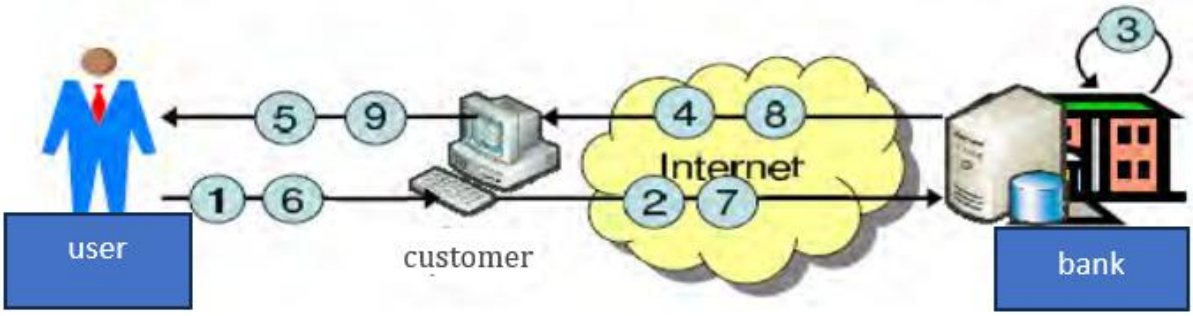

Figure 1. Identity verification in online banking

Figure 1 shows the authentication process in the old Internet banking system. The steps that need to be followed in this Internet banking system are as follows:

1) Generate user ID and password

p-ISSN 0854-1418
e-ISSN 2503-426X

2) Transfer user ID and password

3) Verify user ID and password

4) Transfer service options

5) Display service options

6) Request transaction

7) Transfer transaction request

8) Confirm transfer request

9) Display transaction confirmation

QUANTUM CODING

Quantum coding is based on the Heisenberg uncertainty principle of quantum mechanics and the polarization of photons. According to the Heisenberg uncertainty principle, it is not possible to measure the quantum state of a system without disturbing that system. Therefore, the polarization of a photon or light component can only be determined at the point where it is measured. Second, the photon polarization principle describes how photons of light can be polarized or shaped in a particular direction. Furthermore, a polarized photon can only be detected by a correctly polarized photon filter, otherwise it is lost. It is this "one-way nature" of photons in the Heisenberg uncertainty that makes quantum coding an attractive option for ensuring data confidentiality and neutralizing eavesdropping.

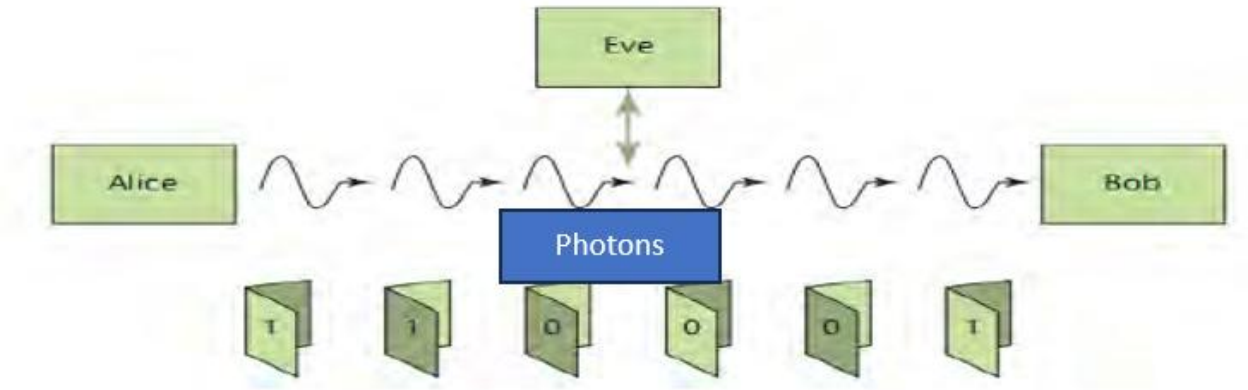

Figure 2. The basic idea of quantum coding

The concept of quantum coding (QC) was introduced by Bennett and Brassard in the early 1980s. The BB84 protocol was the first quantum key distribution (QKD) protocol, introduced by Bennett and Brassard in 1984.

