International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Securing Data Transmission in Content Delivery Networks with Visual and Quantum Cryptography

[1]Sadaf Faraz Aleem Sahil, [2]Swati Patil

[#]M.Tech, Department of Computer Science & Engineering, Wainganga College of Engineering & Management, Nagpur, Maharashtra, India

[*]Assistant Professor, Department of Computer Science & Engineering, Wainganga College of Engineering & Management, Nagpur, Maharashtra, India

ABSTRACT

The secure transmission in the genuine worldwide condition is the essential necessity for a web or system client. Quantum cryptography is a situation and the application particular cryptography technique that uses the material science law for key generation. The cryptography technique separates the vitality highlights to apply information encoding and insert the key generation calculation with cryptography process. On the collector side, the key translating is utilized quantum technique and this separated key is then utilized for information disentangling. There are distinctive strategies for key generation which are investigated in this paper. The paper additionally investigated the extent of quantum key convention for key generation and encoding.

Keywords : Quantum Cryptography, Encoding, Decoding, Secure Transmission, Secure Communication, Content Based Routing.

I. INTRODUCTION

The cryptography is going to encode the data with the goal that the entrance and correspondence level security will be accomplished. Cryptography technique additionally guarantees the verified correspondence. The key particular cryptography spares the data to the verified people hand so the data transmission in the private and open condition can be more secure. As the security is the essential prerequisite when data go in open condition, on account of this part of work is done in cryptography technique to enhance the security, unwavering quality, heartiness and viability of cryptography strategies. The entire cryptography process is isolated in three fundamental stages. In first stage, the cryptography keys are produced. These keys are created by sender side. There can be single key for both encryption and decoding or there can be distinctive key for each procedure. Once the key is produced, the following work is to share the key on collector side. Distinctive sharing techniques are characterized for key conveyance. The key dissemination is either controlled by sender, incorporated control or the outsider. In the wake of conveying the key, the last stage is to utilize the key-cryptography strategy for secure correspondence. On sender side, the key construct encoding is performed and with respect to recipient side, the key based deciphering is performing. The essential encoding and deciphering process is appeared in figure 1.

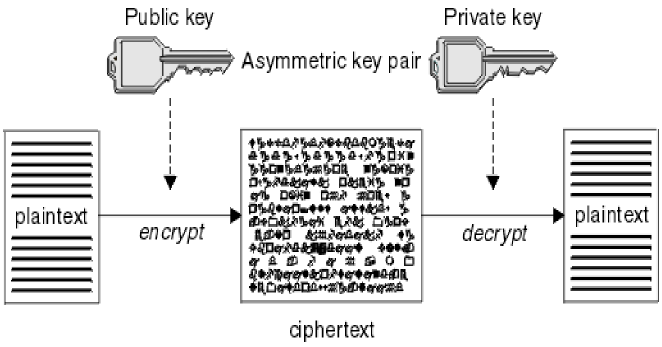


Figure 1: Key Based Encoding

Diverse cryptography and strategy level arrangements are given by various analysts. A standout amongst the best cryptography strategies is a quantum cryptography technique. The depiction of this cryptographic strategy is portrayed in this segment.

II. RELATED WORK

A) Cryptography

The word cryptography is taken from two Greek words which signify "mystery composing". Cryptography is the way toward scrambling the first content by adjusting and substituting the first content, masterminding it in an apparently unintelligible arrangement for others. Cryptography is a successful approach to secure the data that is transmitting through the system correspondence ways. Cryptology is the science that arrangements about cryptography and cryptanalysis. Cryptography is the methodology of sending the messages subtly and safely to the goal. Cryptanalysis is the technique for getting the installed messages into unique writings. By and large, cryptography is exchanging information from source to goal by modifying it through a mystery code. The cryptosystems utilizes a plaintext as information and create a figure content utilizing encryption calculation taking mystery key as information.

