4th International Conference on Recent Innovations in Science Engineering and Management
India International Centre, New Delhi
(ICRISEM-16)
20th March 2016, www.conferenceworld.in
ISBN: 978-81-932074-6-8

SECURED ENCRYPTION AND DECRYPTION FOR IMAGE TRANSMISSION USING VISUAL CRYPTOGRAPHY

Akshatha A Shenoy[1], Jaipriya K[2], Pooja[3], Mrs. Archana R Priyadarshini[4]

[1,2,3]*Department of CSE, Canara Engineering College, (India)*

[4]*Asst. Professor B.E., M.Tech, MISTE, Department of CSE, Canara Engineering College, (India)*

ABSTRACT

When communication occurs through images, the images can either be confidential or not. But when we want to transmit an image that has to be known only to the sender and the receiver it becomes complicated. Because, during the transmission there may be loss of data which is been sent or a person could hack these image and misuse it. In such scenarios, security of the data is essential. For this we use the technique for the original image so that it is encrypted at the sender site and can be decrypted only at the receiver site.

Keywords: Authentication, Cryptography, Decryption, Encryption, Hashing.

I. INTRODUCTION

Information and communication technology are developing at a faster pace, and huge data is transmitted over communication medium, which needs high security. Even personal data or secret data should always be kept safe and secure from being misused. Several applications like information storage, information management, client information security, satellite image security, confidential video conferencing, telemedicine, military information security and many other applications, require information security in their corresponding areas. For this reason, cryptographers are always trying to propose new methods and techniques to keep data/information secure.

Confidential communication has long been a common practice in the social life. However, as information can be communicated electronically, it is exposed in public domain and unavoidably resulted in interceptions. A scientific approach to respond to the demands of achieving the sense of security is termed as cryptography. The term cryptosystem, also called cipher, is often used in cryptography. The main theme of encryption is to change the message in which its original message can only be identified by an authorized recipient. Encryption methods can also be implemented for images. The image encryption [1] methods are usually classified

Into three types:

(1) Position permutation

(2) Value transformation

(3) Visual transformation

ISBN: 978-81-932074-6-8

Visual Cryptography (VC) is an encryption technique where a secret image is cryptographically encoded into n shares. The images can be transformed or encoded into some other form which one would know, using visual transformation techniques.

In visual secret sharing scheme (k, n) the secret images can be visually revealed by stacking together any k or more transparencies of the shares and by inspecting less than k shares one cannot retrieve the secret image. A nice way of secure communication is obtained through a simple algorithm where decoding is done without any cryptographic computation. Using visual cryptographic scheme, any image or text to be encrypted is fed as an image in the system to generate shares. Shares will be like random noise or it can be called as blur image. Some important goals while developing a visual cryptography scheme is to always have an optimum number of shares ,a good quality of reconstructed image and keeping the size of share so small. Basic VC schemes are used for secured transfer of images, handwritten documents ,financial documents, text, images, topological maps used in military operations like identification of fugitives, satellite communication etc. in a secured manner.

The technique includes various states. Say at sender site before sending multiple images there are few states. When the original images are split and merged together to form a different image and when decrypted the states are repeated and we get back the original image.

II. LITERATURE SURVEY

The Image Based Encryption Technique [2] paper was a proposed method with statistical analysis, key sensitivity analysis and information entropy analysis to prove the existing method is secure against the most common attacks. First we define the histogram and the correlation of the two adjacent pixels in the image to prove the stability against statistical attacks. Second we define the key sensitivity analysis in the image to make brute force attacks infeasible. Third we define the information entropy analysis in the image to protect the information in the encryption process. Then there is no unauthorized access of information in the encryption process.

The image histogram show the distribution of pixels is an image by plotting the number of pixels at each gray scale level we can say that histograms of the plain image and encrypted image are different to each other. The histogram of encrypted image is uniform. Thus, this histogram analysis is robust against statistical attacks. Correlation is defined as the relation of adjacent pixels in an image. Each pixel is highly correlated with its adjacent pixels either in horizontally, vertically or diagonally. In a plain image correlation value is very close to 1, while in encrypted image its value should be as low as possible.

Image Encryption using Different Techniques for High Security Transmission over a Network [3] paper proposes an idea where a single image can be split into n number of modules and they can be encrypted using suitable algorithms so that they can be securely transmitted in the form of shared image. Then in the next phase the split shared images are combined to form a single shared image and then decrypted.

Securing Images using Encryption Techniques [1] paper proposes an idea where the password is given along with the input image. Value of each pixel of input image is converted into equivalent 8 bit binary number. Now length of password is considered for bit rotation and reversal. i.e., Number of bits to be rotated to left and reversed will be decided by the length of password. Since the weight of each pixel is responsible for its color,

ISBN: 978-81-932074-6-8

the change occurred in the weight of each pixel of input image due to bits rotation reversal generates the encrypted image. Finally extended hill cipher is applied to make it more secure.

III. WORKING

3.1 Problem statement

The main problems that arise during image transmission process are with respect to the time it takes to reach the destination and its security level. For real time image encryption only those ciphers are preferable which takes lesser amount of computational time.

