Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.98549418

A REVIEW PAPER FOR TRANSMISSION OF ENCRYPTED IMAGE OVER CLOUD SYSTEM

Mr. Prabal Joshi
Research Scholar, Department of CSA, Desh Bhagat University,Mandi Gobindgarh, Punjab
prabaljoshi1@gmail.com

Dr. Shweta Pandey
Assit Professor, Department of CSA, Desh Bhagat University,Mandi Gobindgarh,, Punjab, India
pandey.shweta1608@gmail.com

Abstract

In different cases of data transmission in a communication system of clouds the most widely used approach is encryption which is considered by far a necessary step. Encryption in simple words is locking of information in a box which needs a key to unlock; now it all depends upon the type of technique and its necessary awareness becomes a mandatory part of complete communication systems. Cryptography involves a 5-tuple (P, K, C, and E, D) consisting of the plain text or message P, set of keys K, cipher text C, encryption algorithm E and decryption algorithm D. An Original message is known as the plaintext, while the coded message is called the cipher text. The process of converting from plaintext to cipher text is known as enciphering or encryption; restoring the plaintext from the cipher text is deciphering or decryption. The many scheme used for encryption constitute the area of study known as cryptography. To ensure information and data privacy over the cloud, application is encrypting the user data before sending it over the cloud. In our research work we propose a new scheme which encrypts the text or image message in decrypt form by executing some steps. We expect that results of this technique are very fruitful as compared other technique.

Keywords: Encryption, Decryption, Cloud, Transmission

1. INTRODUCTION

The standard and concept of ―What You See Is What You Get (WYSIWYG)‖ which we encounter sometimes while printing images or other materials, is no longer precise and would not fool a steganography as it does not always hold true. Images can be more than what we see with our Human Visual System (HVS); hence, they can convey more than merely 1000 words. For decades people strove to develop innovative methods for secret communication. The remainder of this introduction highlights briefly some historical facts and attacks on methods [1].

Three techniques are interlinked, steganography, watermarking and cryptography. The first two are quite difficult to tease apart especially for those coming from different disciplines. Steganography is hiding a message in an image so the manner that the very existence of the message is unknown [2].

- 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.
- Steganalysis is the art of discovering and rendering useless such covert messages.

2. BACKGROUND

Pia Singh, 2013 Encryption and decryption of images using a secret-key block cipher called 64-bits Blowfish designed to increase security and to improve performance. This algorithm will be used as a variable key size up to 448 bits. It employs Feistel network which iterates simple function 16 times.

Pratibha S. Ghode, 2014, three different approaches being followed in image encryption, the first approach to key oriented encryption and second approach to Image splitting and the final approach multiple shares. Anchal Jain · Navin Rajpal, 2015 the input image is DNA encoded and a mask is generated by using 1D chaotic map This mask is added with the DNA encoded image using DNA addition. Intermediate result is DNA complemented with the help of a complement matrix produced by two 1D chaotic maps.

3. LITERATURE REVIEW

3.1 Deeply has research on that the Steganography is the technique of hiding private or sensitive information within something that appears to be nothing out of the usual. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between the two is that Steganography involves hiding information so it appears that no information is hidden at all. In this paper, we describe method of Steganography based on embedding encrypted message bits using RSA Algorithm in the 1st least significant (LSB Technique) and last 4 significant bits (Modulus 4 bit technique) of the pixel of image. Here we also provide integrity using MD5 hash algorithm. The analysis shows that the PSNR is improved in the case of LSB technique. Use of hash algorithm provides data integrity [1].

3.2 Attalla M. Al-Shatnawi has discuss on that Steganography is a Greek origin word which means hidden writing. Steganography word is classified into two parts: Stefano's which means "secret or covered" (where you want to hide the secret messages) and the graphic which means "writing" (text). In this paper, a new Steganography technique is presented, implemented and analyzed. The proposed method hides the secret message based on searching about the identical bits between the secret messages and image pixels values. The proposed method is compared with the LSB benchmarking method. It is implemented to hide the secret message "I will come to see you on the first of June" on two Bmp images, with size (24 x 502 x 333) and (24 x 646 x 165) respectively. The results of the proposed and LSB hiding methods are discussed and analyzed based on the ratio between the number of the identical and the non-identical bits between the pixel color values and the secret message values. The proposed method is efficient, simple and fast it robust to attack and improve the image quality, hence it obtained an accuracy ratio of 83% [2].

3.3 T. Morel et al. research on that Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This paper intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganography algorithm and briefly reflects on which steganography techniques are more suitable for which applications [3].

3.4 Prof. Akhil Khare, In any communication, security is the most important issue ill today's world Lots of data security and data hiding algorithms have been developed in the last decade, which worked as motivation for our research. In this project, named "Efficient Algorithm For Digital Image Steganography", we have designed a system that will allow an average user to securely transfer text messages by hiding them in a digital image file using the local characteristics within an image. This project is a combination of steganography and encryption algorithms, which provides a strong backbone for its security.

