ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (140-145), Month: July - September 2016, Available at: www.researchpublish.com

SECURE MOSAIC IMAGE TRANSMISSION THROUGH NETWORK

Haritha G

M.G University, Mount Zion College of Engineering, Pathanamthitta, India

Abstract: **The Secret Mosaic Image Transmission through Network using Attribute key encryption is the most secure technique for the confidential data transfer across the network. Create the Mosaic image same as that of the target image. It is completely a client-server communication system. The sender side include embedding part and receiver side include extraction part. The receiver will open a port and will wait for the response from the sender. For the smooth functioning of client and server it is designed as separate threads in the application. The user can select a file and then specify compression to encrypt it. The secret key is encrypted using the key. He can then specify a recipient and a title for the message and send the file and the encrypted secret key. In receiver end the decryption process is done automatically when a user is downloading a document. Then the key is used to decrypt the encrypted file to obtain the plain text file. If the keys don't match then a message will be displayed. For establishing the communication the sender system will open a port and will wait for the response from the client. Then the encrypted file will be captured at the client, save it in to the system with the relevant information and send a message to server. When the message is received the client will display it and go back to client mode. For the smooth functioning of client and server it is designed as separate threads in the application. For encryption we are using attribute key encryption method, we associate each data file with a set of attributes, and then assign each user an expressive access structure which is defined over these attributes. To enforce such kind of access control, we utilize KP-ABE to escort data encryption keys of data files. This construction enables us to immediately enjoy fine-graininess of access control.**

Keywords: **Attribute Key Encryption, Client Server Communication, MFT Protocol Image Encryption, Mosaic Image, Secure Image Transmission.**

I. INTRODUCTION

A new technique for secure image transmission is needed, to transform a secret image into one meaningful Mosaic tile image having size almost same and looking similar as that of target image. The whole application is designed based on sender to receiver architecture. This module handles the communication between the server and the client. The sender side include embedding part and receiver side include extraction part. The receiver will open a port and will wait for the response from the sender. For the smooth functioning of client and server it is designed as separate threads in the application. Managed file transfer (MFT) refers to solutions that facilitate the secure transfer of data from one computer to another through a network. MFT solutions are often built to support the FTP network protocol.

As compared with FTP, here MFT offers a higher level of security and control than FTP. This module manages the transfer of encrypted file through the network. A client can then rendezvous with the server at the server's port. While one of the sockets listens for a connection request, the other asks for a connection. If once two sockets have been connected, then it can be used to transmit the data into both or either one of the directions. In order to increase security the encryption process is done when the user is composing a document to be transmitted across the network. The decryption process is done automatically when a user is downloading a document. Then the key is used to decrypt the encrypted file to obtain the plain text file. If the keys don't match a message will be displayed. This module handles the communication between

two system. Here for encryption we are using attribute key encryption method, and also we associate each data files with a set of attributes, then assign each user an expressive access structure which is defined over these attributes.

II. EXISTING SYSTEM

Recently, many methods have been proposed for the purpose of secure image transmission, for which two common approaches are image encryption technique and data hiding method but the most recently used method is Secure Image Transmission Technique via Mosaic Images.

A. Image Encryption

Image encryption is a technique that makes use of the natural property of an image, such as high redundancy and strong spatial correlation, to get an encrypted image based on Shannon's confusion and diffusion properties. The encrypted image is a noise image so that no one can obtain the secret image from it unless he/she has the correct key. However, the encrypted image is a meaningless file, which cannot provide additional information before decryption and may arouse an attacker's attention during transmission due to its randomness in form. An alternative to avoid this problem is data hiding that hides a secret message into a cover image so that no one can realize the existence of the secret data, in which the data type of the secret message investigated here is an image.

B. Data Hiding Technique

The method is very efficient especially when applied to those images whose pixels are scattered homogeneously and for small data. The given image is partitioned into four level blocks, and the data will be embedded into selected the four diagonal sub blocks values depend upon key. This algorithm only requires fewer steps and it can embed data efficiently without discarding image. Embedding 4 bits information in a 4*4 pixel block need to change very less pixels on average. Furthermore, the quality of the produced stego-images is better than that of other methods.

C. Mosaic Image Transmission Technique

A new impregnable image transmission technique is proposed here, which transforms automatically a huge-size of secret image into the secret-fragment-visible mosaic image of the same size. The mosaic image is looks similar to an arbitrarily selected target image. It can be obtained by fragmenting the secret image and transforming their color characteristics corresponding to the blocks of the target image. Here the dexterous techniques are designed to conduct the color transformation process then the secret image can be recovered without any loss. The converted Pixels' color values having overflows/ underflows can be handled by recording the color differences in the transformed color spaces is also proposed. The mosaic image is embedded by the information required to recover the secret image using a lossless data hiding scheme along with a key.

