Review of Intelligent Video Surveillance: System Concept

Kashmira Mhatre, Ameya Mandhare, Jyoti Kachare, Rohini Kokate.
kashmiramhatre1493@gmail.com, ameya.mandhare16@gmail.com, kacharejyoti88@gmail.com, rohinikokate11@gmail.com.
ELECTRONICS AND TELECOMMUNICATION DEPARTMENT, MAHATMA GANDHI MISSION'S COLLEGE OF ENGINEERING AND TECHNOLOGY, KAMOTHE.

Abstract— This paper highlights- the various distributed platforms that can be used in a Video Surveillance System and their influence on the performance of the Real-Time Video Service in comparison to other existing solutions. Video surveillance finds its uses in almost every aspect of daily routine of human life: both private and public. With its growing applications, its quality, scope and ease of use are the factors which continuously need upgradation. An interesting part of Intelligent Video Surveillance technology is that it can recognize object and identify human faces or track it also it helps in behaviour patterns. One of the key aspects in the development of Video Surveillance system is the use of quantum cryptography communication technology which takes the help of light source such as entangled photon pairs. The information is carried through photon pair used to keep the transmission of video information confidential which is passed through an optical fibre medium. Unprocessed video information contains a lot of redundant data. It was found that, H.264 video compression algorithm could eliminate redundant information of spatial-time and visual data which gives an advantage of no redundant data in the video information. An Intelligent Video Surveillance System based on quantum cryptographic communication technology is discussed, which not only improves the data transmission rate but also enhances data confidentiality. Remote monitoring is an area which is in need of such technologies but without the baggage of cables. Therefore, we intend to achieve this goal by integrating wireless communication technology with our surveillance system.

Index Terms— Data Security, Quantum cryptography, Real-Time Video, S3C6410 processor, Video surveillance, x264 coding arithmetic, Wireless communication.

1 INTRODUCTION

DEVELOPMENT of smart city construction, video surveillance systems are widely used, personal videos constantly being leaked has become a serious problem in today's society, the traditional information encryption method is easy to be cracked. Video communication security is concerned [3].

Quantum communication is a new communication technology with security. In addition, unprocessed video data contains a lot of redundant data, this is undoubtedly easy to acquire and to process safety video, which had a serious impediment. It was found that, X264 video compression algorithm could eliminate redundant information of spatial-time and visual data.
The quantum coding technology was used in the process of emission, transmission and receiving of video information. We are working on a video monitoring system based on single photon quantum communication technology [3].

X264 provides a command line interface as well as an API (In computer programming, an application programming interface (API) is a set of subroutine definitions, protocols, and tools for building software and applications. A good API makes it easier to develop a program by providing all the building blocks, which are then put together by the programmer).X264 implements a large number of features compared to other H.264 encoders. X264 contains some psych visual enhancements which aim to increase the subjective video quality of the encoded video [3].

2 BLOCK DIAGRAM

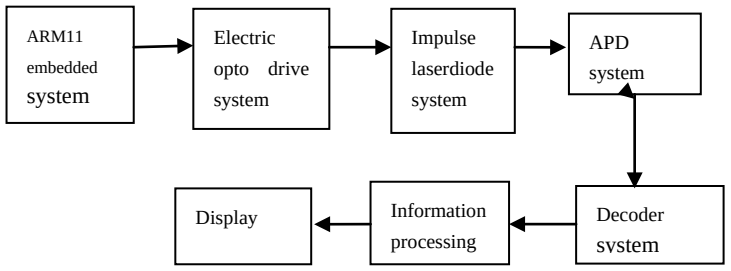

Fig 1. The quantum-based video monitor sytem schematic diagram.

The world wherein we live, there is constantly some thing or the other going on, say crimes, terrorist attacks, bank robbery, murder, petty thievery etc. Hence video monitoring for the world has become a necessity. Everything needs to be monitored and along with monitoring it is important to know that what is being monitored is not being seen by a third person. Thus encryption is a must while transmitting our data. Along with this increase in speed of communication with advancement in current methods is required [1].

Paper Objectives:

The most important objective of this paper is remote monitoring of an area or region.
Along with that we intend to secure the video data using quantum cryptography to avoid data breach.
Most importantly we will be making the transmission process faster using an optical network.

