Imperial Journal of Interdisciplinary Research (IJIR)
Vol-2, Issue-5, 2016
ISSN: 2454-1362, http://www.onlinejournal.in

Secured Transmission of Images Using Key Based Dissemination Technique

S. Dileep Kumar[1], M.S. Deepak Prasad[2] &
M. Prasanth Kumar Reddy[3]
[1,2,3]Department of Computer Science, Geethnajali College of Engineering and Technology,

Abstract: *An Image is worth more than a textual data where in short time bunch of information is taken and can be easily understood. Image consists of large portion of complex data. various algorithms are implemented for the encryption of an image but which are cumbersome. This paper proposes a new technique by which the images gets divided into small blocks and then re-arranged by using the key which can be shared between the sender and receiver.*

Keywords:
Encryption, Decryption, Splitting, Chunks, Viewing, sub-blocks.

1. INTRODUCTION

Digital Transformation over the internet has become in our day to day life, in the digital media the images play a very important role and the sharing of the various image types over the internet is also necessary in order to avoid the security threats. Different techniques were applied by the intruders in order to steal the secret images over the network. There are various algorithms implemented for the image security that may take more time for the execution, hence their time and space complexity is more.

Hence different types of techniques involve many processing phases which reduces the quality of images and may that processing steps cannot be applicable for all the image types like bmp, webp, jpef, png, etc.

1. PROPOSED METHOD

This technique gets implemented by following three phases such as [1] Uploading, [4][6] Splitting (Encryption, automatic key generation), [3] Viewing(Decryption). In this system the transform of the secret image is done between the sender and receiver, hence the conversation can also be implemented between the sender and the receiver. First when the user acts as a sender he/her need to upload the correct image type which is very important because it is the first phase of the system to get processed, the image ID gets generated and stored when they upload any new image. Once they uploaded their secret image which is to be shared then they need to apply the algorithm that is dividing the image in to small chunks which is done by giving the number of rows and columns, It is done by the backend admin where he monitors the users actions and give 'n' number of rows and columns in the encryption algorithm , hence key gets generated automatically from the splitting(encryption) image algorithm then the user share this image and their respective keys via any encrypted social network communications. On the receiver side he can view the original image by giving the key that is get shared to his social network accounts by the sender.

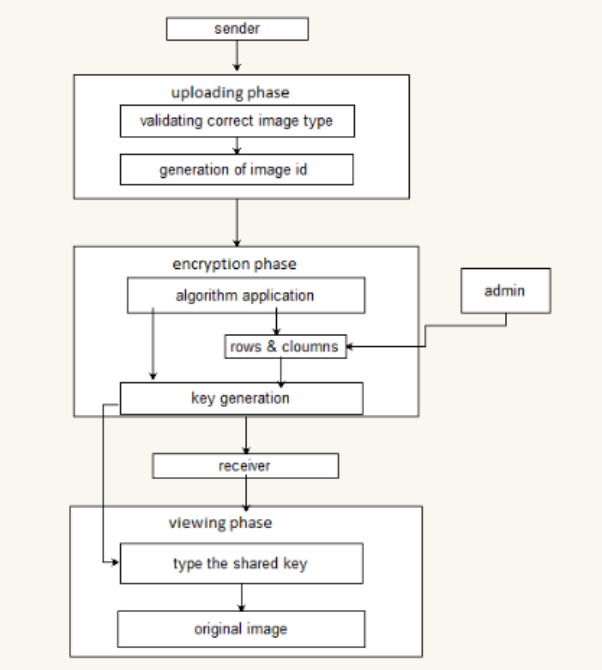

Fig 1. Proposed Method

2.1 Uploading Phase

In this phase the registered user's login to the site by using their credentials then they avail all the functions like update details, upload image, split image, search split images, view image. The

user needs to uploads only the correct image types only because all image formats are not same hence they get rejected while uploading, some image types like jpg, png, are applicable other types may not applicable hence the image size also matters while uploading. Once the uploading of an image is done then automatically for an uploaded image its respective image ID is generated by using the random function.

