International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V69I4P207

Volume 69 Issue 4, 44-48, April 2021
© 2021 Seventh Sense Research Group®

A Novel Pixel Shuffling And Amalgamation Scheme For Visual Secret Sharing In Cloud Environment

P.Anusha[1], Dr.R.Maruthi[2], Dr.L.Rama Parvathy[3]

[1]*Research Scholar, PRIST University,Thanjavur,Tamilnadu,India.*
[2]*Professor, Department of Computer Science, PRIST University, Thanjavur,Tamilnadu,India.*
[3]*Professor, Department of CSE, saveetha school of Engineering,Saveetha institute of medical & Technical Science, Chennai,Tamilnadu,India.*

[1]shivanu08@gmail.com, [2]rmaruthi2014@gmail.com, [3]ramaparvathyl.sse@saveetha.com

Abstract *- Nowadays, centralized storage has to be implemented in each and every organization to make their data available from anywhere through a cloud environment. The accessibility of data can be varied for public and private clouds. The main reason behind the centralization is the legitimate users can able to make utilization of data stored. Here the visual images can also be stored and shared with the members and non-members of the cloud environment. It is to make secure storage and transmission of image data with the visual secret sharing techniques. However, the existing techniques provide more security over the data sharing through the VSS techniques, sometimes it is vulnerable to threats and attacks, and the main reason is the need to make this transmission without degrading the quality of visual images. Here a novel pixel shuffling and amalgamation scheme has been developed and utilized for visual secret sharing with meaningful shares in the cloud environment. It can able to make secret visual images with high throughput and highly secure with the protection of threats while sharing with cloud members. The experimental results show that the novel algorithm can give high performance and accuracy with the security mechanisms.*

Keywords— *Visual Secret Sharing, Public and Private Clouds, Cloud Security*

I. INTRODUCTION

Cloud computing is the centralized web environment that connects the users to make avail and share the data stored in it. It is upgraded from the functionalities of web servers with an active file transfer protocol. Many organizations need the most important functionality of cloud computing, i.e., sharing the data from the storage to inter and intracloud users [1]. Even the deployment model used for this functionality can be done as a private or community cloud. Even though the deployment models define the accessibility of data from the users, it needs some security measures for the data sharing to members. Thus the data security [8] [9] can be ensured in data sharing among the members of the cloud.

In existing, some of the various kinds of visual secret sharing scheme [2][3] has proposed and even implemented for the existing real-time applications. It is mandated to ensure that the techniques are secure and support the real-time applications which need data sharing in both meaningful and meaningless shares. Even the techniques provide a more secure need to make improved efficiency through the novelty proposed. Here the data sharing can be made as Security as a Service in the centralized cloud environment. It concentrates on the implementation of data security through the cover image with meaningful share with low-intensity variation [18][19].

At first VSS scheme was introduced by Shamir and Blakley in 1971 [7]. It works with the method of securing the data through applying the threshold scheme done through the subsets of shares creation and recreation of data. This number of subsets should be reduced to make effective secret sharing using the technique (k, L, n), but it takes more cost for upgraded protection for secret sharing [10]. Nowadays, cloud sharing can also need VSS techniques [6] [11] to make the higher protection. It is highly complex when we go with the multiple subsets sharing because it uses multiple servers and distributes to the users who are under various cloud network[14][15][16]. Even the pixel blending schemes are also used nowadays to provide high secure data management. The blended image can be reconstructed if the key management could failures.

Here a proposed framework can be designed to perform the sharing without performing the subset creation and distribution, a novel pixel shuffling and amalgamation technique can be proposed in this paper to make secure sharing of data in inter and intracloud systems. It is concentrated on the technique such as pixel identification, rearrange the pixels to make complex for obtaining the data and amalgamation is the most important technique used for proposal sending. Here the data sharing can also be implemented over the centralized cloud storage.

II. RELATED WORKS

It is mandated to obtain the existing discussions to make the clarification in our problem identified and also make some study over the background things. Takahashi S and K Iwamura [12] have discussed the schemes for providing secret sharing in a cloud environment. Here this paper concentrates on the loss of information in the contents over the process of encryption and decryption. An Advanced Encryption Standard (AES) and an RGB cryptographic technique combined together to form a hybrid encryption process approach [5] [20]. The AES key generation and RGB pixel shuffling can be done through this scheme with no pixel so that there was no quality loss.

In [4], X Jin et al. have proposed a methodology for extraction of background with privacy-preserving from video surveillance in multiple cloud servers using the Chinese Remainder Theorem. It can be obtained through the formation of methodologies such as frame segmentation and the separated encryption process. The main advantages of the encryption method such as the original videos cannot be changed over the encryption process, and the video frame information can be learned in the cloud servers to avoid degradation of original data, and it also can reduce the security issues and also enhance the processing efficiency. Learning video frame details makes it more complex so that it has some issues over the real-time implementations.