When an original image is been transmitted from one end to another over a network, security is essential. In order to secure the data which we send it has to be encrypted. So that the intruder would not get to know or the data cannot be hacked. The images are split and combined, at the decryption end using the same techniques original images are obtained. Hence, the image transmission takes place safely.

3.2 Problem Description

Image is a collection of pixels, which depicts a scenario, an object, etc. Images are of many types like grayscale, colored etc. The advance in communication technology has seen strong interest in digital signal transmission. However, illegal data access has become more easy and prevalent in wireless and general communication networks.

In this scheme, we deal with two images, which is confidential, that has to be transmitted from one end to another. So in between there can be intruders who may be able to read the images. In order to deliver the image with high security we use image splitting and fusion method for encryption and decryption.

At the receiver end, when the receiver receives the message and inserts the appropriate password, the combined or the fused images are split into original images. The process of splitting and fusion of images takes place both while encrypting and decrypting. Hence forth the shared image is been safely transmitted to a specific receiver.

3.3 Objectives

- To successfully transmit multiple images.
- To encrypt and decrypt the images so that no intruder can access the data over a network while transmitting.
- To provide high security at the receiver end so that the actual image can be accessed if and only if password is been known that is been sent from the sender site.

3.4 Outcome

- One will be able to receive the original images which is been sent with no data loss occurrence which cannot be hacked as it is encrypted from the sender site.
- The quality of the images are retained the same.

3.5 Scope

- To successfully transmit two confidential images.
- To encrypt and decrypt the images so that no intruder can access the data over a network while transmitting.
- To ensure high security by providing key from the sender which is used at the receiver end so that the actual image can be accessed if and only if key is known.

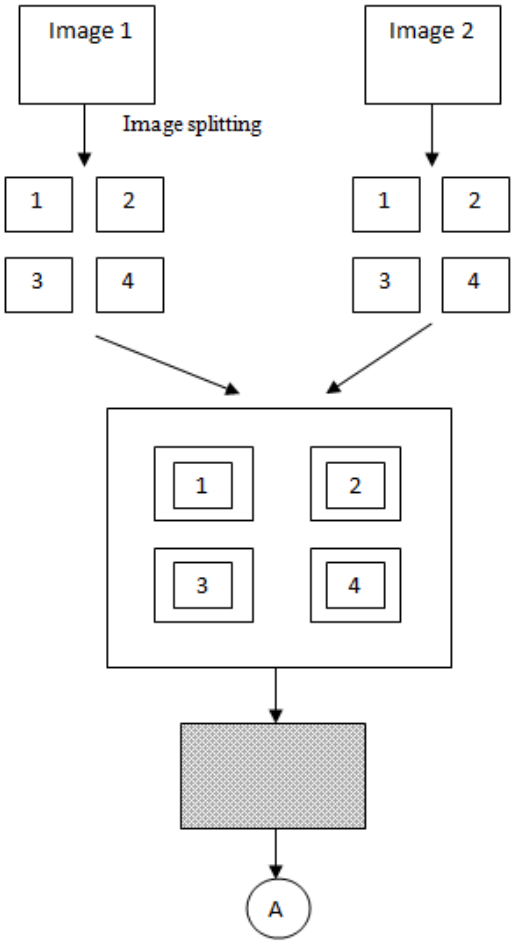
ISBN: 978-81-932074-6-8

3.6 Methodology

Encryption - Here we take two images 1 and 2 (Fig 1) by using an external interface, then we will divide the images into J*J parts i.e. (2*2) parts. Each part of the image will be treated as a single image; we can say 1, 2, 3 & 4. At this stage we use hashing technique to enhance security

The two separate confidential images that have to be transmitted from one end to another are combined to form a single overlapped image. Then the overlapped image is encrypted using an algorithm so that the intruder cannot gain access to the original images forwarded.

Decryption - At the receiver end the receiver should have complete authorization to access the forwarded image. One has to know the password to obtain the original image. If not then a message has to be displayed stating that the user has no complete authorization on the retrieval of the images. If the entered password is accurate then the process of decryption begins. In the decryption process the shared image is again converted into an overlapped image. Then the image is divided into two separate images. In the last stage the two separate split images are merged to obtain the original images.



