

SECURE DOCUMENT SHARING IN E- LEARNING WITH VISUAL CRYPTOGRAPHY

¹Kavitha Chandrakanthan, ²V, Latha Parthiban

ABSTRACT:

E- Learning is a domain that facilitates learning through internet using electronic devices. E- learning allows the students to learn whenever and where ever needed. Communication of materials between student and tutor are to be secured. This work introduces a novel concept of visual cryptography based method for secure communication in e -learning. The proposed work retrieves the secure document using standard encryption algorithm techniques The outcomes shows annotated way of e-learning content paving way for secure transfer of materials thereby providing student satisfaction and cost effectiveness.

Keywords: E-Learning, visual cryptography, annotation, encryption.

I. INTRODUCTION:

Learning methods are the broad way of creating different interaction between learner and presenter Today there is a need for selecting the learning methods in eLearning. Few methods of learning are pedagogy teaching, m-learning, e-learning. Most commonly used method in olden days is pedagogy method where learning is done in classroom with available material such as notes, blackboard, chalk piece. The classroom belongs to teacher and students. The teacher prepares the notes and delivers in classroom creating interaction in classroom environment. The teacher has the full control to position the student and engage the students by giving assignments, activities and collective contents. M-learning otherwise called as mobile learning where learning is provided using personal electronic devices with portable technologies that is accessible from virtually anywhere. Streaming e-learning is the type of learning used today. Web based learning is most famous concept to convey e -learning services. E-learning provides an open source environment where learning can be done any where and at any time according to the wish of the learners.

Visual cryptography is a technique of cryptography introduced by Naor and Shamir (1994). Visual Cryptography encodes confident image into n shares where any k or more can virtually recover the confidential image ,then directly decodes using human vision . The visual cryptography method uses the secret image by

¹ Research Scholar, Faculty of Computer Science and Engineering, Sathyabama Institute of Science and Technology.

² Department of Computer Science, Pondicherry University CC, Puducherry

stacking operation. The first advantage of visual cryptography technique is computation problem are released during decryption process. Secondly decodes directly using human vision.

II. LITERATURE REVIEW:



Knock's media (2005) described synchronous communication helping in psychological arousal in e-learning. Panayiokes et al. (2011) proved interaction design and issues created in E-Learning. Chirag et al. (2013) studied e-learning based on Learning Management System (LMS). Veeramanicham et al. (2016) described the importance about using cloud computing environment to allow the learners with possible benefits. Signe et al. (2015) concluded to target the output learning according to the effectiveness and learning design.

Ren-Junn Hwang (2002) proposed visual cryptography method with efficient watermark method. Parag and Asoke (2014) proposed on potential tool to improve the quality using Massive Open Online Courses (MOOC's). Lakshmeeswari and Shubham Goel (2016) worked to support anti-phishing framework with the hand of visual cryptography. The outcomes safe guard the framework from phishing attacks. Sejal and Prashant (2016) made a literature review on various visual cryptography techniques such as half tone visual cryptography, multiple secret sharing scheme, extended visual cryptography and natural image visual cryptography method. Rajendra Prasad (2013) proposed an idea of using SaaS, PaaS and IaaS to contribute powerful computing capacity to the end-users. The author showed the implication based on security, reliability and cost effectiveness.

III. PROPOSED WORK

Visual Cryptography is a cryptography technique decoding is done without the use of computation . The use of binary image in visual cryptography are black pixels and white pixels . The undiscloses image selected are partitioned into two shares. Then the partioned part are stacked together and the resultant image is obtained from Human Vision System (HVS) The visual secret sharing scheme has n shares and m transparencies when place together .The confident image are shown as black and white pixels. Encryption is done for each pixel. Encoding and stacking the pixel is shown in Fig. 1

Visual cryptography-based method is mainly used confident material transfer in the cloud. The concept oriented with visual cryptography is to protect the materials .Initially the material needed file is uploaded and converted into readable text format . Secondly that format is converted into image and uploaded in cloud. Further the downloaded image is converted into readable text and again into material needed format as shown in Fig. 2.

