Systematic Literature Review on Quantum Cryptography

Manav Sohal [1], Mandeep Kaur Sandhu [2,*], Rupinder kaur[3]

[1,2,3] Guru Nanak Dev University College, Pathankot, Punjab, India

***** Correspondence: gimeti4@gmail.com

Abstract

In the field of cryptography, new tasks are generated when advancement has taken place from conventional computing to quantum computing. In case of computer security, cryptography had always been a valuable and essential tool.When quantum mechanics principles are applied to cryptography, it gives rise to a new system that will secure communication and also assures that no spying can take place.The work below presents the review on quantum cryptography, which includes the concept of quantum cryptography and what can be its evaluation measures. Articles of quantum cryptography from various databases has been studied. In this SLR various research questions are identified and on the basis of their answers results have been formulated for this review along with that various performance measures are also discussed.

Keywords: cryptography; quantum; image encryption

1.Introduction

Cryptography is the science dealing with the encryption and decryption of the data in order to secure it and avail a secure transmission. In order to do so, encryption is performed by adding additional information and the encrypted image (also known as CIPHER Image) is brought in the original form by performing decryption on it [17]. For the purpose keys are used which are randomly generated, but are vulnerable to eavesdropping but by employing Quantum communication, i.e. using key distribution accomplished by quantum cryptography, we can get rid of the problem. Thus Quantum Cryptography is actually a procedure of key distribution, but not the message itself.
Quantum Cryptography enforces better security as it is not possible to tap single signal. Hence, an eavesdropper can't intercept and retransmit the system because in quantum mechanics any observation can't be thought of as a possessed value. Also, Due to Heisenberg Uncertainty principle, any external activity would introduce an irreversible change in quantum states before they are transmitted to the receiver. Thus, resulting in a high error rate and intended receiver to detect the eavesdropping. Thus, quantum Cryptography on one hand ensures reliability of the key material, on the other hand detects any attempt of eavesdropping [18].

In 1984, Bennet and Bussarat published first quantum Cryptography protocol, known as BB84[19]. In1991, Bennet et.al.[20] used polarized photons as a working prototype of BB84 protocol.In 1991, Ekerst[21] proposed the use of Einstein-Podol-Sky-Rosen entangled two state particles to implement a quantum cryptography protocol. In 1992, Bennet [21] proposed a quantum key distribution method, known as B92 could be implemented by employing

single photon interference with photon propagating for long distance over optical fiber. Afterwards, other protocols [22] were published and many groups [23] developed optical-fiber based prototype.

2. Evaluation Measures

2.1. Differential measures

To crack the key, attackers often make a slight change in the plain image and then the slightly changed image is encrypted using the same secret key. Afterwards relationship between the encrypted original and modified image is looked upon, thus for better efficiency an algorithm must be sensitive towards the slightest change which is a test using NPCR (Number of pixel change rate) and UACI (Unified average changing intensity).

1.1. 1. NPCR: Number of pixel change rate is percentage of different pixel numbers between two encrypted images, whose original images have one pixel difference only. Higher value ensures higher reliability against differential attacks. It is given by:

$$NPCR=\frac{1}{w*h}\sum_{\substack{1\le i\le w\\ 1\le j<h}} D(i,j)*100 \quad (1)$$

D(i,j)=0 when C1(i,j)=C2(i,j) and
D(i,j)=1 when C1(i,j)≠C2(i,j)

Where w and h denotes width and Height of the image respectively. D(i, j) denotes the difference between corresponding pixels of original encrypted image. Range of NPCR ϵ [0,100].

2.1.2.UACI: Unified Average Changing Intensity is a measure of average intensity between two encrypted images whose original images have one pixel difference only. It is given by :-

$$UACI=\left[\sum_{\substack{0\le i\le w\\ 0<j<h}}\frac{|C1(i,j)-C2(i,j)|}{255}\right]*\frac{100}{w*h} \quad (2)$$

2.2 STATISTICAL ANALYSIS:
To avoid statistical attacks the statistical analysis is performed. Histogram Analysis and Correlation Coefficient are used to test the strength of the algorithm against statistical attack.

2.2.1 Histogram Analysis (HA) : unfolds the distribution of pixel values of an image. The histogram of the plain image should be entirely different to that of the histogram of an encrypted one. The histograms of plain images are not uniform in nature, whereas of encrypted images should be uniform i.e. all the pixels should be uniformly distributed in space.