B) Quantum Cryptography

This cryptographic strategy utilizes the material science law or the quantum system to give secure correspondence. It is the secure imparted specialized strategy to irregular encoding plan for applying the key particular encryption and decoding. The portrayal of this technique should be possible under various parameters in light of nature and the application. The key cryptography strategy utilizes the quantum transmission to give the secure correspondence against the interlopers. This cryptography strategy utilizes the quantum or the photon polarization technique to enhance the secure correspondence. The cryptosystem utilizes the light photon arranged spellbound technique to set the cryptographic headings. The strategy guarantees the verification technique with main correspondence arrangement. The procedure connected by quantum cryptography technique against busybody is appeared in figure 2. The figure demonstrates that the encryption framework is coordinated with quantum arrange generator on sender side on plain content to apply information encoding. The quantum channel based correspondence is performed utilizing quantum cryptography technique. On beneficiary side, the encoded information is connected under quantum state finder to remove the concealed key. In light of this key, the decoding calculation is connected to separate the substance back. The work show can give the secure encoded correspondence in genuine condition.

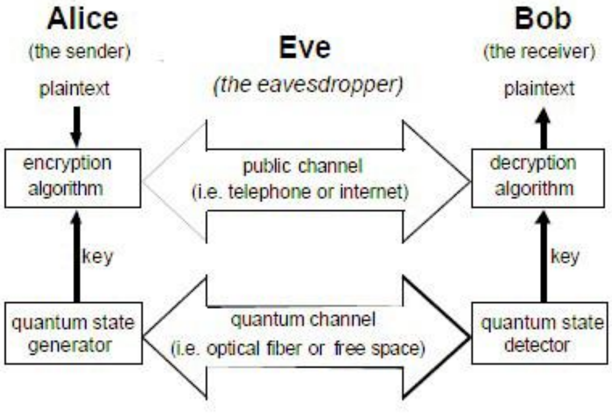


Figure 2 : Quantum Cryptography

In this paper, an investigation to the quantum cryptography techniques is characterized. The paper has recognized the extent of quantum cryptography and investigated distinctive key generation and sharing strategies. In this area, the prerequisite of cryptography strategy for secure correspondence is characterized. The area additionally distinguished the extent of quantum cryptography. In segment II, the work characterized by before analysts is talked about. In area III, the secure key generation techniques are investigated under quantum strategies. In segment IV, the finish of the work is characterized.

C) Steganography

Steganography is the act of hiding a record, message, picture, or video inside another document, message, picture, or video. The word steganography joins the Greek words steganos (στεγανός), signifying "secured, disguised, or ensured", and graphein (γράφειν) signifying "composing".

The initially recorded utilization of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, camouflaged as a book on enchantment. By and large, the shrouded messages have all the earmarks of being (or are a piece of) something else: pictures, articles, shopping records, or some other cover content. For instance, the concealed message might be in imperceptible ink between the noticeable lines of a private letter. A few executions of steganography that do not have a common mystery are types of security through lack of clarity, while key-subordinate steganographic plans stick to Kerckhoffs' principle.

The benefit of steganography over cryptography alone is that the planned mystery message does not draw in thoughtfulness regarding itself as a protest of examination. Obviously noticeable encoded messages—regardless of how unbreakable—excite intrigue, and may in themselves be implicating in nations where encryption is illegal. Thus, while cryptography is the act of securing the substance of a message alone, steganography is worried with hiding the way that a mystery message is being sent, and in addition hiding the substance of the message.

Steganography incorporates the disguise of data inside PC records. In computerized steganography, electronic interchanges may incorporate steganographic coding within a vehicle layer, for example, a record document, picture record, program or convention. Media documents are perfect for steganographic transmission on account of their huge size. For instance, a sender may begin with a harmless picture record and conform the shade of each 100th pixel to compare to a letter in the letter set, a change so unpretentious that somebody not particularly searching for it is probably not going to notice it.

