International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. **05** Special Issue **01** | **2020**

Visual Secret Sharing

[1]Mrs. K Santha Sheela, [2]K.Gayathree, [3]P.Vijayarani, [4]J.Suji Violet, [5]R.Sobika
[1,2,3,4,5] *Department of Computer Science And Engineering, Velammal College of Engineering and Technology Madurai*

ABSTRACT

Multiple secret sharing (SS) scheme is a cryptosystem which encrypts a secret into multiple shares so that any qualified combination of shares can reconstruct the secret, while any forbidden combination of shares reveals no information about the secret in the existing process, the system has more complex stages by introducing two stages for making secure VSS. The first stage is message-based privacy. The Secret Share content was Reversed and content is encrypted with the help of triple DES algorithm. The second stage is image-based privacy. The image-based privacy is applied by embedding encrypted message and user key into multi-media object(image) using LSB based water marking Techniques and then the image is encrypted using AES algorithm. The encrypted image is segmented into shares by file merge and split algorithm. The user key and shares are sent to receiver through mail. The valid receiver can be able to reconstruct the shares into image. By using the user key encrypted message will be obtained. Then the message will be decrypted and reversed to get the secret message. Through this approach the new system improve our privacy and protection of secret sharing.

Keywords*-secret sharing, triple DES, watermarking technique, file merge and split*

I. INTRODUCTION

With the coming era of the internet more and more multimedia data are transmitted and exchanged on the network system with rapid speed. In electronic commerce there is a need to solve the problem of ensuring information safety in today's increasingly open network environment. The encryption is a very important field in the present era in which information security is an important issue in communication and storage of images, the encrypting technologies of traditional cryptography are used to protect information security. With such technologies, the data become disordered after being encrypted and can then be recovered by a correct key. Without the correct key, the encrypted source content can hardly be detected even though unauthorized persons steal the data. Visual Cryptography is a new Cryptography technique which is used to secure the images. This technique divided the image into parts called shares and then they are distributed to the participants. . For security concerns, it also ensures that hackers cannot perceive any clues about a secret image from individual cover images.

Visualcryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decrypted information appears as a visual image.One of the best-known techniques has been credited to Moninoar and Adi Shamir, who developed it in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into *n* shares so that only someone with all *n* shares could decrypt the image, while any $n - 1$ shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all *n* shares were overlaid, the original image would appear. There are several generalizations of the basic scheme including k-out-of-n visual cryptography, and using opaque sheets but illuminating them by multiple sets of identical illumination patterns under the recording of only one single-pixel detector.

II. MODULE DESCRIPTION

A. System initialization

This module will allow the user to register as a valid user by submitting their profile to the Administrator. Once the User will be registered, the user can share secret communication through local mail. The sent and received mail will received as per registered account. The approach of multi-stage secret sharing scheme will be utilized remaining modules.

B. Secret share generation

The Secret Sharing Generation having 2 stages like communication based preprocessing and multimedia object reconstruction through multi-stages. This module is maintain communication based preprocessing like Reversing the original content, Algorithm based Encrypt the reversed content and keep security key based multimedia object embedding of secret message.

C. Secret construction and distribution

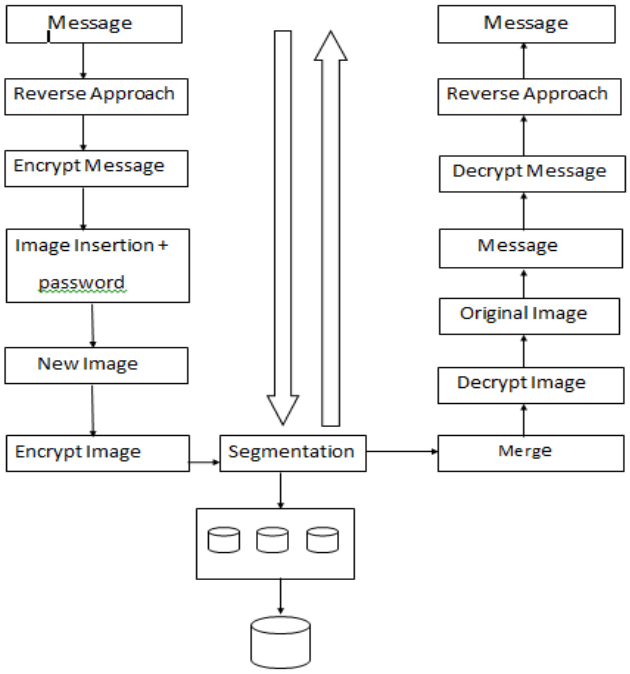
The complete process of Secret share generation , construction process started. This module is multi-based construction with secret share generation result. The Secret Construction using embedding encrypted message into multi-media object, continue to apply file encryption and File Split and Merge also. The segmented original identity will distribute single or multiple recipient with secret key.

D. Verification and secret reconstruction

The verification and reconstruction module consists valid receiver will be reconstruct the sender produced secret sharing scheme. The reviewed multi-segmented identity will download and continue to merging, decrypting. The reviewed original identity having security key with encrypted message.

The encrypted message will applied stage-1 of reconstruction. The message oriented reconstruction used to identify secret message and get original object also.

III. ARCHITECTURE



a.Architecture of Visual secret sharing

A.Text-based secure algorithm:

The text is encrypted using triple DES algorithm.Triple DES (3DES or TDES), officially the Triple Data Encryption Algorithm (TDEA or Triple DEA), is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block. The Data Encryption Standard's (DES) 56-bit key is no longer considered adequate in the face of modern cryptanalytic techniques and supercomputing power. However, an adapted version of DES, Triple DES (3DES), uses the same algorithm to produce a more secure encryption.