Other protocols such as the two-state protocol, the six-state protocol, the Einstein–Podolsky–Rosen protocol, and others were then successful. All of them featured perturbations of quantum states caused by carelessness. However, most experiments on quantum coding are now focused on the BB84 protocol due to its simplicity and the need for fewer physical devices for implementation. In the early 1990s, the first experiments were performed by Charles Bennett and Brassard and their colleagues at the IBM Laboratory at a distance of 30 cm and through the air. The first successful demonstration on an optical fiber was performed at the University of Geneva in 1993.

p-ISSN 0854-1418
e-ISSN 2503-426X

QC IN INTERNET BANKING

Internet banking is becoming increasingly complex. The Internet is becoming increasingly popular for checking balances and statements and transferring funds between accounts around the world. As wired and wireless banking becomes more widespread around the world, their security remains a major concern among users.

Today, banks and financial institutions use symmetric or asymmetric encryption. However, due to the advancement of sophisticated technology and encryption mechanisms, security solutions are not completely secure. As computers become more powerful, encryption and decryption keys need to be longer in order to maintain a level of difficulty. Therefore, transactions can be destroyed or altered without the bank's knowledge.This poses a serious risk, as criminals and malicious organizations can exploit this vulnerability to commit theft and fraud. Securing financial transactions is imperative and the need to combat economic crime is increasing.

One of the biggest concerns in online banking is cyber threats. This section discusses the most important challenge of online banking, namely, authentication. Since most online banking applications use passwords or PINs to complete business transactions, researchers are actively involved in developing secure methods for online banking over the Internet. Authentication is a more critical issue in online banking. The banking industry is regulated and supervised by the government, and online banking must assure regulators that its customers are safe.Researchers around the world are experimenting with new techniques for authentication to make online banking more secure. The idea is that user information can be transmitted via QKD. Quantum cryptography has attracted the attention of banks, companies, and institutions, and many are testing the technology, which is commercially available.

Single-factor authentication in online banking is no longer sufficient to protect accounts. Our goal is to propose an authentication method for online banking security. The starting point is the user request. After creating the request, the user is directed to an authentication service that requires their password or PIN. After verifying that password, the user has access to the quantum code system. The presence of quantum cryptography / quantum key distribution is only required for the purpose of authentication.The entities involved in this system include the user, the user's password / PIN, and the quantum code system.

We are mapping the entire authentication process using user authentication and user authentication using QKD to decide whether to grant access or not.

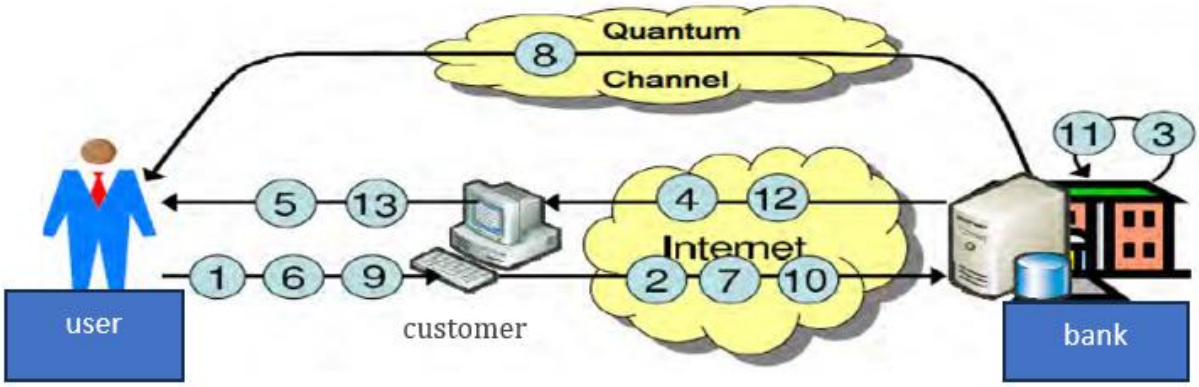

Figure 3. User authentication through quantum cryptography

Here we have a step-by-step diagram of our proposed authentication mechanism. In this proposed model, we introduce the concept of quantum encryption for authentication. Figure 3 shows the authentication steps. We have used two levels of authentication to make the authentication in the online banking system stronger.