2.2.2 Correlation Coefficient (CC): It is a measure of similarity between corresponding pixels of an plain and encrypted image. The values of adjacent pixels of an original image are strongly correlated in three directions, i.e., horizontal, diagonal, and vertical. Reduction of this relationship in ciphered image ensures the capability of an algorithm agents statistical attacks. It is denoted by r and given by:

$$r_{xy}=\frac{c(x,y)}{\sqrt{D(x)*D(y)}} \quad (3)$$

Here,

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-\sum(x))^2 \quad (4)$$

$$D(y)=\frac{1}{N}\sum_{i=1}^{N}(y_i-\sum(y))^2 \quad (5)$$

$$c(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-\sum(x))(y_i-\sum(y)) \quad (6)$$

$$\sum(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (7)$$

Where c(x, y) denotes the covariance between the samples x and y i.e. the coordinates of an image. Also D (x) and D (y) denotes the standard deviation of x and y, respectively. K is the number of pixel pairs (xi, yi) and ∑(x) is the mean of xi pixel values.

Range of CC ϵ [−1,1].

2.2.3 Peak Signal to Noise Ratio (PSNR): PSNR a quality measure between the original and decrypted images. PSNR is given by :

$$PSNR = 10\log_{10}\left[\frac{I^2}{MSE}\right] \quad (8)$$

Unit of measuring PSNR are decibel (dB). The value of PSNR for a better algorithm this value should be maximum.

Range of PSNR ϵ [0,∞].

In this article a different quantum cryptography techniques are reviewed by systematic way. This article helps to find various issues with systematically choosing the researching databases, selecting research papers and deciding their selection or refusal criteria. This study will help to the scholars as well as experts in selecting suitable quantum technique for cryptography. This systematic literature review is divided into following sections:

- Methodology for literature review
- Results
- Conclusion and future scope

3. Methodology For Literature Review

The systematic literature study has been exploited to do this research. It is an appropriate and replication process to record significant points of awareness of the exact research range for reviewing and exploratory all current research recognized with research queries. Thus, this examination associates following phases like, identification of research queries, and selection and refusal conditions, and Data Search process.

3.1 Research Queries Identification

Research queries are formulated before starting the Systematic literature review and from the selected article's authors try to find the answers to research questions that are described in the table below in the result section

Research queries are as follows:

RQ-1: IS quantum cryptography is used for Encryption
RQ-2:Whether the technique used in the article is single or hybrid with another technique
RQ-3:Is the proposed technique evaluated by performance metrics
RQ-4: Year of Publication

3.2 Review Procedure Development

Our next step is to design a procedure for searching the appropriate articles. For review procedures, we have deliberated search process, selection and refusal criteria, and data extraction.