3.5 The proposed system not only hides large volume of data within an image, but also limits the perceivable distortion that might occur in an image while processing if. This software has an advantage over other information security software because the hidden text is in the form of images, which are not obvious text information carriers. The project contains several challenges that make it interesting to develop. The central task is to research available steganography and encryption algorithms to pick the one the offer the best combination of strong encryption, usability and performance. The main advantage of this project is a simple, powerful and user-friendly Guff that plays a very large role in the success of the application [4].

4. KEY LINK ALGORITHM

The link algorithm comprises the selection of a portion of c0(x), a binarization process, and the selection of L values to represent each key bit. The central 64x64 portion of c0(x) is extracted. This extraction is to provide translation invariance during subsequent verification attempts. Next, the real and imaginary components of the extracted portion are concatenated to form an enrolment template of dimension 128×64, i.e. an array with 128 columns and 64 rows [3, 4]. For example, if the element a+bi appears at position (x, y) of the 64×64 portion of c0(x), then, in the enrolment template, element a will appear at position (x, y) and element b will appear at position (x+64, y). This concatenation process converts a 64×64 complex-valued array into a 128×64 real-valued array. The enrolment template now contains 8192 real values, d, derived from either the real or imaginary components, a or b, respectively. Each value of the enrolment template is then binaries with respect to 0.0, i.e.:

$d \rightarrow 1$ if $d \geq 0.0$ $d \rightarrow 0$ if $d \leq 0.0$

This forms a 128×64 binaries enrolment template, which will be used to link with k0.

5. USE CASE DIAGRAM

The diagram describes the capabilities expected from the proposed system. For this purpose use-cases were used, which show typical interactions between the user and the system under development. The purpose was to capture each possible task that a user can perform with the system in a use-case. All the use-cases together should describe the full system functionality [5, 6]. Fig. 1 presents the use-case diagram for the proposed cipher program.

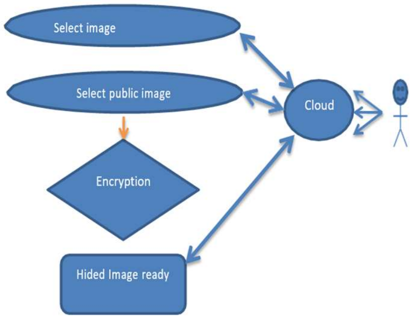

Fig 1 Use Case Diagram

6. PROBLEM STATEMENT

Steganography is a technique which leads to hiding content of one format to another or within the same format. In case of an image there has been a lot of work has been done in the same contrast .The techniques have been proved to a revolutionary step in the field of data hiding [8]. As the passes on , the complexity to hide the data increases .We also need to prevent the base image (refers to the image in which we are hiding the data), so that if the image gets hacked the hacker won‘t be able to assume that some data has been into the base image by looking at the image.

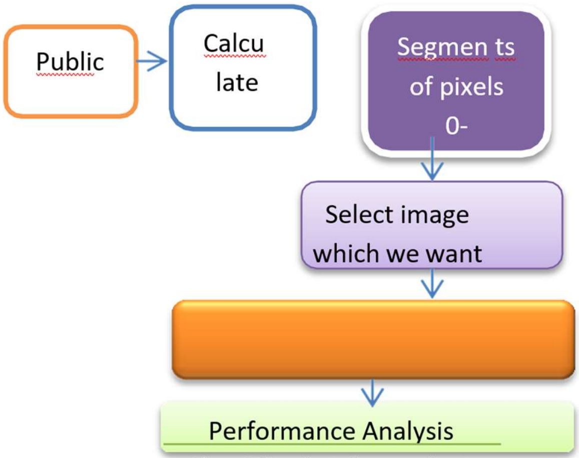

Figure 2 Flowchart of proposed system

7. USED OF ENCRYPTION AND DECRYPTION

Encryption is the process of converting normal message (plaintext) into meaningless message (Ciphertext). Whereas Decryption is the process of converting meaningless message (Ciphertext) into its original form (Plaintext). The major distinction between secret writing associated secret writing is that the conversion of a message into an unintelligible kind that’s undecipherable unless decrypted. whereas secret writing is that the recovery of the first message from the encrypted information.

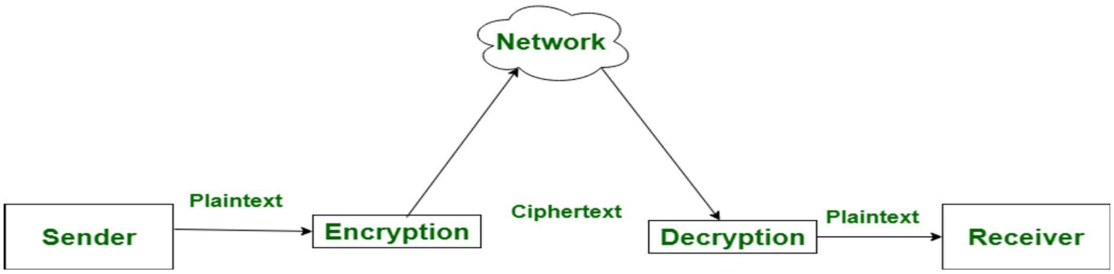

Fig 3. Encryption and Decryption System

7.1 Encryption is a process which transforms the original information into an unrecognizable form. This new form of the message is entirely different from the original message. That's why a hacker is not able to read the data as senders use an encryption algorithm. Encryption is usually done using key algorithms. Data is encrypted to make it safe from stealing. However, many known companies also encrypt data to keep their trade secret from their competitors.