	WHITE	BLACK
PIXEL		
Shares	50/100 50/100	50/100 50/100


I		
II		
I & II		

Fig. 1 Stacking the pixel



Fig. 2 Proposed Architecture

Encryption process

The user needs to upload a material containing confident message to be encrypted using encryption process. This encryption techniques involves two phases. At first material is converted into readable text and the text file is encrypted using AES Rejindael encryption algorithm. Each line t is read character wise is converted to ASCII code. Each pixel is put onto a buffer using Set RGB process. A line of the pixel is deposited as first, second and third image. The process is repeated till it completes the file. Image file is bufferd in cloud as shown in Fig. 3.

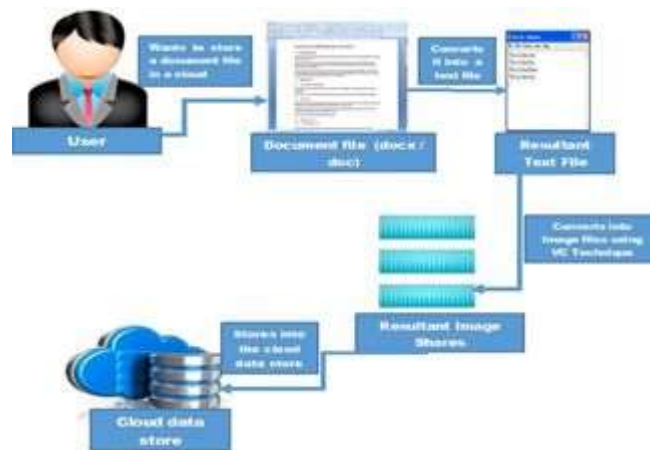


Fig. 3 Image file in cloud

Algorithm for Encryption

- Step 1: Read the material with “.docx”
- Step 2: Access the MS -word file
- Step 3: .XPF extractor returns from word file.
- Step 4: Function getText () is used
- Step 5: Save text file.

Encryption of a text file into image share.

- Step 1: Open “Confident .txt” in only read mode
- Step 2: Create image as image 1, image 2, image 3 and read as character stream.
- Step 3: Compute the width and height.
- Step 4: Read the line from dynamic array list.
- Step 5: Repeat step 3 until end of file.

Decryption process

The material stored is decrypted using decryption algorithm. Decryption process undergoes two stages. At first the image is implemented into text. Each pixel is extracted and converted into hexa code format and the outcome character are fed in the buffer. Secondly the buffer is transferred into original document file. Materials are obtained from the image format is shown in Fig. 4