III. PROBLEM DEFINITION

The whole application is designed based on sender to receiver architecture. This module handles the communication between the server and the client. The sender side include embedding part and receiver side include extraction part. The receiver will open a port and will wait for the response from the sender. For the smooth functioning of client and server it is designed as separate threads in the application. Managed file transfer (MFT) refers to solutions that facilitate the secure transfer of data from one computer to another through a network. MFT solutions are often built to support the FTP network protocol. MFT offers a higher level of security and control than FTP. This module manages the transfer of encrypted file through the network. In order to do communication over the TCP protocol, a connection must first be established between the pair of sockets. TCP provides a point-to-point channel for applications that require reliable communications for MFT.

IV. MAIN MODULES OF PROPOSED SYSTEM

A. Mosaic image creation

i) Secret image consists of the tile images should be fit into the preselected target image having the target blocks.

ii) The color characteristics of each tile image in the secret image could be transforming to become that of the corresponding target block in the target image.

iii) With respect to the corresponding target block, rotating each tile image into direction with the minimum RMSE value.

iv) For future recovery of the secret image, the relevant information should be embedding into the created mosaic image.

B. Domain Authority Module

The domain authorities are authorized and managed by the trusted authority. In this module a new domain authority has to register under the trusted authority and the trusted authority distributes master key to it based on its domain name attribute. This master key can be used for authorizing the users that registered under the domain authority. The master key for domain authority is generated by the trusted authority using the steps :

1. The public key and master key of the trusted authority is taken and exored.
2. The exored result is again exored with the domain name attribute.

The final exored result is stored as the master key of the domain authority. This key is used for creating secret key for users. The domain authority can login to the system and can view the details of all the users with their uploaded files and access policies. The domain authority can revoke an existing user from the list. The revoked user can still do all the operations provided, but decrypting the ciphertext files.

C. Data User Module

The data users can register under a domain authority and the domain authority distribute secret key based on the attribute value that particular user. The user attributes chosen are username, password, role etc. The secret key generation is as follows:

1. The attributes department, agency and role are exored successively and it is exored with an alphanumeric string
2. The exored result is again exored with the master key of the domain authority and the final result is stored as the secret key of the user.

While we using the existing files in the system, the logined user can create files, for file process and can delete the file owned by him from server. Only text files can be created and processed in the system. The file access is allowed in read mode only. In the process of file creation, the user can create text files by inputting the text message and the filename. The file will be saved in the current directory of the system. A file is chosen and encrypted in file process, using a symmetric key. Then the symmetric key is encrypted using attribute based scheme to provide security. Then both ciphertexts are uploaded in cloud. The users can download files from the cloud and using his secret key the ciphertext of the symmetric key is decrypted and then by using these symmetric key, the ciphertext file is decrypted. The symmetric key is generated using file properties such as filename, size and last modified. These attributes are exored successively to get the symmetric key.

- Fractioning of the text into 64-bit that means 8 octet blocks;
- The initial permutations of blocks;
- Breakdown of the blocks into two parts: left part and right part, named L and R;
- 16 times or rounds, the Permutation and substitution are steps repeated.
- Re-joining of the left and right parts then inverse initial permutation.

The encryption of the symmetric key is using by the public key of the system. After encrypting an access policy is associated with the file. The access policy specifies to whom the file can be decrypted. The access policy is a combination of attributes and the logical AND and/or OR gates. Both encrypted text file and the key are uploaded in the cloud. The data consumer downloads the files from the cloud to decrypt. Before decrypting the file, the access policy associated with the file is checked with the attributes the user's secret key as in CP-ABE scheme. If these two matches, then the encrypted key can be decrypted using the secret key of the user. This symmetric key can be used for decrypting

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (140-145), Month: July - September 2016, Available at: www.researchpublish.com

the ciphertext of the text file. After this, the user can view the plaintext that is, the contents of the text file. In file deletion, the uploaded files can be deleted from cloud. The file deletion can be performed only the data owner of the file. Up on the request for deletion from a user, the cloud checks whether he is the data owner of that file, or not. If he is the data owner, the particular file will be deleted from the server.

D. Managed Image Transfer

Managed file transfer (MFT) refers to solutions that facilitate the secure transfer of data from one computer to another through a network. MFT solutions are often built to support the FTP network protocol. MFT offers a higher level of security and control than FTP. This module manages the transfer of encrypted file through the network. Here streaming control protocol known as TCP (transfer control protocol), that is a connection oriented protocol. A connection must first be established between the pair of sockets for the communication over the TCP protocol. A point-to-point channel provides by the TCP protocol for the applications that require reliable communications for MFT. A server application binds a socket to a specific port number in the connection-based communication such as TCP. While we registering the server with the system to receive all data destined for that port. Then the client can meet or rendezvous with the server at the server's port. When one of the sockets listens for a connection request or as server, then other asks for a connection that means client. Once two sockets are being connected, then they can be used to transmit data in both or either two directions. A socket is bound with a port number. So that the TCP layer can recognize the application that data is designed to be sent. This is similar like the end-point of tunnel or pipe-line design. The java.net package provides two classes- Socket and ServerSocket- that helps to implement the client side connection and the server side of the connection, respectively.