7.2 Decryption is a process of converting encoded/encrypted data in a form that is readable and understood by a human or a computer. This method is performed by un-encrypting the text manually or by using keys used to encrypt the original data.

8. Types of Keys

8.1 Symmetric Key:

Symmetric-key encryption are algorithms which use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext.

8.2 Asymmetric Key:

Asymmetric encryption uses 2 pairs of key for encryption. Public key is available to anyone while the secret key is only made available to the receiver of the message. This boots security.

8.3 Public Key:

Public key cryptography is an encryption system which is based on two pairs of keys. Public keys are used to encrypt messages for a receiver.

8.4 Private Key:

Private key may be part of a public/ private asymmetric key pair. It can be used in asymmetric encryption as you can use the same key to encrypt and decrypt data.

8.5 Pre-Shared Key:

In cryptography, a pre-shared key (PSK) is a shared secret which was earlier shared between the two parties using a secure channel before it is used.

9. CONCLUSIONS

Image Encryption is an algorithm for the linking and retrieval of digital keys, which can be used as a method for the secure management of cryptographic keys. In this paper, a cryptography and steganography methods have proposed for providing better security of data in a network environment. With system that we have proposed data can be transferred between sender and receiver via unsecured network environment. Obviously, in a network environment this system is one of the best ways of hiding the secret of message from intruders. The main focus of the paper is to develop a system with extra security features. The convenience and security provided by Image Encryption will undoubtedly help to promote more widespread use of cryptographic systems.

10. REFERENCES

[1] D. Reshetnikova and P. D. Dunaev, "Academician andrei dmitrievich ado and the kazan scientific research institute of epidemiology and microbiology," Kazan medical journal, vol. 102, no. 1, pp. 115–122, 2021.
View at: Publisher Site | Google Scholar
[2]P. Amudha, J. Jayapriya, and J. Gowri, "An algorithmic approach for encryption using graph labeling," Journal of Physics: Conference Series, vol. 1770, no. 1, Article ID 012072, p. 9, 2021.
View at: Publisher Site | Google Scholar
[3]R. E. Christenson and M. J. Harris, "Real-time hybrid simulation using analogue electronic computer technology," International Journal of Lifecycle Performance Engineering, vol. 4, no. 1/2/3, p. 25, 2020.
View at: Publisher Site | Google Scholar
[4]S. A. Eftekhari, M. Nikooghadam, and M. Rafighi, "Security-enhanced three-party pairwise secret key agreement protocol for fog-based vehicular ad-hoc communications," Vehicular Communications, vol. 28, no. 1, Article ID 100306, 2021.
View at: Publisher Site | Google Scholar
[5]G. M. Kiran and N. Nalini, "Enhanced security-aware technique and ontology data access control in cloud computing," International Journal of Communication Systems, vol. 33, no. 23, Article ID e4554, 2020.
View at: Publisher Site | Google Scholar
[6]A. Ramamoorthy and P. Jayagowri, "A secure public key cryptosystem based medical records using non-commutative group," Journal of Physics: Conference Series, vol. 1964, no. 2, Article ID 022011, 2021.
View at: Publisher Site | Google Scholar
[7]F. Ramzan, S. Klees, A. O. Schmitt, D. Cavero, and M. Gultas, "Identification of age-specific and common key regulatory mechanisms governing eggshell strength in chicken using random forests," Genes, vol. 11, no. 4, p. 464, 2020.
View at: Publisher Site | Google Scholar
[8]G. Qiu, C. Wang, S. Luo, and W. Xu, "A Dual Dynamic Key Chaotic Encryption System for Industrial Cyber-Physical Systems," IEICE Electronics Express, vol. 17, no. 24, 2020.
View at: Google Scholar
[9]M. Arun, S. Praveenkumar, P. S. Rajakumar, and P. Thamizhikkavi, "Cbca: consignment based communal authentication and encryption scheme for internet of things using digital signature algorithm," IOP Conference Series: Materials Science and Engineering, vol. 1074, no. 1, Article ID 012003, p. 16, 2021. View at: Publisher Site | Google Scholar

[10]Iwase, L. Pusztai, K. Blenman et al., “Validation of an immunomodulatory gene signature algorithm to predict response to neoadjuvant immunochemotherapy in patients with primary triple-negative breast cancer,” Journal of Clinical Oncology, vol. 38, no. 15, p. 3117, 2020.

[11]Pia Singh et al "Image Encryption and Decryption Using Blowfish Algorithm in Matlab," International Journal of Scientific & Engineering Research, vol. 4, Issue. 7, July 2013

[12]Vishwagupta, Gajendra Singh ,Ravindra Gupta,―Advance cryptography algorithm for improving data security‖, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012

[13] P. S. Ghode, ―A Keyless approach to Lossless Image Encryption‖, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE.), vol. 4, Issue. 5, pp. 1459- 1467, May 2014.