The system eventually achieve the stability and good image quality, higher inter frame compression and video acquisition system. This implements the confidentiality in the process of video information communication, and there is no data loss. The system is reasonable, stable and reliable. The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical communication [3].

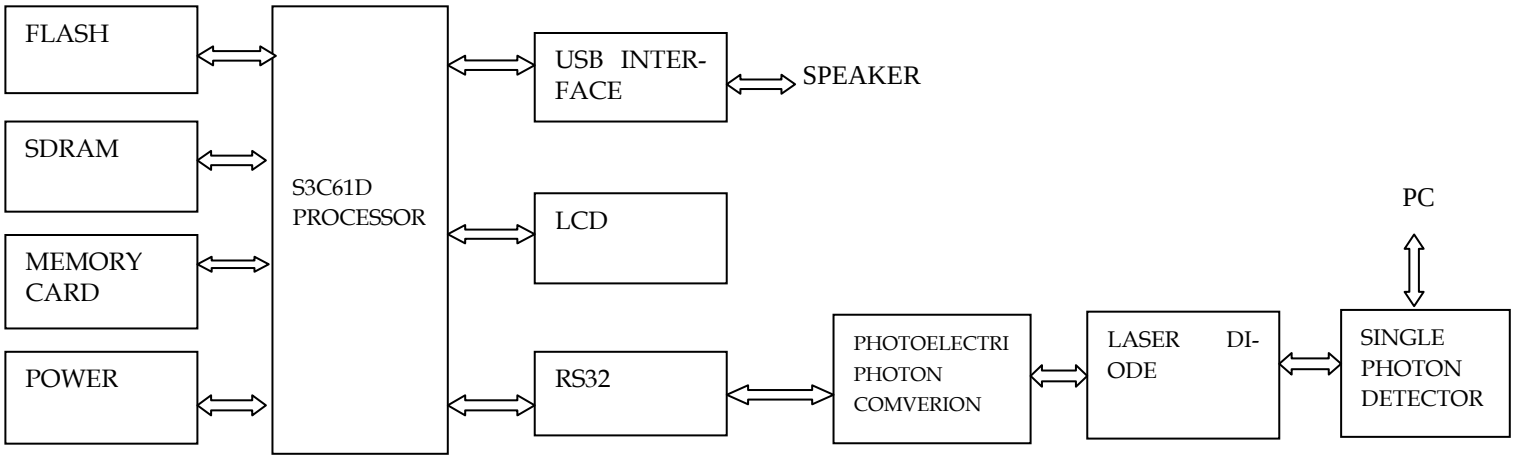

Fig 2. Hardware structure of the designed system.

2.1 WORKING

The information through ARM board was emitted out with a laser diode drivers attenuated, which generates approximate single photon pulse. The video information, was transferred by quantum state coded. Any measurement for quantum carrier or copy behavior will change the original quantum state according to the uncertainty principle of quantum mechanics. The data was detected by APD and recorded by a counter and, received by PC. Finally the macro block coding mode selection algorithm was put forward for fast frame rate distortion optimization, which could markedly improve the coding efficiency. ARM processor drives the embedded C system as the video acquisition and processing terminal, USB interface of the camera was used for video data acquisition, the video information of emission, transmission and reception was fulfilled by the laser diode and single photon detector. PC was responsible for the video acquisition system debugging and optimization of compression algorithm Embedded system collects video information through the camera, this collection of video data is quantum source. Information processed by the photoelectric transfer module, pulsed diode laser system avalanche photodiode system then transforming the message into quantum bit, the quantum states as carriers of messages transmit quantum information. At the receiver, quantum decoder converts quantum information bits into the general bit message, and then the processed information in video format for playback.
The quantum communication technology based on entangled light source. The carrier of information is photon pairs entangled, in which the entangled photon pairs were used to keep transmission of video information confidential [3], [4].