1) Generate User ID and Password

2) Transfer User ID and Password

3) Verify User ID and Password

4) Transfer Service Options

5) Display Service Options

6) Request Transaction

7) Transfer Transaction Request

8) Distribute Quantum Key

9) Generate Quantum Code

10) Transfer Quantum Code

11) Verify Quantum Code

12) Transfer Transaction Confirmation

13) Display Transaction Confirmation

This authentication scheme is an improved form of standard authentication that establishes the customer's identity for the Internet banking system.The power of this quantum identity auction is that it allows the user to have more confidence in any communication with the bank and gives users a sense of security when logging into their user accounts.

CONCLUSION

New information technology is becoming an important factor in the future development of the financial services industry, and especially the banking industry. Internet banking is multifaceted and has been affected by technological changes, deregulation of parts of finance, the emergence of new banking institutions, and economic restructuring. The relationship between theory and practice may be considered weak and unstructured, as qualitative methods have been criticized for not inducing theoretical factors. In order to achieve this goal, this paper attempts to address this issue by creating a theoretical framework that may enhance the security of Internet banking.Today, the cost of a quantum encryption system is estimated to be around hundreds of thousands of dollars, but we expect this system to become cheaper and to be implemented in banks within the next few years.

REFERENCES

[1] Ali Mohammadi, Sajjad and Ghasemi Tadvani, Mohammad, 2024, Presenting a Cyber Attack Detection System in the Industrial Internet of Things Using Neural Network in Combination with Gray Wolf Metaheuristic Algorithm and Refrigeration Tree, Third Cyberspace Conference, Tehran, https: / / civilica.com / doc / 2384062

[2] Jafarzadeh, Seyed Hossein and Mohammad Hosseini, Ghazaleh, 2025, Automatic Evaluation and Recognition of Facial Features with Convolutional Neural Networks in Identity and Emotion Recognition, Second International Conference on "Artificial Intelligence in the Era of Digital Transformation (Innovations, Challenges and Opportunities)", Tehran, https: / / civilica.com / doc / 2339302

[3] Mousavi Khansari, Seyed Mohsen and Sadeghi, Mehdi, 2025, Quantum Ultra-Compact Coding Using Multipartite States, Seventh National Conference on Applied Research in Electrical, Mechanical and Mechatronics, Tehran, https: / / civilica.com / doc / 1920768

