International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 8, August 2017)

A Novel Approach for Transmission of Encrypted Image over Clouds Using GUI

Shaweta Singh[1], Dr. Rajender Bhatla[2]
[1]M. Tech Scholar, [2]Assistant Professor, CSE Dept, HCTM, Kaithal, Haryana, India

***Abstract*— 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. 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 by executing some steps and then decrypt that text/image at other side using descriptor. We get that result of this technique which are fruitful in case of time saving and near about 85 % accurate.**

***Keywords*—Encryption, Decryption, Cloud, Transmission**

I. Introduction To Steganography

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.

II. 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.

III. 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.:

$$d \rightarrow 1 \text{ if } d \geq 0.0$$
$$d \rightarrow 0 \text{ if } d \leq 0.0$$

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

IV. 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.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 8, August 2017)

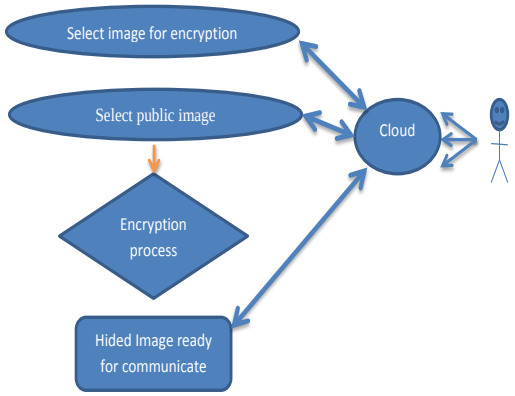

Figure 1 Use Case Diagrams

V. Motivational Story

The study of steganography in machine cryptography was first stated in the prisoner's problem by Simmons. Two inmates Alice and Bob are accomplices in a crime and are sent to the prison. They need to communicate with each other but they have to use a public channel which is monitored by the Warden of the jail. The warden will only forward the messages if they are intelligible. The prisoners accept this condition and find a way to communicate secretly in exchanges establishing a subliminal channel even though the messages themselves are not encrypted. The warden will also try to deceive them, so they will authenticate each other's messages before accepting them – authentication without secrecy.

The situation is paradoxical because the warden demands access and the prisoner's need to authenticate each other [7]. Authentication without secrecy channels achieves that by placing a pre-arranged condition on all messages. It is this capability that creates a subliminal channel for the prisoners. If 'm' redundant bits are allowed to establish authenticity, then these redundant bits create a bit by bit subliminal channel which can be used to transmit extra information.

VI. 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.

VII. Flowchart

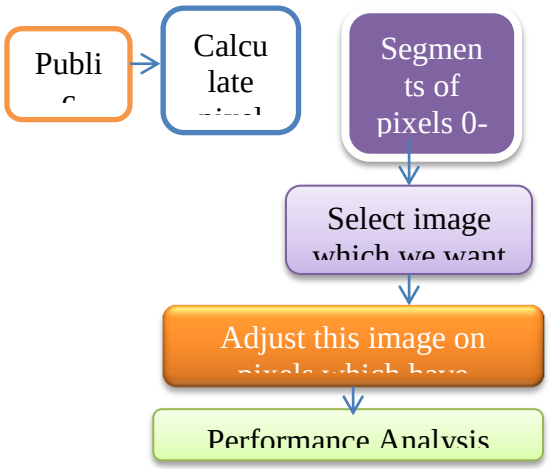

Figure 2 Flowchart of proposed system

VIII. Tool Used For Implementation

MATLAB (MATRIX LABORATORY) is providing an environment for computation in numerical form and we can say it a programming language of 4th generation. Math Works developed it, there is matrix manipulations, interaction with user, create functions, compatible with other languages as like C, C++ etc. By survey it found that near about one million users are available in market which follows MATLAB for programming and numerical computing. Students from any stream like engineering, science etc can use this tool for implementation of proposed algorithm. Many research institutes also use MATLAB as research platform tool.