The encryption algorithm is:

Ciphertext=Ek3(Dk2(Ek1(plaintext)));

That is, DES encrypt with {\displaystyle K1}k1, DES decrypt with {\displaystyle K2}k2, then DES encrypt with {\displaystyle K3}k3.

Decryption is the reverse:

plaintext=Dk1(Ek2(Dk3(Ciphertext)));

That is, decrypt with {\displaystyle K3}k3, encrypt with {\displaystyle K2}k2, then decrypt with {\displaystyle K1}k1.

This encrypted text is embedded into the image usingLSB based water marking algorithm, that is each bit of encrypted text is overwritten into each 8-bit pixel's least significant bit to hide the data. If data is encoded to only the last significant bits of each color component it is most likely not going to be detectable.The human retina becomes the limiting factor in viewing pictures.

B.Image-based secure algorithm:

The image is encrypted using AES algorithm. The image can only be viewed by the receiver as the image is encrypted using AES and the key is only known to the sender and receiver.Since the key size is 192 bits, it makes the encryption and decryption more secure.The AES algorithm uses a round function that is composed of four different byte-oriented transformations. For encryption purpose four rounds consist of: Substitute byte , Shift row , Mix columns , Add round key While the decryption process is the reverse process of the encryption which consists of: Inverse shift row , Inverse substitute byte , Add round key ,Inverse mix columns.
The encrypted image is segmented into shares using file merge and split algorithm.Split and merge segmentation is an image processing technique used to segment an image. The image is successively split into quadrants based on a homogeneity criterion and similar regions are merged to create the segmented result.

- Define the criterion to be used for homogeneity
- Split the image into equal size regions
- Calculate homogeneity for each region
- If the region is homogeneous, then merge it with neighbors
- The process is repeated until all regions pass the homogeneity test

IV. CONCLUSION AND FUTUTRE WORKS

The system is thus creating secure secret sharing of text in multiple encrypted images. Everyday new VSS techniques are evolving hence selection of the fast and secure Visual secret sharing technique will always useful mainly in terms of security issues. In the future, our project will include sharing of other multi-media such as image, audio and video in multiple encrypted image.

V.REFERENCES

[1] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, “Extendedcapabilities for visual cryptography,” *Theoretical Computer Science*, vol.250, no. 1–2, pp. 143–161, 2001.
[2] A. Beimel, “Secret-sharing schemes: A survey,” in *Proceedings of the3rd International Workshop on Coding and Cryptology (IWCC 2011)*,ser. Lecture Notes in Computer Science. Springer-Verlag, 2011, vol.6639, pp. 11–46.
[3] A. Beimel and I. Orlov, “Secret sharing and non-shannon informationinequalities,” *IEEE Transactions on Information Theory*, vol. 57, no. 9,pp. 5634–5649, 2011.
[4] G. R. Blakley, “Safeguarding cryptographic keys,” in *Proceedings of theNational Computer Conference*. Monval, NJ, USA: AFIPS Press, 1979,pp. 313–317.
[5] C. Blundo, P. D’Arco, A. D. Santis, and D. R. Stinson, “Contrast optimalthreshold visual cryptography schemes,” *SIAM Journal on DiscreteMathematics*, vol. 16, no. 2, pp. 224–261, 2003.
[6] M. Bose and R. Mukerjee, “Optimal (*k, n*) visual cryptographicschemes for general k,” *Designs, Codes and Cryptography*, vol. 55,no. 1, pp. 19–35, 2010.
[7] Y. C. Chen, “Fully incrementing visual cryptography from a succinctnon-monotonic structure,” *IEEE Transactions on Information Forensicsand Security*, vol. 12, no. 5, pp. 1082–1091, May 2017.
[8] S. Cimato, R. De Prisco, and A. De Santis, “Optimal colored thresholdvisual cryptography schemes,” *Designs, Codes and Cryptography*,vol. 35, no. 3, pp. 311–335, 2005.
[9] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed.Wiley-Interscience, 2006.[10] L. Csirmaz, “The size of a share must be large,” *Journal of Cryptology*,vol. 10, no. 4, pp. 223–231, 1997.
[10] Y. Desmedt, S. Hou, and J.-J.Quisquater, “Audio and optical cryptography,”in *Proceedings of Advances in Cryptology – Asiacrypt ’98*, ser.Lecture Notes in Computer Science, vol. 1514. Springer-Verlag, 1998,pp. 392–404.
[11]Lu, C. F., Kao, Y. S., Chiang, H. L., & Yang, C. H. (2003, October).Fast implementation of AEScryptographic algorithms in smart cards.In Security Technology, 2003.Proceedings. IEEE 37th Annual 2003 International Carnahan Conference on (pp. 573-579). IEEE.
[12] Su, C. P., Horng, C. L., Huang, C. T., & Wu, C. W. (2005, January). A configurable AES processor for enhanced security. In Proceedings of the 2005 Asia and South Pacific Design AutomationConference (pp. 361-366).ACM.
[13] Zhang, Z.; Chen, C.; Sun, J. & Chan, K.L. EM algorithmsfor Gaussian mixtures with split-and-merge operation.
Pattern Recognition Lett., 2003, 36(9), 1973-983.
[14] M. Naor and B. Pinkas, “Visual authentication and identification,” in*Proceedings of Advances in Cryptology – Crypto ’97*, ser. Lecture Notesin Computer Science, vol. 1294. Springer-Verlag, 1997, pp. 322–336.