3.3 Search Process

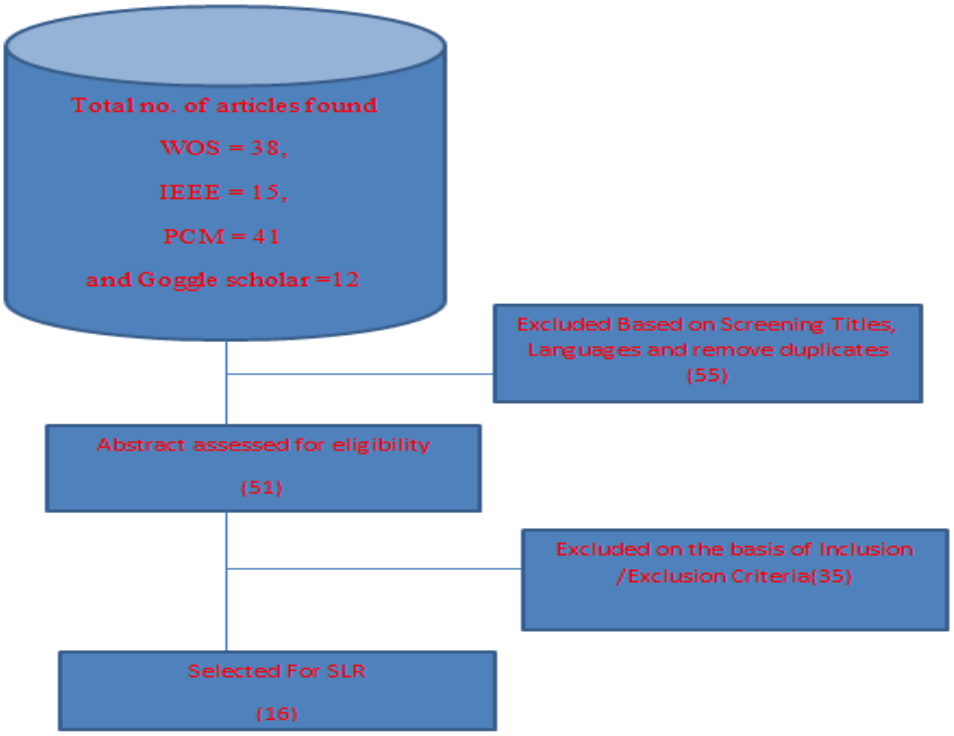

Figure1. Article search

Figure1. Shows that we have chosen four valid databases (i.e. WOS, IEEE, PCM and Goggle scholar) with a specific procedure to complete our search. These prominent databases have maximum result regarding our query and we have selected the article via the self-designed process as described below.

We have year-wise selected range from "2015–2020" for selection of research articles for this Review from selected databases. We have applied AND operator in between keywords related to our topic for searching the articles. In this way the search process is refined and non-relevant articles are uninvolved.

NO. of articles			
Library	Total Papers	Accepted	Rejected
WOS	38	5	33
IEEE	15	4	11
PCM	41	2	39
Goggle Scholar	12	5	7
Total	106	16	90

Table I Summary of database searched and accepted

3.4 Selection And Rejection Criteria

We describe the solid paradigm for the selecting and rejecting of the research articles for this SLR. Four parameters are considered to assure the correctness of the suitable responses to our research queries. The research articles will be selected on the principle of these factors as given below.

A. Selection

i. Year Wise Range 2015-2020

The Chosen research article must be dispersed from 2015 to 2020 by introducing the filter an off year-wise selection in each database that will result diminish overall results and supports in concluding the research article. All other articles are rejected that are not in the described range set in the year wise selection mechanism.

ii. Publisher

Selected research articles must be published in one of the popular scientific databases that are selected, i.e. Goggle scholar, WOS, IEEE, and PCM.

iii. Crucial-Effects

Chosen research articles must have vital, valuable results with respect to image encryption under quantum cryptography. Terminate the research articles if its algorithm does not have a great contribution for image encryption.

iv. Results-Oriented

Selected research articles must be results-oriented, not a survey, review, or case study. Have a short look at the simulation result section of the selected studies and verify that its influence worth in the field of image encryption. Result confirmation must be carried out by a dominant survey if it does not so terminate that article.

B. REJECTION

i. Repetition

All searches in an exact search setting can't be unified. Thus, terminate the research article if these are vague in the given search setting and just a single (published in journal) of them is chosen.

ii. Rejection on the Title Basis

Selected research article can be acceptable by having a look at the title of the research paper. The title has been terminated if it is not matched with the SLR topics.

iii. Rejection on Abstract Basis.

Occasionally it is very hard to take judgment while selecting the research study by checking the title only of the article so in this respect it is essential to study the abstract of the research article from which we can get correct information about the research article.

4. **Results Of The Systematic Review**

The outcome of the review is addressed in the form of answers to the research questions.

RQ-1: IS quantum cryptography is used for Encryption
RQ-2: Which quantum technique is used
RQ-3: Whether the technique used in the article is single or hybrid with another technique
RQ-4: Is the proposed technique evaluated by performance metrics
RQ-5: Year of Publication

Study No.	RQ1	RQ2	RQ3	RQ4
[1]	YES	CAQW Controlled Alternate Quantum Walks	Single	YES
[2]	YES	Spin Matries and their Entaglement	Hybrid	YES
[3]	YES	Quantum Rotation Operators	Single	YES
[4]	YES	NCQI	Hybrid	YES
[5]	YES	BB84, B92, EPR	Hybrid	YES
[6]	YES	State Qubit	Hybrid	YES
[7]	YES	Random Rotation Of Qubit and Quantum Fourier Transform	Single	YES
[8]	YES	QCNN	Hybrid	YES
[9]	YES	Quantum Chaotic Map	Hybrid	YES
[10]	YES	Cascaded Descrete Quantum Walks	Hybrid	YES
[11]	YES	Quantum Walks BASED Quantum Hash Funtion	Single	YES
[12]	YES	Quantum Gray code NCQI Model Based	Hybrid	YES
[13]	YES	Quantum Walks - NCQI Model Based	Single	YES
[14]	YES	CAQW Controlled Alternate Quantum Walks - NCQI Model Based	Single	YES
[15]	YES	QW S-walks	Single	YES
[16]	YES	Quantum walks	Single	YES

Table II list the Answer of RQ1,RQ3,RQ4 and RQ5

RQ5. The year of research article published

The Table IV below gives the quantity of research papers distributed on machine learning based effort estimation over the predetermined period. The appropriation of papers over years demonstrates that reliable efforts were made by researchers to improve the effort estimations utilizing new technologies and techniques. The significant distributing sources are Web of Science and IEEE advanced Xplore.