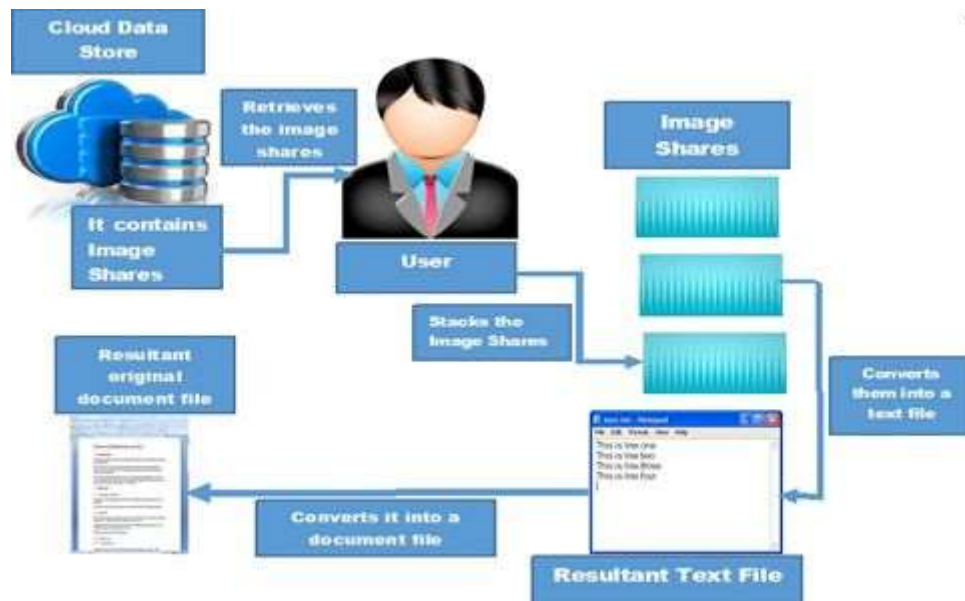


Fig. 4 Material obtained from image

Algorithm for decryption

- Step1: Read the image .
- Step 2: Create new file and new buffer.
- Step 3: Read each line from image 1, image 2, image3.
- Step 4: Extract each pixel using get RGB method.
- Step 5: convert pixel to hexa code.

Converting the text file into original document

- Step 1: Read input file.
- Step 2: Create MS word using XWPFD
- Step 3: read every line from buffer.
- Step 4: Save the material.
- Step 5: Repeat Step 3 till file ends.

IV. Result and Discussion

The proposed work was implemented in Java and experimental results are carried out. Encryption algorithm AES and DES are used. Encryption method done for materials for converting into read mode and then implemented into image . The material is converted shown in fig 5a and fig 5b. and then encrypted into image file as shown in Fig. 6a, 6b, 6c. The resultant image file is decrypted into readable format and converted into materials for the shown in Fig.

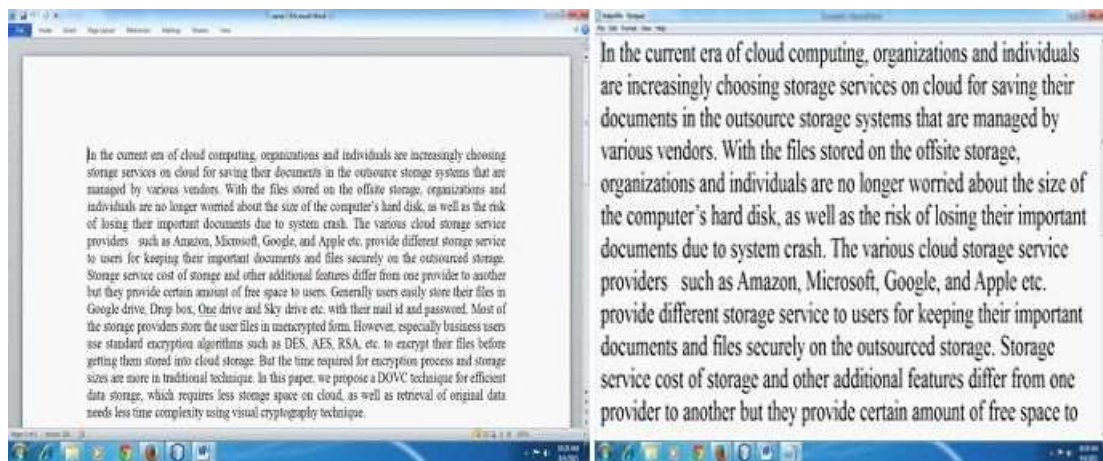


Fig.5 Material

Fig. 5b Image

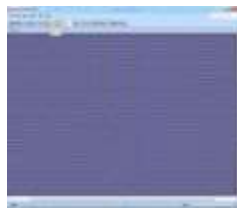


Fig. 6a Image 1

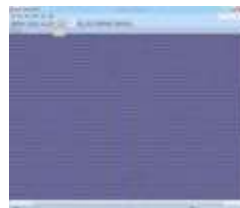


Fig. 6b Image 2

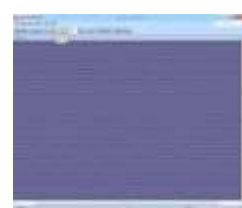


Fig. 6c Image 3



Fig. 7 Original Document

Usage and Satisfaction

The resultant graph shows the usage and satisfaction of E -learning on secure document as shown in Fig.8