R Dutta and Annappa B [3] have developed and proposed a novel technique using the threshold-based visual secret sharing scheme. It addressed the major issues of privacy and trust in the database as a service through cloud databases. It considered the indexing technique for the visual secret shares of records in a large-scale database with some properties of secret sharing techniques. It was having some issues over the non-key aggregate queries through the query processing techniques in secret sharing.

Sometimes, shadow construction techniques have been used for the implementation of secret image sharing with meaningful image shares. This technique [17] increases the efficiency of management and also decreases the encryption suspiciousness. Based on a survey with the secret image sharing and meaningful shadow construction techniques, they have designed a well-efficient technique for secret sharing with no pixel expansion.

III. PIXEL SHUFFLING AND AMALGAMATION SCHEME

A novel technique has been proposed to provide high secure encryption scheme with no pixel expansion [13] and shuffling. Here the technique can be evolved into four major phases. It should satisfy the contributions over the cloud network medium. The most important thing is to we are going to perform the operations without making n shares of visual images. Here the most important to make this proposed work without producing the shares of images. It will make some loss of information over the process of combining together at the receiver end. It is planned to perform the pixel expansion, pixel shuffling, and pixel amalgamation with the cover image. Then the metadata of these processes are also indexed and stored in cloud storage, and it can be shared further.

A. Pixel Shuffling

In this phase, the pixel shuffling can be done through the pixel place allocation methodology. Here the pixels can be extracted and expanded for the original image and cover image. Here visual secrets are shared through the cover image. Thus the algorithm for this phase as follows:

```
Algorithm: Pixel Shuffling
def pixel_shuffle(Image image)
{
    set I as image
    eI = extract_pixels(I)
    n=get the Size
    get the random values r for eI
    dI = shuffle using random values r in eI
    store the random key rk in index
    obtain dI
}
```

Here the algorithm should run with two iterations for the original image and cover images; if we need the meaningful shares for the visual secret sharing, it should be

```
pixel_shuffle(orig_image)
```

If we need to perform un-meaningful shares, then we need to call the function for both the original and cover images. So that the pixels of these two images are displaced with that image pixels simultaneously

```
pixel_shuffle(orig_image)
pixel_shuffle(cov_image)
```

where pixel_ shuffle() is a defined function for pixel extraction and shuffling, orig_image is the original image for sharing, cov_image is the cover image used to share the original image.

B. Pixel Amalgamation

In this phase, the pixel values of two images can be amalgamating into the secret image. Here the input for this phase can be taken from the proceeding phase of pixel extraction and shuffling. It needs to get the pixels of the range (0, 0) from the orig_image and (0, 0) from the cov_image, and then it XORed or added to make a new pixel. This pixel formation makes a new image a secret image.

```
Algorithm: Pixel Amalgamation
def pixel_amalgamate(Image orig_image, Image cov_image)
{
    get the extracted images dI_orig and dI_cov
    get the pixels for dI_orig and dI_cov
    amalgamate dI_orig and dI_cov
    obtain and store enc_Image
    store the pixel index
}
 where dI_orig is displaced original image and dI_cov is
    displaced cover image
```

This function has been called when we need to share the secret images to the members of the cloud environment as pixel_amalgamate(displaced original image, displaced cover image).

IV. SYSTEM MODEL

In this section, the system model for this proposed scheme can be explained in detail with the architecture shown in fig.1. The data owner or sender who needs to send the secret image can able to share the visual image with the cover image. Here the below diagram shows the process of sharing the un-meaningful image to the data users. If we required meaningful shares, the architecture should be changed in the pixel extraction phase. It needs to do the pixel extraction and shuffling for the cover image then it produces meaningful shares. But here, the pixel extracted for both the original and cover image and then the pixels can also be displaced, then the shuffling details should be indexed with the key.

After the shuffling process, the pixel amalgamation process starts and makes amalgamation with original and cover images that the encrypted image obtained from that process, and then the details are indexed in the hash table and stored in centralized cloud storage. Thus the stored data can be shared among the cloud members. The cloud members need to request and key and hash values from the hash table to decrypt and access the data using their credentials. The image policy can be applied to make the encryption and decryption process at the end of the data owner and data user. In this process of decryption, the reverse process of pixel amalgamation and pixel rearrangement can be done to make the decrypted or original image. Then the secret image can be utilized by the cloud user.

