International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 08
July 2019

Bits to Color Image Spin Cryptography for Secure Data Transmission In Cloud Databases

Author 1: Mrs. Punya Jyothi Vemula is currently pursuing masters degree program in Computer Science and Engineering in Nova College of Engineering and Technology, JNTUK, Jangareddygudem, India, Mobile: +916303652779, Email: punyajyothivemula@gmail.com

Author 2: Mr. Suresh Chanamala is currently working as Associate Professor in Department of Computer Science and Engineering in Nova College of Engineering and Technology, JNTUK, Jangareddygudem, India.

ABSTRACT

Digital signatures enable the "authentication" and non-repudiation‖ of digital messages, assuring the recipient of a digital message of both the identity of the sender and the integrity of the message. As Attribute based encryption is better than Identity based encryption in terms of security I have selected ABE for Encryption. But in ABE third trusted party supplies keys. So to avoid third party ,I have selected quantum Mechanics for key generation and distribution to improve security in the cloud. The problem is that when cloud service providers provide service that time might be hacker hacked username and Password. For Prevent this problem we implement the concept of digital Signature. Our proposing scheme is based on generating the image from the text that we want to send securely and spinning the text based quantum QU bit approach as a base. This means no additional data is added to the initial text it is just a change in its format so that we can send it safely. This may be done using different image formats starting with grayscale images to 24 bits. The most important advantage in our proposed cryptographic technique is that it does not require an additional image to hide the text beneath it, besides it has a small size and very fast in comparison with other techniques.

KEYWORDS: Authentication, digital messages, encryption, digital signature, quantum qu bits, cryptographic techniques, spinning.

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 08
July 2019

INTRODUCTION

Now a day's all the application requires databases in a huge lot. Therefore maintaining servers is the biggest task all around, since it requires space, memory and cost-effective along with maintenance of hardware servers. Consequently, every database required users look at cloud storage units and accessing them with present applications by providing a secured data uploading process from the data owner and protecting from other data used by not obtaining the data even they download it.

With headway of computer group and far-reaching spread of system applications, clients, by and large, need various servers to give several administrations. In like manner, the multi-server engineering has been pervasive, and outlining a safe and proficient remote client verification under multi-server design turns into a nontrivial challenge. In a decade ago, remote client confirmation conventions have been advanced to relate to the multi-server situation necessities. Be that as it may, these plans experienced specific security issues or their cost utilization surpassed clients' obliged capacity. In this paper, we show an unknown remote client validation with a key understanding plan for multi-server design utilizing self-guaranteed open keys without pairings. The proposed plan can hold past plans' points of interest as well as accomplish client protection concern. Besides, our proposition can increase higher productivity by evacuating the pairings operation contrasted and the related plans. Through investigation and examination of the associated methods, we can state that our proposition is as per the situation prerequisites and plausible to the multi-server design.

This research presented a model of implementing of sharing of knowledge through a cloud, security over the data shared and even can't access by the admin of the cloud without the key. This allows personal protection for data owner to share the data for knowledge management.

Sharing of documents between a group of people, students or even in offices will lead us to radiate the knowledge. Radiation of expertise on a specific content or related work between the data owner and the consumer associated with our work using sharing of documents and posting of queries can add in the future contribution.

a) Security over data storing the data.

b) Knowledge sharing between people and groups.

c) Dual personal protection with the private key.

d) True encryption with the key.

Cloud Computing is an emerging technology nowadays. Due to the accessibility, availability, and cost effectiveness, cloud computing has became essential computing system in both, private and public sectors. However, secure data transfer is still a big question where transferring link between user and server are not stabilized yet. As a result, many cloud users lost their valuable data. However, this paper proposes as integrated service of Advanced Quantum Cryptography with Cloud Computing. To ensure the secure Cloud Environment between sender and receiver, Quantum Cryptography proposes the use of photons and physics to generate cryptographic keys.