D) Least Significant Bits Technique for Steganography[4]

Today, when converting an analog image to digital format, we usually choose between three different ways of representing colors:

- 24-bit color: every pixel can have one in 2^24 colors, and these are represented as different quantities of three basic colors: red (R), green (G), blue (B), given by 8 bits (256 values) each.
- 8-bit color: every pixel can have one in 256 (2^8) colors, chosen from a palette, or a table of colors.
- 8-bit gray-scale: every pixel can have one in 256 (2^8) shades of gray.

LSB insertion modifies the LSBs of each color in 24-bit images, or the LSBs of the 8-bit value for 8-bit images.

Example:
The letter 'A' has an ASCII code of 65(decimal), which are 1000001 in binary.
It will need three consecutive pixels for a 24-bit image to store an 'A':
Let's say that the pixels before the insertion are:

10000000.10100100.10110101,
10110101.11110011.10110111,
11100111.10110011.00110011

Then their values after the insertion of an 'A' will be:

1000000**1**.1010010**0**.1011010**0**,
1011010**0**.1111001**0**.1011011**0**,
1110011**0**.1011001**1**.00110011

(The values in **bold** are the ones that were modified by the transformation)
The same example for an 8-bit image would have needed 8 pixels:

10000000, 10100100, 10110101, 10110101, 11110011,
10110111, 11100111, 10110011

Then their values after the insertion of an 'A' would have been:

1000000**1**, 1010010**0**, 1011010**0**, 1011010**0**,
1111001**0**, 1011011**0**, 1110011**0**, 1011001**1**

Taking after the Boneh-Franklin plot, clusters of other character based encryption has been proposed. Some endeavor to improve the level of security; others endeavor to alter remarkable sorts of open key cryptosystems (e.g. different leveled plans, feathery arrangements, et cetera.) to the setting of identity based encryption. In this portion we give a short audit of some essential systems that have been made.

III. EXISTING WORK

Security is most basic angle to share the data in the worldwide condition. To give the secure and verified data, there is the prerequisite of some key particular encoding approach. Cryptography gives distinctive encoding strategies in view of the necessity. There are various existing cryptography that gives confirmation under open key, private key or shared key strategies. A ton of work characterized by various specialists on various key generation, key sharing and key based encoding. Quantum cryptography is one such cryptography frame that uses the procedure level and vitality level parameters.

Vignesh et. al. (Vignesh et. al., 2009) has given a similar investigation on customary and quantum cryptography strategies. Creator recognized the different qualities with respect to adaptability vectors for key sharing and encoding strategies. Creator characterized a limited quantum key dispersion technique for secure correspondence in the system.

Sharbaf et. al. (Sharbaf et. al., 2009) has exhibited an examination construct work with respect to quantum key cryptography. Creator characterized a hypothesis based demonstrating to control organize security and gave this present reality upgrade to the quantum cryptography show.

Creator gave a noteworthy change to quantum cryptography convention for secure correspondence in the system. (Kartalopoulos et. al., 2005) gave a work on related polarization display for canny correspondence utilizing Quantum cryptography strategies. Creator gave an investigation on cryptography strategies and recognized the key generation and distinguishing proof strategy. Creator connected work on fiber optic transmission for topological change.

Creator likewise recognized the specialized issues in respect to the specialized strategy and characterized the key conveyance technique for quantum control in unique strategy. Creator connected the fiber medium based correspondence demonstrating for secure correspondence continuously condition.

Creator (Kurochkin et. al., 2009) gave an impermanent stage construct working in light of quantum cryptography strategies. Creator characterized the work to apply the arrangement under polarization strategy and produced the powerful correspondence line for viable correspondence control progressively technique. (Sharbaf et. al., 2011) has recognized the shortcomings, difficulties of cryptography techniques for quantum parameters. The application driven ramifications of quantum cryptography was connected for various application and enhanced the quality and transmission utilizing quantum key trade techniques. Creator gave the potential change to the significant commitment to secure correspondence in genuine condition.