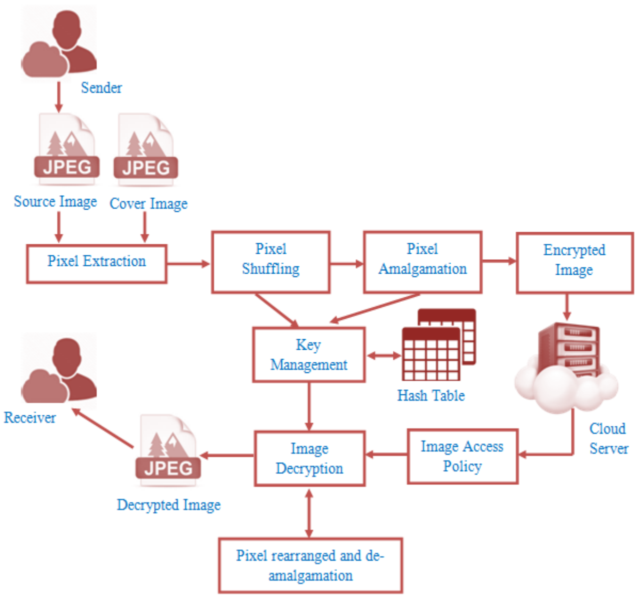

Fig.1 The proposed system model

V. IMPLEMENTATION RESULTS

The implementation of this novel architecture can be done through the Python Jupyter Notebook for obtaining the results over the matplotlib packages. The openCV2 packages are widely used to perform image processing techniques like obtain the histogram values to find the metrics of the image pixel values. The same pixel-sized images should be chosen as cover and secret images shown in fig.1 and fig.2. Let us take universal dataset Lena image in 2000 x 2000 pixels as like that we assume fig.2 in 2000 x 2000 pixels as secret image. Here the color histogram analysis can be used for the performance metrics through the tonal distributions. It has shown in fig.3 and fig.4.

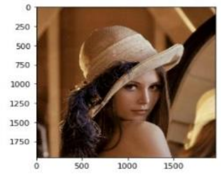

Fig.1 Cover Image

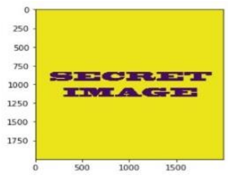

Fig.2 Secret Image

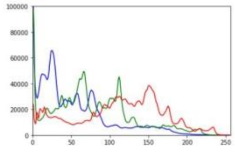

Fig.3 Color Histogram for Cover image

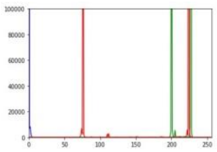

Fig.4 Color Histogram for Secret image

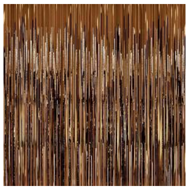

Fig.5. Pixel shuffling of the Cover image

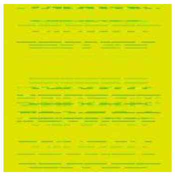

Fig.6. Pixel shuffling of secret image

In this proposed work, we can shuffle both the cover and image for sending the visual secret in un-meaningful ways. Let us take this process and perform shuffling to obtain the results as fig.5 and fig.6. Here we perform both the meaningful share and un-meaningful share by means of amalgamation process so that we can obtain Fig.7 as output secret shared the image as meaningful share with the hidden image as shuffled secret image and fig.8 as un-meaningful share output. The color histogram analysis can be done to make performance metrics using tonal distribution.

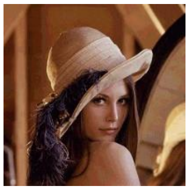

Fig.7. Meaningful share

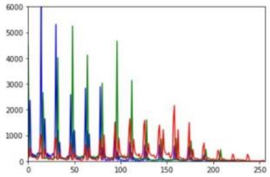

Fig.8. Color Histogram for Meaningful share

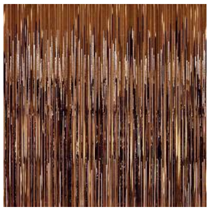

Fig.9. Un-meaningful share.

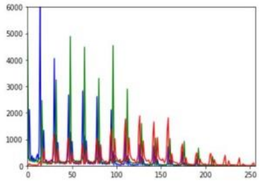

Fig.10. Color Histogram for Un-meaning share

VI. CONCLUSION

Thus the encryption scheme using the novel functionalities of pixel shuffling and amalgamation scheme has been developed and implemented through the Python environment. In this architecture, we have concentrated on the pixel shuffling and replacement through the indexing over the encryption process. If the image encryption can be done by the RSA algorithm, then it produces the secret visual image as unmeaning shares. Here the encryption can be done through the pixel amalgamation scheme. It should be learned with the cover image pixels to make the original image from the encrypted image. In the future, it can able to add to the bit-wise amalgamation for the high security in meaningful and un-meaningful shares in a decentralized cloud environment. Implementation of visual Secret Image Sharing in the decentralized cloud storage will give some challenges over the management of keys and pixel indexes so that it should be overcome in the future.