LITERATURE REVIEW

The Advanced Encryption Standard (AES) has been lately accepted by NIST as the symmetric key standard for encryption and decryption of blocks of data. In encryption, the AES accepts a plaintext input, which is limited to 128 bits, and a key that can be specified to be 128 bits to generate the Cipher text. By exploring different granularities of data-level and task-level parallelism, we map 16 implementations of an Advanced Encryption Standard (AES) cipher with a FPGA Spartan 3. The proposed design has occupied less area and small delay.

Information-hiding techniques have recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent unauthorized copying directly. Military communications systems make increasing use of traffic security techniques which, rather than merely concealing the content of a message using encryption, seek to conceal its sender, its receiver, or its very existence. Similar techniques are used in some mobile phone systems and schemes proposed for digital elections. Criminals try to use whatever traffic security properties are provided intentionally or otherwise in the available communications systems, and police forces try to restrict their use. However, many of the techniques proposed in this young and rapidly evolving field can trace their history back to antiquity, and many of them are surprisingly easy to circumvent. In this article, we try to give an overview of the field, of what we know, what works, what does not, and what are the interesting topics for research.

Nowadays and because of unsecure networks and internet that can be accessed by anyone it became very risky to send important messages and files without any security measures. Before sending an important message we have to make sure that it will arrive to the destination in a secure way without being seen or modified by an intruder. Because of the threats mentioned before, steganography was discovered. Steganography in brief is the art of hiding information by other information. Usually we need to hide a text beneath any type of media. The

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 08
July 2019

most type of media used in hiding text is image. Steganography can be considered a new technology that still needs work and improvements. We are interesting in image steganography base type because it is s very good idea according to a security method to send an image that doesn‟tdraw any attention or suspicions about containing an important message. Another important reason for our choice was the use of this type of security by terrorists to hide their plans so everyone should read and be aware of such subjects. Steganography is one of the newest technologies in sending secure data between sender and receiver. After the large spread of cryptography a new concept was added in order to add a new security level that prevents the detection of hidden information under a cover of any digital media. Nowadays, the internet became a robust and enormous world that offers adiversity of facilities and needs, because of these different functionalities it became easier to find diversity of ways to send messages to people without anyone noticing or even knowing that the message exist. Steganography is the procedure in which one type of communication (text, sound or image beneath another type. Steganography is described by Neil F. Johnson and Sushil Jajodia in their paper „Steganalysis: The Investigation of Hidden Information‟ [1] as „The goal of Steganography is to avoid drawing suspicion to the transmission of a hidden message. If suspicion is raised, then this goal is defeated.‟ This technology is used widely nowadays, and a lot of people started hiding data, images video and audio by using it. For this reason even if a message seems normal and innocent it might be holding within it a secret message with high important data. The source of the word Steganography comes from the Greek word steganos which means covered or secret and the word graphy which means writing or drawing. So the whole meaning is secret writing [2].

METHODOLOGY

Our Generation method differs from other steganography methods in concept because it doesn't require an existing cover file. It is a technique that creates a cover file for the only one reason of hiding the sent message. The biggest advantage of this method is that no one can compare the sent image with another already existing image, using a generation approach the result is always an original file. This file of course has a huge strength against comparison tests. As we said generating technique doesn‟t depend on an already existing image file for this reason we will use the data file itself in order to create or generate a cover file. At the same time, the data that we‟ll send will be hidden in the cover.

We have used the text bits in order to create a new sequence of bits that represents different colors in addition to a common key that the sender and receiver agree on. This main concept of steganography can produce different types of images depending on the way we deal with bits. As a result of our research we will have two main new

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 08
July 2019

techniques of steganography. The first technique that will be explained is generating an image of 8 bit grayscale colors from the original text, while the second technique is generating an RGB image from the original text. This RGB image is a 24 bit image that is generated from the original text.