[4] Mousavi Khansari, Seyed Mohsen, 2025, Simulation and capacity estimation of the GHZ four-qubit ultra-compact coding protocol on the IBM quantum computer platform, Iranian Journal of Electrical and Electronics Engineering, Volume: 22, Issue: 2, https: / / civilica.com / doc / 2346283
[5] Rahmani, Omid and Mohammadzadeh, Javad and Shahkarami, Rezvan, 2025, Intrusion Detection in Internet of Things Networks Based on Flow Analysis and Behavioral Aggregation at the Execution Level, Quarterly Journal of Information Technology and Law Enforcement Communications, Volume: 6, Issue: 24 https: / / civilica.com / doc / 2571282
[6] Roustaei, Abbas, 2025, Identity Recognition from Iris with Artificial Neural Network and Discrete Wavelet, https: / / civilica.com / doc / 2376865
[7] Saeedi, Zahra, 2025, Investigation of new methods and artificial intelligence in identity recognition from the perspective of scientific police, Fifth International Conference on Advanced Research in Management and Humanities, https: / / civilica.com / doc / 2325804
[8] Taghvaei, Hamed and Hassan, Masroor, 2025, Computational Complexity Analysis in Classical to Quantum Data Coding Methods: A Systematic Review, First National Conference on "Artificial Intelligence and Emerging Research: Convergence of Human and Intelligent Systems", Tehran, https: / / civilica.com / doc / 2323413
[9] Zolfaghari, Mohammad and Ebrahimi, Ehsan, 2024, Presenting a Hybrid Method for Face Change Detection Using Image Processing: Machine Learning Approach, Security-Protection Research, Volume: 13, Issue: 50, https: / / civilica.com / doc / 2350890
[10] Zolfaghari, Mohammad, 2025, Presentation of a hybrid method for face change detection using image processing: a machine learning approach, First National Conference on "Artificial Intelligence and Emerging Research: Convergence of Human and Intelligent Systems", Tehran, https: / / civilica.com / doc / 2323344
[11] M.S. Sohail, B. Shanmugham, E-banking and customer preferences in Malaysia: An empirical investigation, Information Sciences (2003).
[12] Osho, G.S., How technology is breaking traditional barriers in the banking industry: Evidence from financial management perspective. European Journal of Economics, Finance and Administrative Sciences, 2008(11): p. 15-21.
[13] A.M. Aladwani, Online banking: a field study of drivers, development challenges, and expectations, International Journal of Information Management 21 (2001) 213-225.
[14] Turban, E., et al., Electronic commerce: a managerial perspective. 4th Edition ed. 2008: Prentice Hall.
[15] M.H. Shah, F.A. Siddiqui, Organisational critical success factors inadoption of e-banking at the Woolwich bank, International Journal of Information Management 26 (2006).
[16] C.S. Elizabeth Daniel, On-line Banking: Strategic and Management Challenges, Long Rang
[17] e Planning 30 (1997) 890-898.
[18] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proc. IEEE Int. Conf. Computers, Systems and Signal Processing, New York, Bangalore, India, 1984, pp. 175-179.
[19] C.H. Bennett, G. Bessette, G. Brassard, L. Salvail, and 1. Smolin, Experimental quantum cryptography, Advanges in Cryptology Eurocrypt '90 Proceedings, pages 351-366, May 1990.
[20] Muller, 1. Breguet, and N. Gisin, Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than lkm, Europhysics Letters, 23:383-388, August 1993.
[21] Anand Sharma, Vibha Ojha, R.C.Belwal, Vishal Goar “Quantum cryptography – The Concept and challenges” in proceeding of 2nd International Conference on Computer and Automation Engineering (ICCAE 2010) Singapore, volume 1, 2010 pp. 710-714.
[22] Lee Y. G., "The influence of security and risk perception on the reuse of internet banking", The Journal of MIS Research, Vol.17, No.1, 2007, pp.77-93 .
[23] Anand Sharma, Vibha ojha, R.C.Belwal, Gaurav Agarwal “Transmission and System Control in Quantum Cryptography” International Journal of Computer Technology and Applications. Volume 2 (3) 2011 pp. 590-593 .
[24] Suh, B. and I. Han, "Effect of trust oncustomer acceptance of Internet banking", Electronic Commerce Research and Applications, Vol.1, 2002, pp.247-263 .

[25] Yu I. and So S. H., "An empirical study on the factors influencing the usage intention of internet banking systems", The Journal of Industrial Economic Research, Vol.17, No.6, 2004, pp.2383-2404 .
[26] M. Quaddus, D. Achjari, a model for electronic commerce success, telecommunications policy (2005) 127-151.
[27] M. Pohjola, "The New Economy: Facts, Impacts and Policies," Information Economics and Policy, 14, 2002. pp. 133–144.
[28] C.S. Yiua, K. Grantc, D. Edgar, Factors affecting the adoption of Internet Banking in Hong Kong—implications for the banking sector, International Journal of Information Management 27 (2007) 336-351.
[29] C.S. Elizabeth Daniel, On-line Banking: Strategic and Management Challenges, Long Range Planning 30 (1997) 890-898.
[30] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," MIS Quarterly, vol. 27, no. 3, pp. 425-478, 2003.
[31] B. H. Wixom and P. A. Todd, "A theoretical integration of user satisfaction and technology acceptance," Information System Research, vol. 12, no. 1, pp. 85-102, 2005.