ISBN: 978-81-932074-6-8

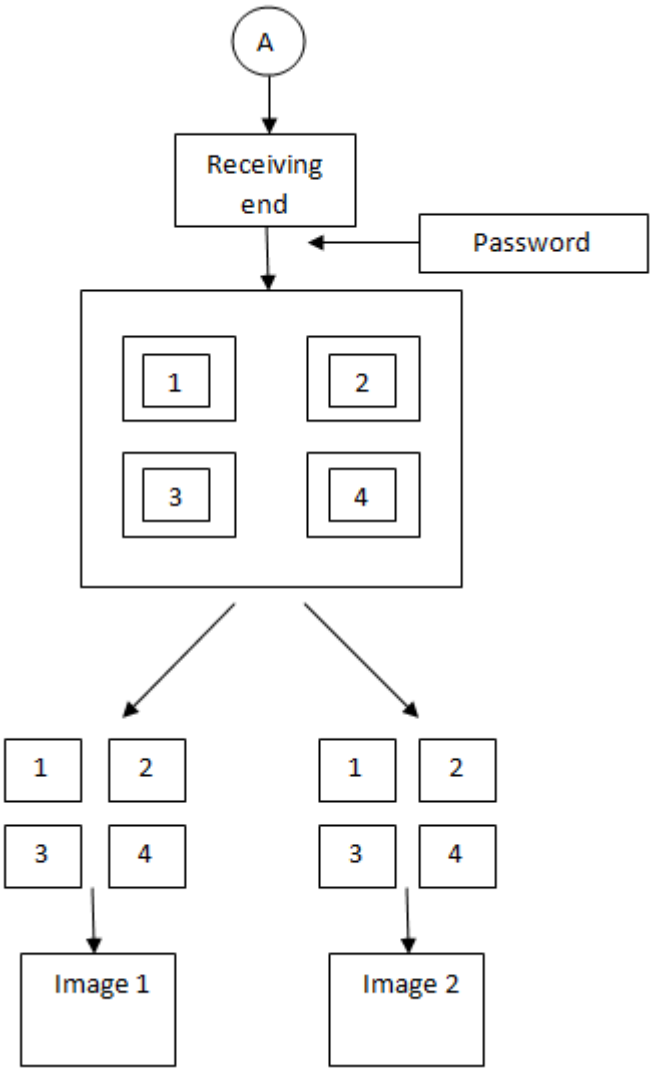


Fig. 1 Process flow

User interface – GUI is used, to easily interact and understand the modules with specified functionalities. We also have a front end page, form page which helps the user to easily upload two images, download images also the labels for user friendliness. Prompts are used in order to acknowledge if the images are been sent successfully or not.

Software interface - We use JAVA to code the modules. We also use different API's and procedure calls to provide communication interface between the modules. Here we make use of different library function which supports the API's. The functions in turn provide interface with the operating system and other software components which are required.

I) Client End

- Front Page – Using web application for the user to interact, download, and upload images.
- Module to split the two images into 4 equal parts respectively.
- Function to apply hashing technique to enhance the security .
- Module to overlap the two split images into a single image.

ISBN: 978-81-932074-6-8

- Module to encrypt the overlapped single image into a shared image.
- Apply RSA algorithm with a key.

II) Server end

- Module to provide interface for the user to enter a key to decrypt the shared image.
- Module to decrypt the shared image in order to obtain a single image which was overlapped.
- Function to split overlapped image as two separate split share of images.
- Function to compare the hash values which were generated during the encryption process.
- Function to obtain back the original confidential images which were initially uploaded from the client end.

III) Functionalities

- Upload image – This function deals with the end user, who has to load the images which are to be transmitted securely. This just loads the image to the interface provided.
- Send image – This includes the function which actually performs all the computation that are required to encrypt the image and transmit the image from one end to the other end.
- Download image – The options or the interface is provided to download the transmitted images that are been sent from the other end. The shared image is downloaded. Meanwhile, the download function also provides the interface or the input method in order to enter the secret key which is been sent from the sender site. After entering the password or key the processing of decryption takes place internally and final original image will be received at the receiver end.

IV. FUTURE WORK

Our future work will mainly focus on to study and analysis of the following:

- Security can be increased by splitting the images into more number of parts and different algorithm can be applied in a single image. If we apply more algorithms it will be more secure than the prior methods which are in use.
- High security can be achieved by providing the physical address at the receiver site.
- Instead of two images multiple images can be used for enhanced security.
- Colored images can be used rather than grayscale images.

V. CONCLUSION

How the images are being transmitted from one end to other securely, providing different security methods at different stages are being presented and discussed in this paper. However there are stages differentiated at both client end and the server end with appropriate modules. Based on these things we would recommend that this project would work successfully and efficiently.

VI. ACKNOWLEDGEMENT

This project is being supported by out institution, Canara Engineering College. We are thankful to our guide Mrs. Archana R Priyadarshini and project coordinator Mrs Sumati Pawar who are providing expertise, which is greatly assisting the project. We are also pleased to acknowledge Mr. Suresha D and Mr. Santosh Hiremat for contributing different feasible ideas to our project.

REFERENCES

[1] Vrinda A, Mr. Arun Anoop M, "Securing Images using Encryption Techniques", International Journal of Computing and Technology, Volume 1, Issue 2, March 2014.

[2] Aman Jain, Namita Tiwari, Madhu Shandilya, "Image Based Encryption Techniques", International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014.

[3] Mohammad Sajid Qamruddin Khizrai , Prof.S.T.Bodkhe , "Image Encryption using Different Techniques for High Security Transmission over a Network", International Journal of Engineering Research and General Science, Volume 2, Issue 4, June-July, 2014.

[4] Xinpeng Zhang, Yanli Ren, Liquan Shen, Zhenxing Qian, and Guorui Feng, "Compressing Encrypted Images With Auxiliary Information", IEEE transactions on multimedia, vol. 16, no. 5, august 2014.