Creator (Goel et. al., 2007) has concentrated his work on investigation of quantum cryptography and recognized the material science law that can be consolidated to enhance the security. Creator additionally recognized the potential plausibility of the security technique to enhance the secure correspondence instrument. Creator (Crepeau et. al., 1999) utilized the proof particular correspondence by watching the quantum conduct of various machines and produced the estimation to give secure correspondence. Creator gave the run based development to cover the troublesome calculation with figuring technique and accomplish top of the line security.

Creator (Mandal et. al., 2013) executed the cryptography model to give security against savage power assault. Creator planned a three phase convention for various photon based correspondence. Creator dissected the numerical answer for hypothetical prerequisite examination and produced a probabilistic guide for administrator particular transmission. Creator gave the secure unitary transmission utilizing energized correspondence through convention encoding.

Creator (Porzio et. al. 2014) distinguished the security issues in private correspondence. A telecom station based coordinated calculation is characterized to give protection improved correspondence. Creator recognized the many-sided quality measures and gave the computational correspondence in genuine condition. Creator distinguished the dubious relations for secure quantum correspondence with convention coordination.

Creator (Shrivastava et. al., 2012) utilized the secure correspondence framework with key sharing technique. Creator utilized somewhat controlled convention for string level correspondence and gave the likelihood driven distinguishing proof of any meddler in the system. Creator accomplished the secure correspondence with quantum key dissemination in private condition.

Creator (Teja et. al., 2007) has given the potential improvement to security framework in practical condition. Creator distinguished the quality and shortcomings of both customary and quantum cryptography technique. Creator connected the innovative improvement to the framework with novel coordinated upgrades. Creator connected the secure correspondence demonstrating in genuine condition and picks up the channel driven quantum correspondence.

Creator (Bencheikh et. al., 2001) has investigated the portrayal of quantum cryptography under various angles. The quantum mechanics, convention joining and key sharing techniques were investigated by the creator. Creator recognized diverse process variables to accomplish the parameter particular change. Creator accomplished the schematic change progressively condition to produce flag mode security.

Creator (Kurochkin et. al., 2010) gave the hypothetical and trial investigation of quantum convention to accomplish the secure correspondence. Creator gave the captivated encoding technique and its degree in assault driven condition. Creator gave the accelerate the correspondence procedure by recognizing the blunders. Creator produced the specialized strategy in genuine condition and picked up the secure correspondence measures.

Creator (Niemiec et. al., 2013) gave the administration of security viewpoint in quantum cryptography display. Creator gave the quantum correspondence observing and gave the security level improvement continuously condition. A string captivated strategy for controlling the correspondence conduct and its control was likewise portrayed by the creator.

IV. PROPOSED SYSTEM

With, quantum PCs, quantum cryptography additionally came into light and now is by all accounts promising in view of its one of a kind elements that make it free from listening stealthily or whatever other outsider interruption in the key circulation frameworks. This system proposes a procedure where we indicate how an old method, for example, steganography can guarantee when we join it with the exceptional key dispersion component of quantum cryptography with some other extra security highlights.

The proposed framework concentrates on instrument which consolidates an old method, for example, steganography with the one of a kind key appropriation component of quantum cryptography. Besides, some extra elements are additionally proposed to make a solid data stream channel between two cutting edge arranges principally with an emphasis on quick and productive QoS giving systems, for example, content conveyance systems.

The essential idea of quantum cryptography incorporated with two principle viewpoints. The primary angle is to produce the information bits utilizing captivated photons and second to apply the physic rules based quantum key generation to improve the secure specialized strategy. Creator characterized as the work to enhance the cryptographic demonstrating to determine the computational trouble and by giving the factorization to the secure specialized technique. The cryptography technique requires dealing with the secure correspondence with determination of tenets and the algorithmic model give information factorization. This factorization is connected at bit level that improves the specialized strategy as well as gives the secure key generation in genuine condition. The key generation strategy under cryptographic demonstrating is appeared in figure 3.