3 QUANTUM CRYPTOGRAPHY

Quantum cryptography is NOT a new algorithm to encrypt and Decrypt data. Rather it is a technique of using photons to generate a cryptographic key and transmit it to a receiver using a suitable communication channel. A cryptographic key plays the most important role in cryptography; it is used to encrypt/decrypt data. Quantum Cryptography uses the Quantum Computation Effects to perform Cryptographic tasks and to break into Cryptographic Systems. The word quantum itself refers to the most fundamental behavior of the smallest particles of matter and energy: quantum theory explains everything that exists and nothing can be in violation of it [3].
Essentially, quantum cryptography is based on the usage of individual particles/waves of light (photon). It is also based on their intrinsic quantum properties to develop an unbreakable cryptosystem. It is so because it is impossible to measure the quantum state of any system without disturbing that system. It is theoretically possible that other particles could be used, but photons offer all the necessary qualities needed, their behavior is comparatively well-understood, and they are the information carriers in optical fiber cables, the most promising medium for extremely high-bandwidth communications [3].
The idea behind quantum cryptography is that two people communicating using a quantum channel can be absolutely sure no one is eavesdropping. Heisenberg's uncertainty principle requires anyone measuring a quantum system to disturb it, and that disturbance alerts legitimate users as to the eavesdropper's presence. No disturbance, no eavesdropper. In simple word quantum cryptography is completely secure [3].
Quantum cryptography uses photons to transmit a key. Once the key is transmitted, coding and encoding using the normal secret-key method can take place. But how does a photon become a

key? How do you attach information to a photon's spin?
This is where binary code comes into play. Each type of a photon's spin represents one piece of information — usually a 1 or a 0, for binary code. This code uses strings of 1s and 0s to create a coherent message. For example, 11100100110 could correspond with h-e-l-l-o. So a binary code can be assigned to each photon — for example, a photon that has a vertical spin (|) can be assigned a 1. Alice can send her photons through randomly chosen filters and record the polarization of each photon. She will then know what photon polarizations Bob should receive.
When Alice sends Bob her photons using an LED, she'll randomly polarize them through either the X or the + filters, so that each polarized photon has one of four possible states: (|), (–), (/) or ( ). As Bob receives these photons, he decides whether to measure each with either his + or X filter he can't use both filters together. Keep in mind, Bob has no idea what filter to use for each photon, he's guessing for each one. After the entire transmission, Bob and Alice have a non-encrypted discussion about the transmission. Quantum key distribution (QKD) uses quantum mechanics to guarantee secure communication. It enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages.

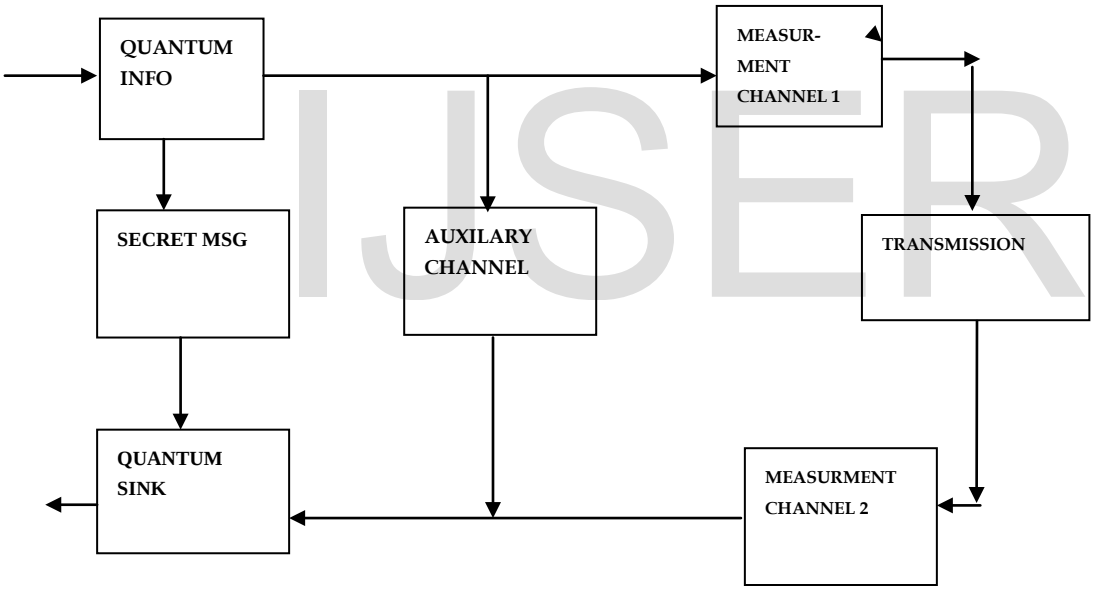

Fig 3. Quantum key video surveillance communication system diagram.

