Novel Image Blend Scheme Based Visual Cryptographic In Cloud Secret Image Sharing

P.Anusha, Dr.R.Maruthi

Abstract: In this internet world, data storage and sharing are the most important processes to make proper data utilization and centralization. Especially, most of the real time applications are storing their data and share the secure data to others whenever required. The cloud secret storage and sharing environment can be used to make applications with the feature of secure storage and sharing the content to the others especially image contents. The authorization and authentication of color image can be preserved in that environment with satisfying confidentiality and reliability. The color image blend scheme can be used to implement this way of real time application. In this paper, it is planned to create a secure cloud environment with versatile storage and sharing features and ensure the authentication and authorization of data using novel methodology. The experiment results show that the improved performance rather than the existing works that using cloud storage and sharing.

Key Terms: Cloud storage, sharing, image blend scheme, authentication and authorization

1 INTRODUCTION
Nowadays, Cloud data centralization [1] [2] plays vital role in data management by providing data storage, sharing and availability from anywhere and anytime. Emerging of data centralization through cloud environment satisfies the data availability for the needed users or may in a group. In recent years, the improvements in the cloud technology, the number of user size is growing rapidly. Cloud [4] incorporates the services such as Storage as a Service, Platform as a Service, Software as a Service, and Infrastructure as a Service. In this Storage as a Service would be more useful for the centralization of important data and sharing of data among the users. Increasing of users may cause some of the security breaches in the cloud environment when the confidential data may store or shared. The secret images are stored and shared to the users of the group or sub groups. It is clear to define the thing in secret sharing. As like as Stegnography, the secret data can be shared to the users through hiding in the images. Here the secret image can be stored and shared to the users in the cloud environment. In existing [3], the secret image sharing can be done through the efficient schemes such as shadow model, gray mixing model and pixel based encryption. Here a novel mechanism has been proposed to enhance the secret image sharing and also it can be implemented in the emerging cloud environment. In existing, the dedicated key can be used for the encryption of secret images while sharing. The two or more images are used for the sharing of secret images using proposed novel methodology named as Color Image Blend Scheme Model (CIBS). The visual cryptography can be achieved through the implementation of image blending with the cover image to hide the secret image. It is to concentrate on the secret sharing to the specified users in the groups and sub groups through the dedicated key cryptographic techniques [3][6] using Traditional RSA algorithm. Here the results for the proposed visual cryptographic mechanism in cloud with the services will be explored through the Virtual Cloud storage (VMware) or CloudSim.

2 BACKGROUND KNOWLEDGE
It is most important to know the background particulars and its explanation for clear identification of the problem or to make right solutions to the issue in visual cryptography through image enhancement scenarios.

A. Cloud Storage and Sharing
Cloud Storage is the centralized environment to access the data from anywhere and anytime. It used to offer the availability of data instead of keeping the data anytime. The server has been created deployed for the storage implementation. It having the capability of storage, indexing and hashing to data consistency and avoid redundancy. The environment can be created with possible to add members with access policy scheme.

B. Cloud User Access Policy
The cloud storage [11] can be always used as a multi tenant design so that more number of users can be able to share the data storage or else group of users can able to share the single host for storage and sharing. Here the access policy can be defined for the security implementation over the cloud storage. The user have to create authentication credentials to enter into the cloud server then the authorization token or key for accessing the data storage. It has been illustrated in fig.1.

C. Secret Image Sharing in Cloud Environment
The secure cloud sharing can be achieved through two different categories. First one is sharing among the cloud; the user can share the data for the users among the same cloud network may be from different hosts has illustrated in fig.2. Second one is to share the data to other cloud or hosts. The
cloud user can store the data to the cloud (Public or Private) through creating credentials as cloud user. The images can be encrypted using authorization key then it can be stored into the cloud. If cloud user 2 can obtain the data encrypted data when this user belongs to the cloud with authentication credentials. The user should obtain the key for the file from the data owner. Then the request has been sent with the authorization key and obtains the image data.

Fig. 2 Secret Image Sharing in Cloud Environment

The encryption standards may differ based on users’ perspective. The encryption standards can be defined by the cloud provider for their convenience.

D. Image Blend Scheme
Image Blend Scheme is the process or technique are used to perform the enhancements in the images. Blending can also be used for hiding the image to another image. Initially it obtains the pixel values of the original input image and performs the blend operations with the pixels extracted from the background image. Thus the background image can be used usually some single colored images are also used to easy blend and extraction [7][12]. But it has less security compared with blend using multi colored image. It can be extracted through the de-blending with the pixel expansion of original background image. The some of the blending options are normal, dissolve, lighten and fraction etc. These options are varied through the result obtained through the blending options.

3 RELATED WORKS
Here it is easier to obtain the similar works based on Q A Kester et al. [6] proposed a hybrid approach for encryption of images using the Advanced Encryption Standard scheme and an also with RGB cryptographic technique. This methodology can be done through the implementation of AES algorithm to generate and providing shared secret key for encrypting and accessing the data. This encryption can be done through the implementation of RGB pixel shuffling and displacement. It can achieve with no loss in image quality. Here it can be improved through the RGB pixel blending so that the backdrop image can looks like a normal and it’s tedious to vulnerable. Marwan M et al., [9] proposed a method based on visual cryptography to provide security to the stored medical images in cloud environment. This technique can be achieved without complex mathematical computations. It also reduces the high operating expenses for storing and retrieving the sophisticated data center. Even more it does not having the feature of sharing their data to the other users. Likewise in [10], the medical imaging data are migrated to the cloud environment. In this regard, the security can be ensured with the visual cryptographic algorithm and also it can be stored and shared when migration required. The innovative technique has been used [13] to achieve the visual cryptography and stored it in a cloud environment. It decomposes the RGB pixels and transforms it into the Y, Cr, Cb channels. It can be sent with the cover images to create meaningful shares. When compared to the initial methodology, it achieved the satisfactory qualities while sharing the meaningful reconstruction of images.