In technical computing MATLAB perform a vital role. It provides a integration of three environment as like computation, visualization, and programming. There many in built data types and functions that are very useful for developer and make it easy to perform. This also support object oriented programming. Due to these types of tools MATLAB is point of attraction for all researchers. We also choose the MATLAB tool as programing of our proposed work. MATLAB is short form of Matrix Laboratory. The following windows are common in starting of Matlab platform:

- *Desktop:* Desktop represents the basic windows and folders that are open and ready to use for user. Current folder, Command window, Workspace etc comes in desktop.
- *Figure Window:* when a programmer run the program then some outputs generated that are represented in figure window. The color of this window is gray and background is white.
- *Editor Window:* all files written and edited in this window which have extension .m.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 8, August 2017)

IX. Result Analysis

We create a GUI to make it user friendly. GUI attracts the all functions and features of model at a single platform. So we initial our project with GUI interface.

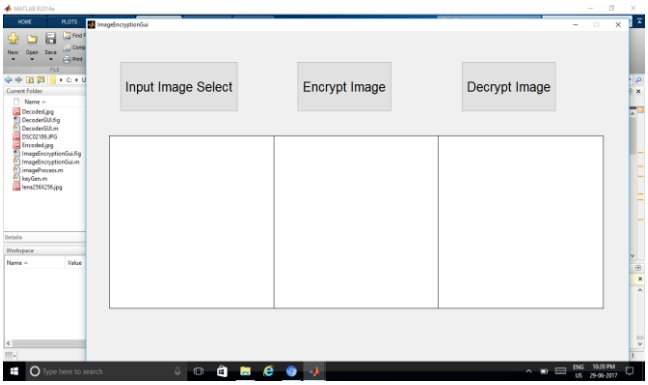

Figure 3 GUI interface of model

Now we need a image which want to encrypt. So we browse it as shown in following figure by pressing the button 'input image select'.

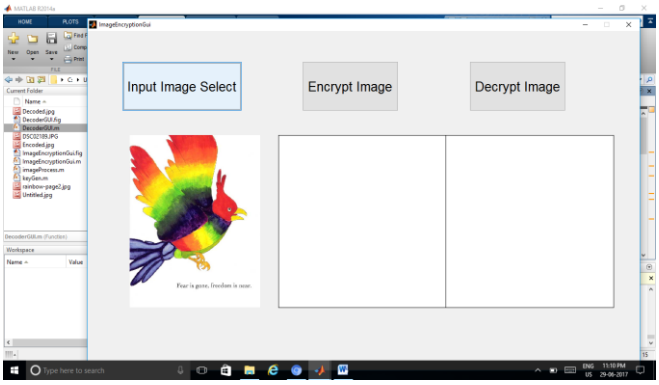

Figure 4 Access of input image for encryption

The output comes from this process is work as like input of proceeding step. The encoded image is shown in middle box. We get this image by pressing the button 'Encrypt image'.

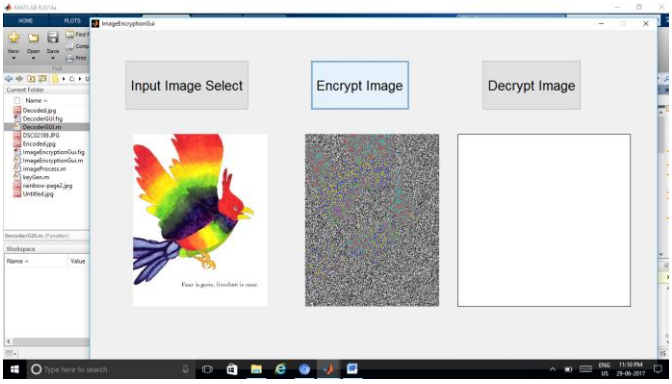

Figure 5 Encoded image after encryption

Now we save decoded image in folder for further transmission over cloud or any social site.

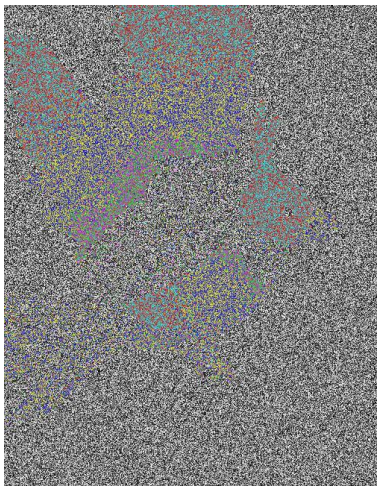

Figure 6 Encoded image save in folder

In this step perform decoding process and the image got as original at same side is as following