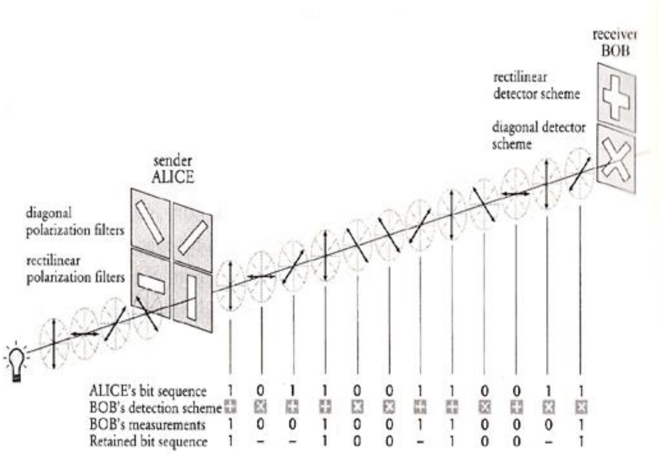
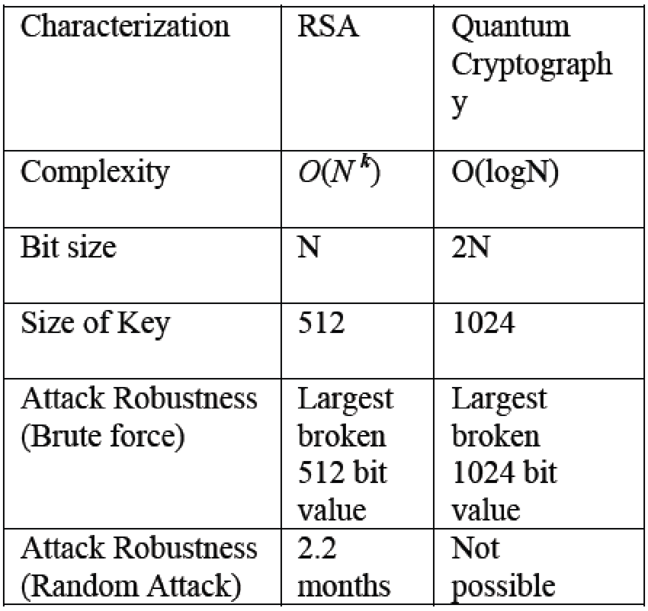

receiver
BOB
rectilinear detector scheme
diagonal detector scheme
sender
ALICE
diagonal polarization filters
rectilinear polarization filters
ALICE's bit sequence 1 0 1 1 0 0 1 1 0 0 1 1
BOB's detection scheme ⊞ ⊠ ⊞ ⊞ ⊠ ⊠ ⊞ ⊞ ⊠ ⊞ ⊠ ⊠
BOB's measurements 1 0 0 1 0 0 1 1 0 0 0 1
Retained bit sequence 1 – – 1 0 0 – 1 0 0 – 1

Figure 3 : Bit Polarized Quantum Cryptography Method

The figure is demonstrating the bit spellbound quantum key generation technique for enhancing the security angles and in addition gives the dispersion of the key utilizing quantum channel. The strategy joins the specialized technique in a coordinated frame so the secure correspondence will be acquired from the strategy itself. It is a stream based strategy in which the square size of information bits is characterized a progression of directional and condition particular operations are connected. These operations can be bearing particular to choose the filtration under related coordinated strategy. The quantum measures are connected on these information pieces to guarantee the secure extraordinary key generation.

V. RESULT ANALYSIS

The dynamic conduct and continuous incorporation demonstrate the quality of this cryptographic strategy over traditional cryptography approach. This approach can distinguish the secure calculation to improve the correspondence framework. It gives the quick and dependable correspondence to with low multifaceted nature based reconciliation. The correspondence under the multifaceted nature measure against customary cryptography technique is characterized in Table 1. The conventional cryptography techniques incorporate RSA strategy. The correlation is here inferred against various cryptographic technique properties.