Quantum Key Distribution (QKD) is a technology, based on the quantum laws of physics, rather than the assumed computational complexity of mathematical problems, to generate and distribute provably secure cipher keys over unsecured channels. It does this using single photon technology and can detect potential eavesdropping via the quantum bit error rates of the quantum channel. Sending randomly encoded information on single photons produces a shared secret that is a random string and the probabilistic nature of measuring the photon state provides the basis of its security [5].
Quantum key distribution is only used to produce and distribute a key, not to transmit any message data. This key can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel. The algorithm most commonly associated with QKD is the one-time pad, as it is provably secure when used with a secret, random key [7].

Why do we need quantum cryptography?
Every new solution is made because of some problem we have with the current solution. The case is no different with this one. Let us see the problem first [8].
The problem with symmetric cryptography is that the same key is used to both encrypt and decrypt the messages. If for some reason that key is leaked to some third party, then it can be used to decrypt communication between two trusted devices or persons. In the worst case, the communication can be intercepted and altered. Today's huge computing power (these days even Xbox and PlayStation at homes have huge power) can be used to crack a key used in symmetric cryptography. Another major problem with this type of cryptography is how to decide which key to use and how to share between trusted devices or persons. Imagine a key has to be shared between India and America, then that communication too has to be secured before sharing the key [8]

Coming to the problem of asymmetric cryptography, it is not something we are facing right now, but seeing the pace of changing technology, we will be facing it soon. Most of the keys used in public key cryptography are at least 128-bit keys which are considered to be very strong. An attacker can easily get hold of the public key because it is shared by the user. But to generate a private key for that public key involves huge amounts of calculations with permutations and combinations. At present a supercomputer is what you need to crack a PKC and many years to complete it. But it will become pretty much possible with the use of quantum computers which use quantum physics to operate and have very high efficiency and computation speed. A quantum computer is a theoretical concept right now and will utilize atoms and molecules to perform computing at a very high speed [8].

4 FLOWCHART

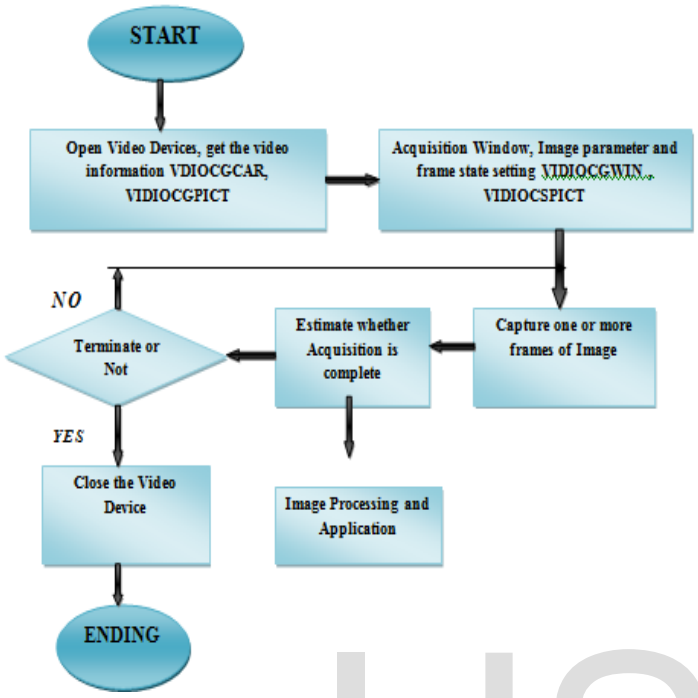

Fig 4. Process of video capture.

5 REVIEW

Cryptography happens to be one of the oldest data hiding techniques, it is a technique in which we encipher the data and use a decrypting key to decipher the enciphered data on the receiver end. Both symmetric as well as asymmetric cryptography have loop holes present. RSA algorithm is one of most commonly used algorithms, it is an asymmetric cryptographic algorithm wherein two different keys are used, one for encrypting and the other for decrypting. Various symmetric and asymmetric algorithms are used in cryptography of which most of them are prone to various attacks such as masquerade attack, man in the middle attack, brute force attack etc. we have observed in various cases during our research that with advancement in techniques of algorithms there is similar amount of improvement in intensity of attacks to data security.