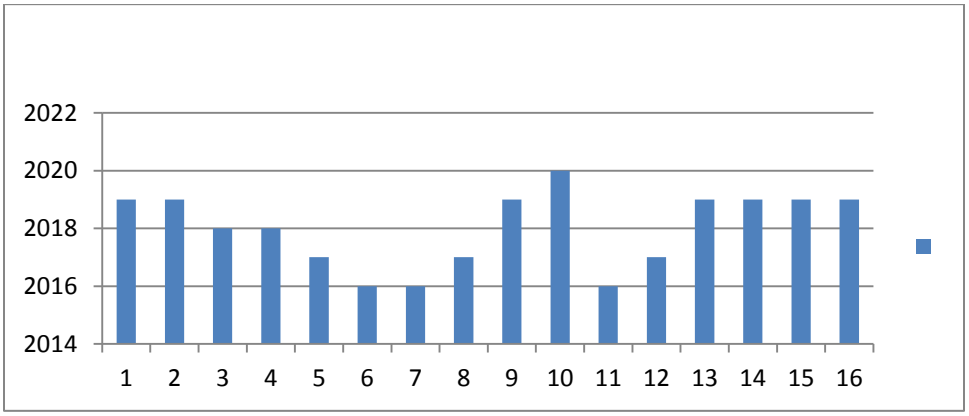

Table IV. Year of Publication

5. Performance Measures

The generally used performance measures are correlation analysis, histogram, key sensitivity and key space. In any case, numerous presentation measures can be utilized depending on the kind of attacks. They are Mean Square Error (MSE), Peak signal noise ratio (PSNR), Noise analysis, etc.

Reference	Corelation Analysis	PSNR	MSE	Histogram	Key Space Analysis	Entropy	UACI	NPCR	Noise Analysis	Key Sensitivity Analysis
[1]	√	-	-	√	√	Information	-	√	√	√
[2]	√	√	√	√	-	Shannon	√	√	-	-
[3]	√	√	√	√	-	Information	√	√	-	-
[4]	√	√	√	√	√	Information	-	-	√	√
[5]	√	-	-	-	-	-	√	√	-	√
[6]	√	-	-	√	-	-	-	-	-	-
[7]	√	√	-	√	√	-	-	-	√	√
[8]	√	-	√	√	√	-	-	-	√	√
[9]	√	√	√	√	√	Information	√	√	√	√
[10]	√	-	-	√	√	Information	-	√	-	√
[11]	√	-	-	√	√	Information	√	√	-	√
[12]	√	-	-	√	-	Shannon	√	√	-	√
[13]	√	-	-	√	√	Shannon	√	√	-	√
[14]	√	-	-	√	√	Shannon	-	-	-	√
[15]	-	√	-	-	-	-	-	-	-	-
[16]	-	√	-	-	-	-	-	-	-	-

6. Findings And Conclusions

The systematic literature review concludes that a significant amount of research was carried out in image encryption using quantum cryptography. The dispersion of research over the years is steady. The major image encryption approaches used are quantum walks, and NCQI Model. When the traditional algorithm of image encryption combined with quantum ideas it became very fast

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] A. Abd EL-Latif, B. Abd-El-Atty, E. M. Abou-Nassar, and S. E. Venegas-Andraca, "Controlled alternate quantum walks based privacy preserving healthcare images in Internet of Things," Opt. LASER Technol., vol. 124, Apr. 2020.

[2] H. M. Waseem and M. Khan, "A new approach to digital content privacy using quantum spin and finite-state machine," Appl. Phys. B-LASERS Opt., vol. 125, no. 2, Feb. 2019.

[3] M. Khan and H. M. Waseem, "A novel image encryption scheme based on quantum dynamical spinning and rotations," PLoS One, vol. 13, no. 11, Nov. 2018.