Characterization	RSA	Quantum Cryptograph y
Complexity	$O(N^k)$	O(logN)
Bit size	N	2N
Size of Key	512	1024
Attack Robustness (Brute force)	Largest broken 512 bit value	Largest broken 1024 bit value
Attack Robustness (Random Attack)	2.2 months	Not possible

Table 1 : Comparative Analysis

The table has given the reasonable contrast between the RSA and the quantum cryptography strategies. The table demonstrates that quantum cryptography furnished the secure arrangement with low multifaceted nature and gave more secure encryption against various assaults.

VI. CONCLUSIONS

The Paper concentrates on instrument which joins an old procedure, for example, steganography with the remarkable key task fragment of quantum cryptography. Likewise, some extra parts are besides proposed to influence a solid data to stream channel between two bleeding edge sorts out for the most part with an emphasis on quick and gainful QoS giving structures, for example, content development systems. 1) It fulfills obvious capability for both figuring at PKG and private key size at customer; 2) User needs not to contact with PKG in the midst of key upgrade, as they say, PKG is allowed to be detached from the net in the wake of sending the foreswearing diagram to KU-CSP; 3) No secure channel or customer certification is required in the midst of key-revive among customer and KU-CSP. In this paper, an investigation to the quantum cryptography techniques is given. The quantum cryptography utilizes the material science low to give secure key generation and dispersion. The paper additionally characterized the near perception to demonstrate the quality of this cryptography strategy.

VII. REFERENCES

[1]. Porzio, "Quantum cryptography: Approaching communication security from a quantum perspective," Photonics Technologies, 2014 Fotonica AEIT Italian Conference on, Naples, 2014, pp. 1-4.

[2]. Shrivastava and M. Singh, "A security enhancement approach in quantum cryptography," Computers and Devices for Communication (CODEC), 2012 5th International Conference on, Kolkata, 2012, pp. 1-4.

[3]. Crepeau, "Cryptography in the quantum world," Information Theory and Networking Workshop, 1999, Metsovo, 1999, pp. 40.

[4]. K. Bencheikh, A. Jankovic, T. Symul and J. A. Levenson, "Quantum cryptography with continuous variables," Quantum Electronics and Laser Science Conference, 2001. QELS '01.

[5]. M. Niemiec and A. R. Pach, "Management of security in quantum cryptography," in IEEE

Communications Magazine, vol. 51, no. 8, pp. 36-41, August 2013.

[6]. M. S. Sharbaf, "Quantum Cryptography: A New Generation of Information Technology Security System," Information Technology: New Generations, 2009. ITNG '09. Sixth International Conference on, Las Vegas, NV, 2009, pp. 1644-1648.

[7]. M. S. Sharbaf, "Quantum cryptography: An emerging technology in network security," Technologies for Homeland Security (HST), 2011 IEEE International Conference on, Waltham, MA, 2011, pp. 13-19.

[8]. N. I. Mowla, I. Doh and K. Chae, "Securing information flow in content delivery networks with visual and quantum cryptography," 2016 International Conference on Information Networking (ICOIN), Kota Kinabalu, 2016, pp. 463-468.

[9]. R. Goel, M. Garuba and A. Girma, "Research Directions in Quantum Cryptography," Information Technology, 2007. ITNG '07. Fourth International Conference on, Las Vegas, NV, 2007, pp. 779-784.

[10]. R. S. Vignesh, S. Sudharssun and K. J. J. Kumar, "Limitations of Quantum & the Versatility of Classical Cryptography: A Comparative Study," Environmental and Computer Science, 2009. ICECS '09. Second International Conference on, Dubai, 2009, pp. 333-337.