4 IBS MODEL FOR CLOUD SECRET IMAGE SHARING
Thus the system architecture has been illustrated below that shows the working principle of CIBS model and user access policy for achieving the visual data from the cloud environment. The cloud user A can take the input color image and extract the pixels using color histogram analysis [7] and thus the pixels should be blend with the background image that can be selected through the user. The two image pixels are blended to obtain resultant image then the resultant image can be encrypted with the RSA image encryption scheme to obtain the encrypted image then this index values are stored in the index table with encryption standard details, background image details and key details. Finally it can be stored into the cloud storage. At the decryption phase, the original image can be shared to other cloud users, they have to send request for the key to make decryption of the images. The images can be decrypted using the decryption key. Thus the de-blending process can also done using the indexed values stored at the time of uploading.

Fig. 3. System architecture for this proposed CIBS model

5 EXPERIMENTAL SETUP
In this case, to provide this experiment as much as real time, the real time jpeg images are taken to test the methodology.
This methodology can be implemented in the Python environment with the editor named Jupyter Notebook with Tensorflow. The results obtained using the keras.models classes from the TensorFlow environment. The natural image data with pixel of 400 x 400 in size can be collected and utilized for the implementation of the proposed detection model.

**Python Syntax:**

**Using TensorFlow backend:**

Thus the cloud environment can be achieved through the implementation of virtual cloud or Windows Azure environment for storage and sharing of visual image data. The proposed scheme is tested in an Windows 8.1/10 64 bit operating system running an Intel CPU (Intel Core i7 Quad CPU 2.5 GHz, 4 GB SDRAM) and the performance is retrieved. The implementation requires Elliptic Curve Diffie-Helman Technique mainly for key generation and it can be indexed with the image blending details, client access privileges, encryption techniques in SHA-1 Hash function used for the initial file uploading of visual image after the encryption process through our model.

### 6 RESULTS AND DISCUSSION

Here this can be experimentally verified through two proposed categories with a single natural image. Fig 4.a shows the input image with white background in jpeg format. Initially this experiment can be done with the single color background image with the RGB values of (0, 255, 0) it shown in the figure 4.b it has been taken as cover image. Then blending options can be performed to get the

**Blended image and it has been shown in fig. 4.c.**

Next to the single RGB image, the multi color image can also be taken as cover shown in fig 5.a and the resultant blend image with the same input image has been shown in fig.5.b. When the considerations of these cover images, the single RGB color image will resembles the hidden input image like watermarking. But the multi colored blend image should not resemblance of actual input image.

The familiar encryption standards like DES, Triple DES, SHA-1 and RSA are considered for the experimentation of this proposed model. The different sized jpeg images are used to validate the encryption time and conclude it with the minimum time taken by the RSA algorithm. Thus the comparisons of these encryption standards are shown in below table.

<table>
<thead>
<tr>
<th>Image Size (MB)</th>
<th>Encryption Time (in milliseconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DES</td>
</tr>
<tr>
<td>64</td>
<td>1250</td>
</tr>
<tr>
<td>128</td>
<td>2580</td>
</tr>
<tr>
<td>256</td>
<td>6033</td>
</tr>
<tr>
<td>512</td>
<td>8435</td>
</tr>
</tbody>
</table>

Among these implementations, it identifies the gradual increase in the encryption time when it increases the size of the image data. Thus the variations in the time usually denote the performance level of the encryption standards. Even more
we are not concentrating on the time, it is a measure used to predict which one is more powerful. It concludes that the traditional RSA algorithm can be used for implementing data security in the cloud environment. Let \( m_1, m_2 \) be the image pixels taken for encryption standard then the algorithm defines as below:

\[
E(m_1) = m_1^e \quad \text{and} \quad E(m_2) = m_2^e
\]

Then we obtain as Ergo…= \( E(m_1) x E(m_2) = m_1^e x m_2^e = E(m_1 x m_2) \)

Further it may improve with the Homomorphic RSA algorithm to obtain more security than the traditional one. The graphical representation of the comparison of encryption standards shown below:

![Graphical representation of encryption standards](image)

**Fig. 6** Graphical representation of encryption standards

### 7 CONCLUSION

Thus a novel methodology can be proposed with innovative scheme of process such as providing blending options over the visual cryptography. In this scheme, the choosing of cover images can optimize the performance of cryptography over the encryption process. Then the secret image can also be protected and achieved by the authorized and authentication cloud users. It is also concentrated how far the confidentiality of data can be achieved through this mechanism. Further, the performance of the visual cryptography will be done with multiple options like pattern assigning, Color scale changing, applying the options such as dissolve, lighten, linear dodge and darken. So that of using these blending options, the visual data security will be obtained in increased manner.

### 8 REFERENCES