We will study the gray scale case only. Gary scale colors are degradation of 256 colors varying between white and black. Each 8 bits combined together represent a different color. After taking the original text that the sender needs to send privately to a specific destination, the sequence of text bits can be XORed with a secret key used for steganography goals. Of course the key size is most of the times different from the size of the text in this case the key will be repeated till its size reaches the size of the text. I this way we obtain a polyalphabetic cipher text. After XORing the bits of text with the resized key bits, a new sequence of bits will be generated. So the text bits themselves are now changed in to a new sequence of bits. After that the new bits will be dividedinto groups of 8 bits (one byte). The reason for this grouping is to have a set of bytes each byte representing one color out of the 256 grayscale colors (numbered 0 up to 255 or 00 till FF in hexadecimal). Now instead of having a sequence of bits representing letters of a text these bits after being xored with a repeated or resized secret key, they represent now different colors of grayscale.

Original text:

Thesis 01010100 01101000 01100101 01110011 01101001 01110011

Key of four letters only:

Sara:

01010011 01100001 01110011 11100001

We will XOR the original bits with the key. As we said the key must be resized, so we must repeat the key till the bits of the text are all xored. In our example the key sequence will be repeated 3 times:

T h e s i s
01010100 01101000 01100101 01110011 01101001 01110011

XOR

S a r a S a
01010011 01100001 01110011 11100001 01010011 01100001

00000111 00000100 00010111 00010010 00111010 00010010

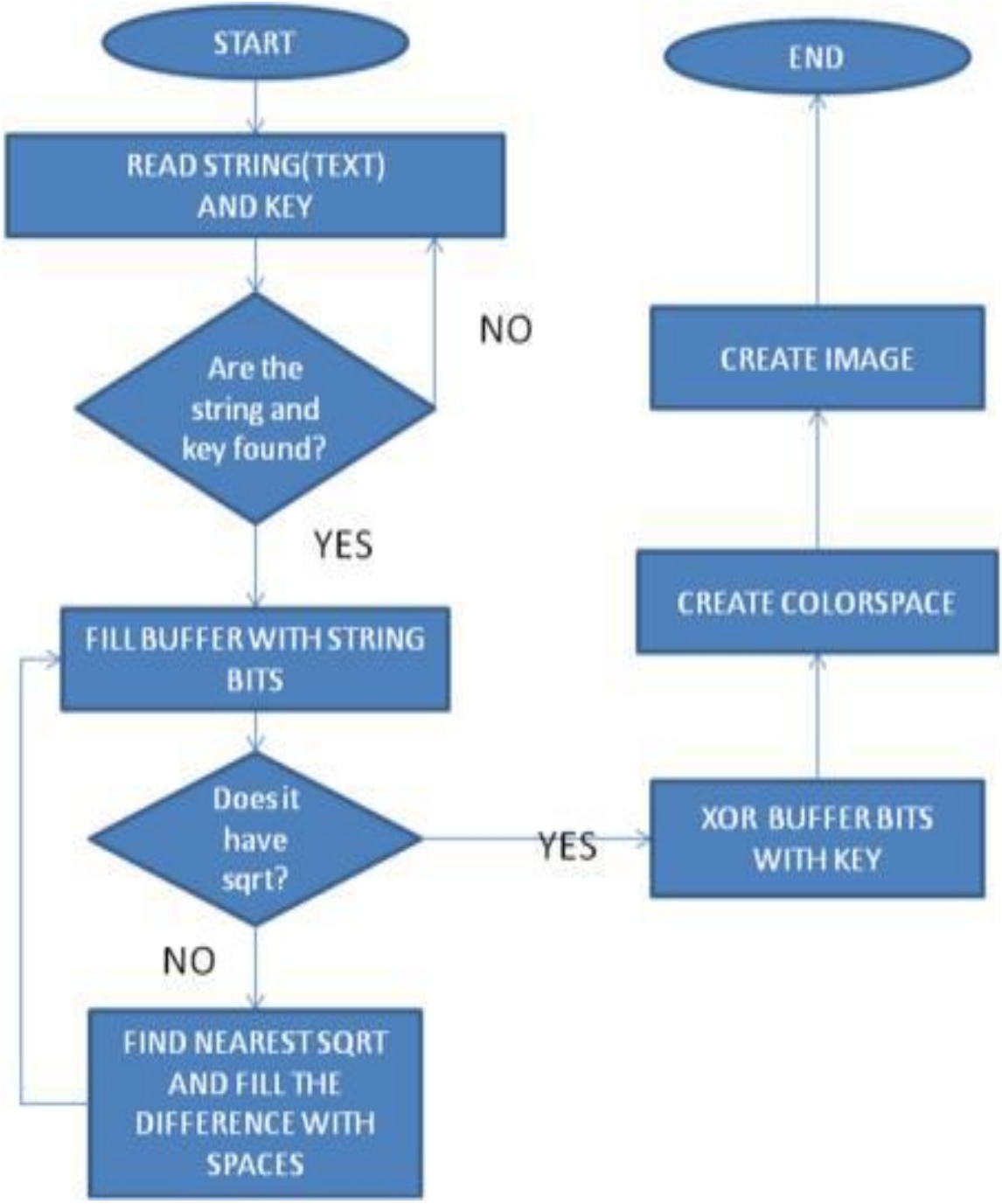
In hexadecimal the bits are:

7 4 17 12 3A 12

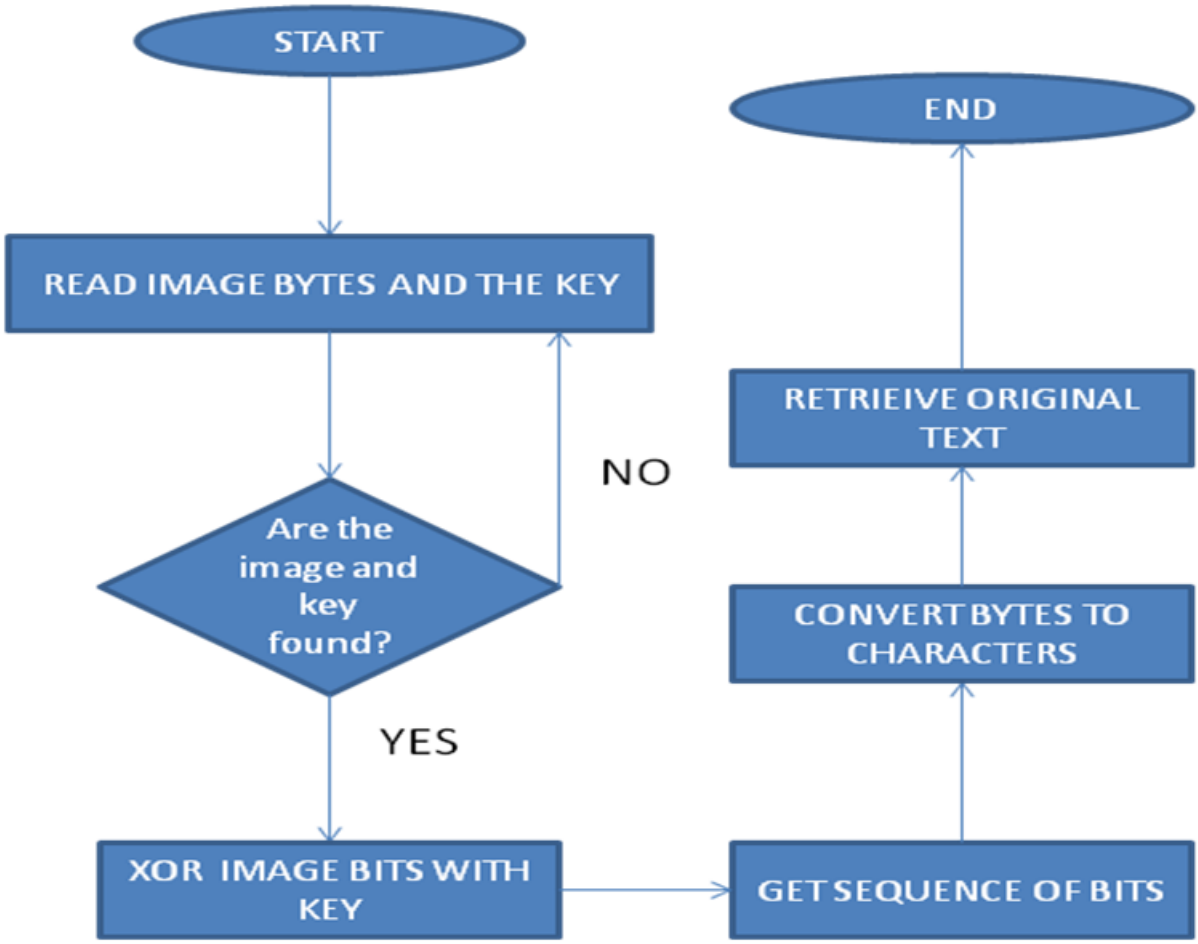
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 08
July 2019