[11]. S. Mandal et al., "Multi-photon implementation of three-stage quantum cryptography protocol," Information Networking (ICOIN), 2013 International Conference on, Bangkok, 2013, pp. 6-11.

[12]. S. V. Kartalopoulos, "Identifying vulnerabilities of quantum cryptography in secure optical data transport," Military Communications Conference, 2005. MILCOM 2005. IEEE, Atlantic City, NJ, 2005, pp. 2788-2796 Vol.

[13]. V. L. Kurochkin and I. G. Neizvestny, "Quantum cryptography," Micro/Nanotechnologies and Electron Devices, 2009. EDM 2009. International Conference and Seminar on, Novosibirsk, 2009, pp. 166-170.

[14]. V. Kurochkin and Y. Kurochkin, "Quantum cryptography security improvement with additional states," Micro/Nanotechnologies and Electron Devices (EDM), 2010 International Conference and Seminar on, Novosibirsk, 2010, pp. 231-233.

[15]. V. Teja, P. Banerjee, N. N. Sharma and R. K. Mittal, "Quantum cryptography: State-of-art, challenges and future perspectives," Nanotechnology, 2007. IEEE-NANO 2007. 7th IEEE Conference on, Hong Kong, 2007, pp. 1296-1301.

[16]. R. Canetti, S. Halevi, and J. Katz, “A forward-secure public-key encryption scheme,” in Advances in Cryptology (EUROCRYPT““03),E. Biham, Ed. Berlin, Germany: Springer, 2003, vol. 2656, pp. 646–646.

[17]. D. Boneh and X. Boyen, “Efficient selective-id secure identity-based encryption without random oracles,” in Advances in Cryptology (EUROCRYPT““04), C. Cachin and J. Camenisch, Eds. Berlin,Germany: Springer, 2004, vol. 3027, pp. 223–238.

[18]. D. Boneh and X. Boyen, “Secure identity based encryption without random oracles,” in Advances in Cryptology (CRYPTO““04),M. Franklin, Ed. Berlin, Germany: Springer, 2004, vol. 3152, pp. 197–206.

[19]. B. Waters, “Efficient identity-based encryption without random oracles,” in Advances in Cryptology (EUROCRYPT““05), R. Cramer, Ed. Berlin, Germany: Springer, 2005, vol. 3494, pp. 114–127.

[20]. C. Gentry, “Practical identity-based encryption without random oracles,” in Advances in Cryptology (EUROCRYPT““06), S. Vaudenay, Ed. Berlin, Germany: Springer, 2006, vol. 4004, pp. 445–464.

[21]. C. Gentry, C. Peikert, and V. Vaikuntanathan, “Trapdoors for hard lattices and new cryptographic constructions,” in Proc. 40th Annu. ACM Symp. Theory Comput. (STOC““08), 2008, pp. 197–206.

[22]. S. Agrawal, D. Boneh, and X. Boyen, “Efficient lattice (h)ibe in the standard model,” in Advances

in Cryptology (EUROCRYPT‟10), H. Gilbert, Ed. Berlin, Germany: Springer, 2010, vol. 6110, pp. 553–572.

[23]. D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, “Bonsai trees, or how to delegate a lattice basis,” in Advances in Cryptology (EUROCRYPT‟10), H. Gilbert, Ed. Berlin, Germany: Springer, 2010,vol. 6110, pp. 523–552

[24]. Y. Hanaoka, G. Hanaoka, J. Shikata, and H. Imai, “Identity-based hierarchical strongly key-insulated encryption and its application,” in Advances in Cryptology (ASIACRYPT‟05), B. Roy, Ed. Berlin, Germany: Springer, 2005, vol. 3788, pp. 495–514.

[25]. Moni Naor, Adi Shamir,” visual cryptography”

[26]. Jithesh K, 2dr. A V Senthil Kumar, “Multi-Layer Information Hiding -A Blend Of Steganography And Visual Cryptography,”

[27]. Young-Chang Hou, “Visual cryptography for color images,”