V. WORKING

Based on the client/server communication the java.net package provides several classes which support socket. The Intent Address class encapsulates the Internet IP addresses and it supports conversion between the dotted decimal address and host names. The Socket, ServerSocket, Datagram Socket and Multicast Socket classes implement client and server sockets for both connection-oriented and connectionless communication. The Socket Implclass and SocketImpl Factory interface provide hooks for implementing custom sockets. The hostname of the machine knows by the client , on which the server is running and the port number on which the server is listening.

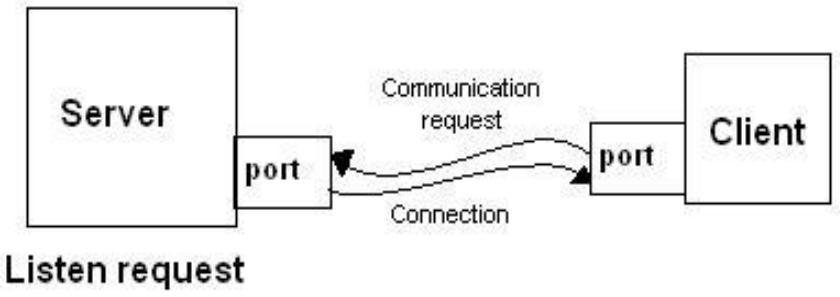

Fig. 1 - Client- Server Communication

The client request to the server on the server's machine and port, for make a connection request. Then the client also has to discover itself to the server so it binds to a local port number which will use during this connection. This is usually assigned by the system. If everything goes well, the server accepts the connection. Upon acceptance, the server will get a new socket which bound to the same local port and also has its remote endpoint set to the address and port of the client. It needs a new socket so that it can continue to listen to the original socket for connection requests while tending to the needs of the connected client. On the client side, if the connection is accepted, a socket is successfully created and the client can use the socket to communicate with the server.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (140-145), Month: July - September 2016, Available at: www.researchpublish.com

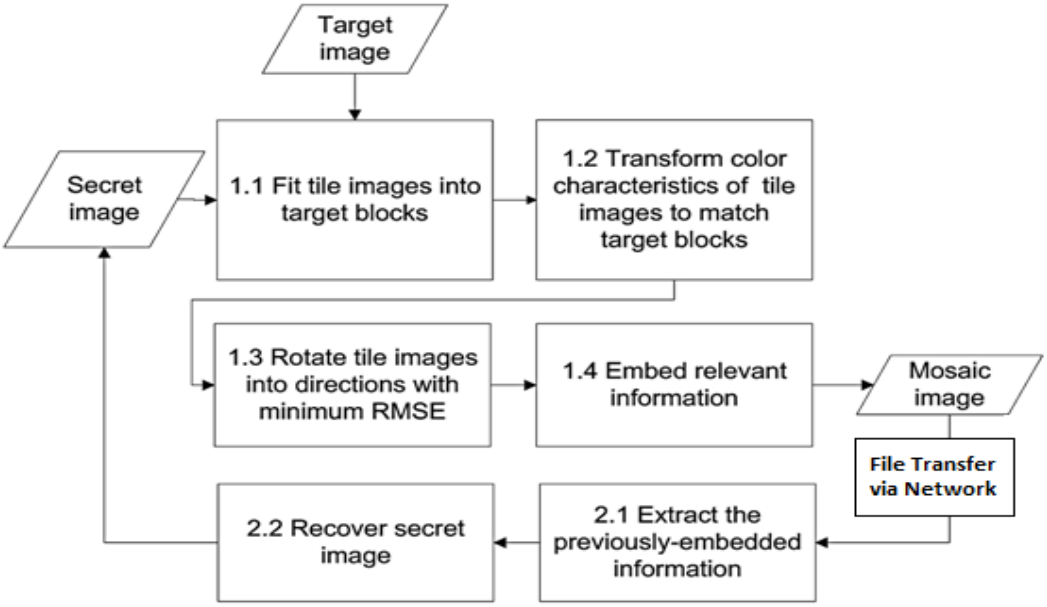

Fig. 2 - Mosaic Image sending and secret image recover.