References

[1] Bincy Jolly and Senthilnathan. T., An Efficient E2C2 Visual Cryptographic Technique to Secure Medical Images in Cloud Environment, Intl. Journal of Innovative Technology and Exploring Engineering, 9(2) (2019) 4709-4714.

[2] C Chen Chang, B Li, and J Sang Lee., Secret Sharing using Visual Cryptography, Journal of Electronic Science and Technology, 8(4) (2010) 289-299.

[3] Dutta, R., & Annappa, B., Privacy and trust in cloud database using threshold-based secret sharing, International Conference on Advances in Computing, Communications and Informatics (ICACCI), India, (2013).

[4] Jin, X., Wu, Y., Li, X., Li, Y., Zhao, G., & Guo, K., PPViBe: Privacy-preserving background extractor via secret sharing in multiple cloud servers, 8th International Conference on Wireless Communications & Signal Processing (WCSP), China, (2016).

[5] Kester, Q.-A., Nana, L., & Pascu, A. C., A Novel Cryptographic Encryption Technique for Securing Digital Images in the Cloud Using AES and RGB Pixel Shuffling, 2013 European Modelling Symposium, UK,(2014)

[6] Kukreja, S., SinghKasana, S., & Kasana, G., Random Grid-Based Extended Visual Secret Sharing Scheme for Image Authentication, 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence), India, January (2018).

[7] Liu, S., Fujiyoshi, M., & Kiya, H., A cheat was preventing method with efficient pixel expansion for Naor-Shamir's visual cryptography, IEEE International Conference on Image Processing (ICIP), France, (2015).

[8] Mamta, Khare, M. D., & Yadav, C. S., Secure data transmission in cloud environment using visual cryptography and genetic algorithm: A review, International Conference on Innovations in Control, Communication and Information Systems (ICICCI), India, March (2019).

[9] Nadlamani, G. F., & Shaikh, S., Preserving privacy using TPA for cloud storage based on regenerating code, International Conference on Recent Trends in Information Technology (ICRTIT), India, September (2016).

[10] P. Li, Z. Liu, and C.-N. Yang., A construction method of (t,k,n) essential secret image sharing scheme, Signal Process., Image Communications., 65 (2018) 210–220.

[11] Reshi, A. A., & Parah, S. A., Performance Evaluation and Future Scope of Image Secret Sharing Schemes, Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC), India, December (2018).

[12] S Takahashi and K Iwamura., Secret Sharing Scheme Suitable for Cloud Computing, IEEE 27th International Conference on Advanced Information Networking and Applications, (2013) 53-537.

[13] Shyong Jian Shyu, & Ming Chiang Chen., Optimum Pixel Expansions for Threshold Visual Secret Sharing Schemes, IEEE Transactions on Information Forensics and Security, 6(1) (2011) 960–969.

[14] Shyu, S. J., & Chen, M. C., Minimizing Pixel Expansion in Visual Cryptographic Scheme for General Access Structures, IEEE Transactions on Circuits and Systems for Video Technology, 25(9)(2015) 1557–1561.

[15] Thomas, S. A., & Gharge, S., Review on Various Visual Cryptography Schemes, International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), India, (2018).

[16] Wu, W.-C., Cheng, K.-C., & Yang, S.-C., Secret digital images over cloud computing using meaningful secret sharing technique, International Conference on Applied System Innovation (ICASI), Japan, (2017).

[17] X Yan, Y Lu, and L Liu., General Meaningful Shadow Construction in Secret Image Sharing, IEEE Access, 6 (2018) 45246-45255.

[18] X. Wu, C.-N. Yang, Y. T. Zhuang, and S.-C. Hsu., Improving recovered image quality in secret image sharing by simple modular arithmetic, Signal Process., Image Communications., 66(2018) 42–49.

[19] Yan, X., Lu, Y., Chen, Y., Lu, C., Zhu, B., & Liao, Q., Secret Image Sharing Based on Error-Correcting Codes, IEEE 3rd International Conference on Big Data Security on Cloud (Big Data Security), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS), China, May (2017).

[20] Zhang, Z., Zhou, F., Qin, S., Jia, Q., & Xu, Z., Privacy-Preserving Image Retrieval and Sharing in Social Multimedia Applications, IEEE Access, 8(2020) 66828–66838.