5.1 FINAL REVIEW

Quantum cryptography refers to the technique in which the principle element is a photon. A photon is used in the process to key transmission. A photon essentially supports 4 spins, vertical, horizontal, diagonal left and right. Binary data can be associated to each spin and can be used as a key if represented in form of binary data, in this case even if there is a breach the actual key cannot be intercepted thus the communication stays secure. Although quantum communication is a complicated and difficult technology but has a good future scope in data security. Another aspect we came across was efficient image compression, for which we intend to use H.264 compression algorithm in our unique design concept of the video capture system, the latest H.264 video compression algorithm transplanted into S3C6410 provides certain value to the existing design and development of video monitoring system. Moreover rate-distortion optimization is an important technology. It aims to minimize the distortion in the process of video transmission with the constraints of the target data rate, which needs to use the rate distortion problem in the information theory that keeping the distortion to a minimum when limiting the bit rate no more than the channel transmission rate.

6 ACKNOWLEDGMENTS

It is our privilege to express our sincerest regards to our project guide Prof. Swati Kulkarni who gave us the golden opportunity to do this wonderful project on the topic “Review of Intelligent Video Surveillance: System Concept.” for Commercial And Public Sector Applications and Prof. Swati Kulkarni, for hervaluable inputs, guidance, encouragement, whole-hearted cooperation and criticism throughput the duration of our project.
We also immensely thank our parents and all other family members for their constant encouragement throughout our project.

7 CONCLUSION

Privacy and data security is right now of utmost importance to people. With quantum cryptography, secure transmission of data is possible, and chances of it being intercepted and altered are very low. This technology has been implemented in some areas. But is still under deeper research before being widely implemented.

REFERENCES

[1] G.Brassard, F.Bussières, N.Godbout and S.Lacroix, “Multiuser quantum key distribution using wavelength division multiplexing,” in Proceedings of SPIE 5260:Applications of Photonic Technology 6, Page(s):149–153 (2003).
[2] Chenchou Huang, HsuFeng Hsiao, “Perceptual rate distortion optimization for block mode selection in hybrid video coding,” in IEEE Conference Publications, Page(s):489-492 (2013).
[3] K. Sato, B.L. Evans, and J.K. Aggarwal, “Designing an Embedded Video Processing Camera Using a 16-bit Microprocessor for Surveillance System,” in Intemational Workshop on Digital and Computational video, Clearwater, FL, Page(s):151-158, November (2002).
[4] Petri Mahonen, “Wireless Video Surveillance: System Concepts,” in Proc. Int. Conf. on Image Analysis and Processing, Page(s):1090-1095, Sep. (1999).
[5] Damian Grzechca, Tomasz Wróbel, Patryk Bielecki. “Indoor location and idetification of objects with video survillance system and WiFi module” in Faculty of Automatic Control, Electronics and Computer Science Silesian University of Technolgy Gliwice, Poland, Page(s):171–174 (2014).
[6] Ce Zhu, Bing Xiong, “Transform-Exempted Calculation of Sum of Absolute Hadamard Transformed Differences” in ieee transactions on circuits and systems for video technology, vol. 19, no. 8, page(s):1183–1188 august (2009).
[7] Francesco Ziliani and Andrea Cavallaro, “Image Analysis for Video Surveillance Based on Spatial Regularization of a statistical Model-Based Change Detection,” in Signal Processing Laboratory, Swiss Federal Institute of Technology, Real-Time Imaging 7, Page(s): 389-399 (2001).

[8] Fernando M. S. Ramos and Filipe M. PatroAcio, "Application of Distributed Platforms in a Video Surveillance System," in University of Aveiro, Dept. of Communication and Art, Page(s): 447-455 (2001).

[9] HU Jianmiao and CEN Jianmei, "Video surveillance in public space in China," Page(s): 474–488 (2009).

[10] Cornelius Held, Julia krumm, petra Markel, and Ralf p. Schenke, "Intelligent Video Surveillance" by the IEEE computer society, Page(s): 83-84, March (2012).