[4] Q. Ran, L. Wang, J. Ma, L. Tan, and S. Yu, "A quantum color image encryption scheme based on coupled hyper-chaotic Lorenz system with three impulse injections," QUANTUM Inf. Process., vol. 17, no. 8, Aug. 2018.

[5] B. Wang, J. Xu, and H. Song, "Research on the improved algorithm for image quantum encryption in multimedia networks," Comput. Electr. Eng., vol. 62, pp. 414–428, Aug. 2017.

[6] H. A. Elsayed, Y. K. Jadaan, and S. K. Guirguis, "Image security using quantum Rivest-Shamir-Adleman cryptosystem algorithm and digital watermarking," in 2016 Progress in Electromagnetic Research Symposium (PIERS), 2016, pp. 3978–3982.

[7] X. Liu, H. Xiao, P. Li, and Y. Zhao, "Design and Implementation of Color Image Encryption Based on Qubit Rotation About Axis," Chinese J. Electron., vol. 27, no. 4, pp. 799–807, 2018.

[8] J. Li, X. Di, X. Liu, and X. Chen, "Image encryption based on quantum-CNN hyperchaos system and Anamorphic Fractional Fourier Transform," in 2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI), 2017, pp. 1–6.

[9] J. Xu, P. Li, F. Yang, and H. Yan, "High Intensity Image Encryption Scheme Based on Quantum Logistic Chaotic Map and Complex Hyperchaotic System," IEEE Access, vol. 7, pp. 167904–167918, 2019.

[10] Ahmed A. Abd El-Latif, Bassem Abd-El-Atty, Mohamed Amin, Abdullah M. Iliyasu, "Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications," Sci Rep. 2020; 10: 1930. Published online, Feb, 2020.

[11] Yu-Guang Yang, Peng Xu, Rui Yang, Yi-Hua Zhou, Wei-Min Shi, "Quantum Hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption," Sci Rep. 2016; 6: 19788. Published online, Jan, 2016.

[12] El-Latif, A. A. A., Abd-El-Atty, B. & Talha, M. Robust encryption of quantum medical images. IEEE Access. 6, 1073–1081, 2017.

[13] Abd-El-Atty, B., EL-Latif, A. A. A. & Venegas-Andraca, S. E. An encryption protocol for NEQR images based on one-particle quantum walks on a circle. Quantum Inf. Process. 18, 272 (2019).

[14] EL-Latif, A. A. A., Abd-El-Atty, B. & Venegas-Andraca, S. E. Controlled alternate quantum walk-based pseudo-random number generator and its application to quantum color image encryption. Physica A: Statistical Mechanics and its Applications, 2019.

[15] EL-Latif, A. A. A., Abd-El-Atty, B. & Venegas-Andraca, S. E. A novel image steganography technique based on quantum substitution boxes. Opt. Laser Technol. 116, 92–102, 2019.

[16] El-Latif, A. A. A. et al. Secret images transfer in cloud system based on investigating quantum walks in steganography approaches. Physica A: Statistical Mechanics and its Applications 123687,2019.

[17] Goyal A, Aggarwal S, Jain A. Quantum Cryptography & its Comparison with Classical Cryptography: A Review Paper. In5th IEEE International Conference on Advanced Computing & Communication Technologies [ICACCT-2011] 2011.

[18] Hughes, R. J., Alde, D. M., Dyer, P., Luther, G. G., Morgan, G. L., & Schauer, M. (1995). Quantum cryptography. Contemporary Physics, 36(3), 149–163.

[19] D. Mayers and A. Yao, "Quantum cryptography with imperfect apparatus," Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280), Palo Alto, CA, USA, 1998, pp. 503-509.

[20] Bennett, C.H., Bessette, F., Brassard, G. et al. Experimental quantum cryptography. J. Cryptology 5, 3–28 ,1992

[21] C. H. Bennett, G. Brassard and A. K. Ekert, "Quantum Cryptography," Scientific American, Vol. 267, No. 4, 1992, pp. 50-57.

[22] S.M. Barnett and S. J. D. Phoenix , "Philosophical Transactions: Mathematical, Physical and Engineering Sciences ," Nonlinear Optics for Information Processing and Communication,Vol. 354, No. 1708, pp. 793-803.

[23] J. Breguet, A. Muller & N. Gisin, "Quantum Cryptography with Polarized Photons in Optical Fibres", Journal of Modern Optics, 41:12, 2405-2412, 1994