The resultant outcome of our secured system is be like this

Our approach flow chart for encryption



Our approach for decryption



The most important advantage in this cryptographic technique is that it does not require an additional image to hide the text beneath it, besides it has a small size in comparison with all other techniques because no additional bits or data is added to the encrypted file so the receiver receives the file with same size as the original text (Table II). Additionally, our technique is polyalphabetic because when a letter of the original text is changed in to a color it is not necessary to have the same color in the entire image, on the contrary the diversity of colors that will appear encoding the same letter gives our method more strength against cryptoanalysis.

CONCLUSION

In this paper we proposed a novel technique that encrypted the message such a ways that the message encoded as well as hidden in an image. The proposed solution is to use image cryptography to hide textual message. The proposed technique use of an encryption technique that is based on ASCII series & image conversion and a secret key generating the image and spin theory will be used further.

REFERENCES

[1] M. Naor and A. Shamir,"Visual cryptography, "Advances in Cryptography: EUROCRYPT'94, LNCS" , vol. 950, pp. 1–12, 1995

[2] Daoshun Wang,Feng Yi and Xiaobo li, "Probabilistic visual secret sharing schemes for grey scale images and color images,2011",Information Sciences181(2011)

[3] Young-Chang Hou and Zen-Yu Quan, "Progressive Visual Cryptography",J.Electron.Imag(2011).

[4] Kai-Hui Lee, Pei-Ling Chiu "A high contrast and capacity efficient visual cryptography scheme for encryption of multiple secret images",Optics Communications 284(2011).

[5] Tzung-Her Chen n, Chang-SianWu. "Efficient multi-secret image sharing based on Boolean operations",Signal Processing 91(2011).

[6] Shyong Jian Shyu , Kun Chen "Visual multiple secret sharing based upon turning and flipping",Information Sciences (2011).

[7] Tsung-Lieh Lin a, Shi-Jinn Horng, "A novel visual secret sharing scheme for multiple secrets without pixel expansion", Exp. Syst. Applicat., vol. 37, no. 12, pp. 7858–7869, 2010.

[8] Ran-Zan Wang and Shuo-Fang Hsu, ' Tagged Visual Cryptography', IEEE SIGNAL PROCESSING LETTERS, VOL. 18, NO. 11, NOVEMBER 2011 627

[9] DRL Prasanna, LJ Anbarasi, MJ Vincent, A novel approach for secret data transfer using image steganography and visual cryptography International Conference on Communication, Computing and Security, 596-599, February 12 - 14, 2011

[10] LJ Anbarasi, MJ Vincent, GSA Mala, A novel visual secret sharing scheme for multiple secrets via error diffusion in halftone visual cryptography, International Conference on Recent Trends in Information Technology (ICRTIT), 129-133 ,2011

[11] A Vinodhini, LJ Ambarasi, Visual Cryptography for Authentication Using CAPTCHA, International Journal of Computer and Internet Security,vol.2, issue 1,pp.67-76, 2010