The encryption process is done when the user is composing a document to be transmitted across the network. The user can select a file and then specify compression to encrypt it. The secret key is then encrypted using the key. He can then specify a recipient and a title for the message and send the file and the encrypted secret key. The decryption process is done automatically when a user is downloading a document. Then the key is used to decrypt the encrypted file to obtain the plain text file. If the keys don't match a message will be displayed. This module handles the communication between two system. The sender system will open a port and will wait for the response from the client. Then the encrypted file will be captured at the client, save it in to the system with the relevant information and send a message to server. After sending the data the client will open another port and wait for response i.e its operation now will be in server mode. On receiving the message the server will display the file with relevant information. When the message is received the client will display it and go back to client mode. For the smooth functioning of client and server it is designed as separate threads in the application.

V1. PERFORMANCE ANALYSIS

It can be seen from the that the created mosaic image retains more details of the target image when the tile image is smaller. It can also be seen that the block ness effect is visible when the image is magnified to be large; but if the image is observed as a whole, it still looks like a mosaic image with its presence similar to the target image. This fact in another way a mosaic image created with minor tile images has a smaller RMSE value with respect to the target image. At first, we compute the means and standard deviations of T and B, respectively, in each of the three color channels R, G, and B These results proves that the proposed data hiding technique is totally revertible, and the original mosaic image can be retrieved at the receiver side without any distortion and by using HSV color transformation, secret image can be retrieved with less distortion than RGB color conversion method.

In mosaic image are yield by dividing the secret image into tile images and then transforming their color characteristics to be those of the corresponding target blocks, one problem arise here is that during color transforming, edge distortion may occur and during the recovery stage, low similar secret image is recovered. But in this method, first color conversion of secret image is done then tiling of both images is take place. So that edge distortion can be reduced and maximum similar image can be recovered. In RGB color conversion method, mean and standard deviation quotient method of target image are taken from its 3 channel and based on this value secret image color are converted.

Here, In order to increase the security level, first target image color is converted to HSV and based on this H, S, V value; mean and standard deviation quotient value are calculated and then convert secret image color based on it. By this method, difference between target image and mosaic image can be reduced and after hiding of this mosaic image, visual distortion of target image can also reduce. Thus an intruder can't easily identify that inside this image some other values

are present. From the table it is clear that target image with HSV hidden image has low RMSE value so it has less distortion when compared to RGB image. And from table, it is clear that recovered image after HSV color converted image has less distortion with respect to its original image than RGB color converted image. And also it is clear that secret image with tiff format hidden inside target image in jpg format has less RMSE value than other target images. To increase the security of the proposed method, the embedded information is encrypted with a secret key and also mosaic images are hidden inside the target image in different bit positions. Only the receiver who has the key and correct order in which mosaic image hidden can decode the secret image.

VII. CONCLUSION

The image transmission technique via network using attribute key encryption method is the most powerful and secures way of data transfer scheme. Here the created mosaic image is similar as per that of the target image. Attribute key encryption provides more security to the confidential data to be transfer. Here the encrypted data is transfer among the network. The whole application is designed based on sender to receiver architecture. This module handles the communication between the server and the client. The sender side include embedding part and receiver side include extraction part. The receiver will open a port and will wait for the response from the sender. For the smooth functioning of client and server it is designed as separate threads in the application. Managed file transfer (MFT) refers to solutions that facilitate the secure transfer of data from one computer to another through a network. MFT solutions are often built to support the FTP network protocol. MFT offers a higher level of security and control than FTP. This module manages the transfer of encrypted file through the network.

VIII. ACKNOWLEDGEMENT

I would like to extend my thankfulness to the reference authors, as well as reviewer of my paper.

REFERENCES

[1] Suchitra Raman, “An Image Transport Protocol for the Internet”. *Chaos*, vol. 6, 1-12- 2000.

[2] R. Ramya, M. Pachaiyammal, “Secure Data Retrieval by Cipher text-policy Attribute- Based Encryption in Military Networks,” vol. 21, 17-10-2015.

[3] L. H. Zhang, X. F. Liao, and X. B. Wang, “Fast Lossy Internet Image Transmission ,” vol. 24, 8-7- 2005.

[4] A. Albanese, J. Bloemer, “Priority Encoding Transmission,” vol. 32, 4-8- 2007.

[5] Charles J., L. Larry Peterson, “ Image transfer: and end-to-end design,” vol. 35, 10-9- 2008.

[6] R. Neal, and J. Cleary, “Arithmetic coding for data compression”, vol.50, 3-7-2009.

[7] V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, “A robust and secure chaotic standard map based pseudorandom permutation substitution scheme for image encryption,” *Opt. Commun.*, vol. 284, 9-8-2011.

[8] C. Leicher, “Hierarchical encoding of MPEG sequences using priority encoding transmission (PET),"vol. 16, March 2006.

[9] J. Fridrich, “Symmetric ciphers based on two-dimensional chaoticmaps,” *Int. J. Bifurcat. Chaos*, vol. 8, 1-12-1998.

[10] G. Chen,Y. Mao, and C. K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps,” vol. 21, 17-10-2004.