2.2 Splitting (Encryption Algorithm application)

Once the user uploaded the image then he got the rights to apply the algorithm, in this algorithm the uploaded image is divided into small [7] chunks, for the stronger encryption process the images can be divided into more number of sub-blocks or chunks, the image gets divided only for a particular image id that is generated while uploading an image. The algorithm consists of number of rows and columns basing on this only the image is divided into chunks or blocks. The backend admin role is to give the number of rows and columns based on the different image types when the user uploads an image, from there the admin can view the different image types.

Below is the algorithm which is applied for the encryption of an image, in this the image is divided into blocks in which it is unidentifiable.

```
int rows = 2;

 int cols = 2;

int chunks = rows * cols;

int chunkWidth
=image.getWidth() / cols; //
determines the chunk width
and height

intchunkHeight=image.getHeig
ht() / rows;

for (int x = 0; x < rows;
x++)

{

 for (int y = 0; y < cols;
y++) {

 //Initialize the image
array with image chunks

imgs[count] = new
BufferedImage(chunkWidth,
chunkHeight,
image.getType());  //image
bloks gets stored

}

}
```

After the splitting of an image is done automatically the key gets generated by using the random function for a particular image id. Here we can increase the key size using the random function for the security purpose. Finally, the image is sent to the receiver along the key.

2.3 Viewing (Decryption)

This phase is implemented on the receiver side. Once he/her need to view the original message which is sent by the sender. The receiver can view the image by using the function display original image in that he/her need to give the key that is shared by the sender in this way the original or secret image is decrypted and displayed on their page, in case the key is wrong the receiver will not be able to view the original image, Once the key gets matched for the particular image id then it's all blocks of the image are combined to form an original image.

3. Experimental Result:

The proposed method is implemented to the following image, in this the image which is uploaded by the user is get divided into [4]2X2 when the rows=2 and columns=2 are given, then the number of sub-images get generated are 4 with their image number is get stored. The image is completely unable to identify by this technique. On the receiver side if the key gets authenticated to a particular sender's uploaded image then only the original image is displayed. The size of the actual image is less than the newly generated sub blocks of images.

4. Conclusion & Scope:

The proposed technique provides confidentiality to color image with less computations process is much quick and effective. The key generation process is unique and is a different process. This method can be extended in trying to handle multiple images instead of single image. Further it can be applied to different types of image types.

Large number of [7] image sub-blocks can be generated to achieve high security for the image transmission.

5. Limitations:

This system is applicable only to the following:

- Image size is less than 1MB.
- Applicable only to the jpg, png types.
- If the size increases the splitting function will not work effectively.
- The size of the sub-block images differs from original/secret image

5. References

[1] Chin-Chen Chang, Min-Shian Hwang, Tung-ShouChen, “A new encryption algorithm for image cryptosystems”, The Journal of Systems and Software, 2001, 83-91

[2] M. V. Droogenbroech, R. Benedett, "Techniques for a selective encryption of uncompressed and compressed images," In ACIVS’02, Ghent, Belgium. Proceedings of

Advanced Concepts for Intelligent Vision Systems, 2002.

[3] I. Ozturk, I.Sogukpinar, "Analysis and comparison of image encryption algorithm", Journal of transactions on engineering computing and technology, December, vol. 3, 2004, p.38.

[4] A. Mitra, , Y V. Subba Rao, and S. R. M. Prasanna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science, vol. 1, no. 1, p.127, 2006.

[5] Li. Shujun, Li. Chengqing, C. Guanrong, Dan Zhang., and ikolaos,G., Bourbakis, "A general cryptanalysis of permutation-only multimedia encryption algorithms," 2004, http://eprint.iacr. Org/2004/374.pdf

[6] Mohammad Ali Bani Younes and Aman Jantan, “Image Encryption Using Block-Based Transformation Algorithm”, IAENG International Journal of Computer Science, Feb 2008.

[7] Mohammad Ali Bani Younes and Aman Jantan “An Image Encryption Approach Using a Combination of Permutation

[8] Technique Followed by Encryption”, IJCSNS International Journal of Computer Science and Network Security, Vol.8 No.4, April 2008 191.