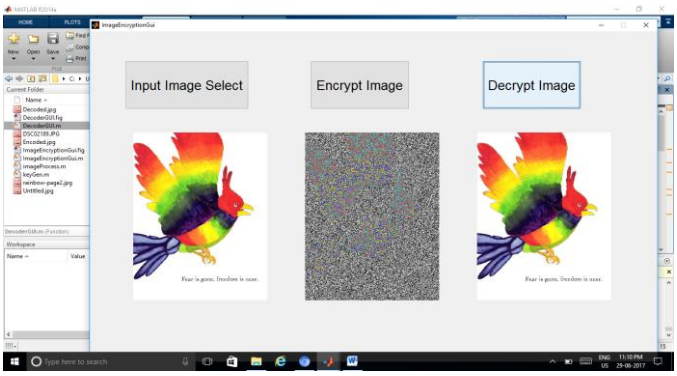

Figure 7 Decrypted image received at same side

Now we upload the image on any social site that is visible to publically and anyone can download. The client or user only can decrypt it to which we sent decoder code. After receiving the code the following GUI open at receiver side:

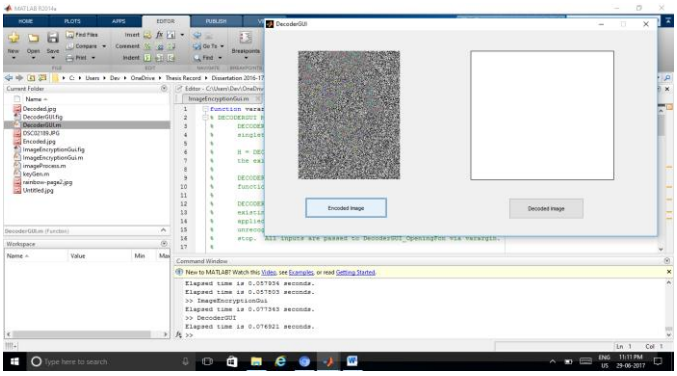

Figure 8 Browse downloaded decoded image for apply decryption process

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 8, August 2017)

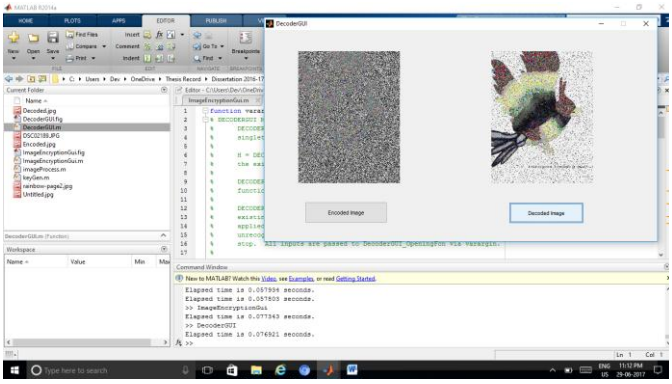

Figure 9 Image received after decryption

Limitation of Encryption Model

As we performed the image encryption on this model, some issues created in it. We introduce the problem of accuracy at client side. When we encrypt the image at sender side then that image loss some features and at receiving side it is very difficult to recover that features because no original image exist at receiving side.

X. 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.

REFERENCES

[1] 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

[2] 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

[3] 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.

[4] W. Zhu, "Image Encryption using CAT Mapping and Chaos Approach," International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 7, no. 3, pp.1-8, 2014

[5] A, Anagaw and V. Sreenivasarao, "A Modified RSA Encryption Technique Based on Multiple public keys". International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 4, June, 2013

[6] P, Kumar and V, Sharma." Information Security Based on Steganography & Cryptography Techniques: A Review". International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue 10, October 2014.

[7] O, Mohammad and A, Al-Hazaimeh." Hiding Data in Images Using New Random Technique". IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 2, July 2012.

[8] C. J, Ezeofor and Ulasi A. G. "Analysis of Network Data Encryption & Decryption Techniques In Communication Systems". International Journal of Innovative Research in Science, Engineering and Technology, pp:17797-17807, Dec 2014

[9] A. Jain et al "A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps," Multimedia Tools and Applications, An International Journal, Springer Science + Business Media Ne Yourk, pp. 1-18, Feb 2015.

[10] A. Devi et al "A Review on DES, AES and Blowfish for Image Encryption & Decryption," (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 6, Issue. 3, pp. 3034-3036, 2015