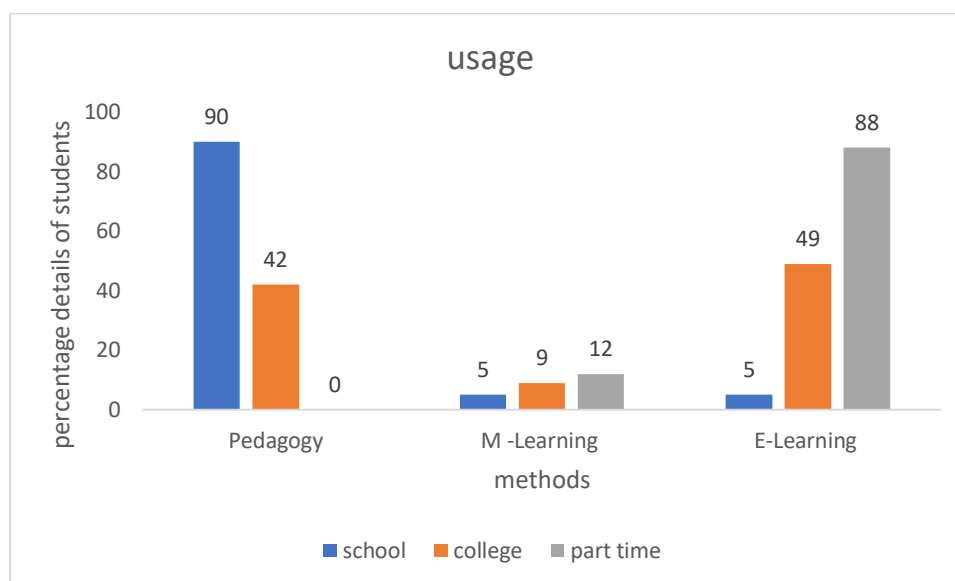


Fig. 8 Learning methods and its usage

V. Conclusion

Visual cryptography achieves data privacy in cloud computing model. The standard encryption algorithm proves the annotated way of E-Learning content in secure transfer of document. The complexity of the approach is less when compared to traditional way of retrieving document. The result also proves student satisfaction and cost effectiveness.

References.

- [1] Naor M.A Shamir (1995), Visual Cryptography - In: Proc. Of Advance in Cryptography, EUROCRYPT '94, In: Lecture notes on Computer Science, Vol.950, pp.1-12.
- [2] Ned Knock (2005), Media Richness or Naturalness? The Evolution of our Biological Communication Apparatus and its influence on our Behavior Towards E – Communication Tools, IEEE Transaction on professional Communication, Vol.48, No.2, pp. 117- 130
- [3] Panniyiokes Koutsabasis, Modestos Stavrakes, Thomas Spyrou and John Darzentas (2011), Perceived impact of asynchronous E – Learning after long term use: Implication for design and development, Int. Journal of Human – Computer Interaction, Vol.27, No.2, pp.191 – 213.
- [4] Chirag Indravadanbhai Patel, Mahesh Gadhave, Atul Patel (2013), A Survey paper in E – Learning based Management System (LMS), Int. Journal of Scientific and Engineering Research, Vol.4, No.6, pp.171 – 176.
- [5] Veeramanicham M R M, Mohana Priya M (2016), Research Paper on E -Learning Application Design Features: Using Cloud Computing and Software Engineering Approach, IEEE Conference on Information Communication and Embedded System, pp. 1 – 6.

- [6] Signe Schake Nose Goard, Rikke Green (2015), The Effectiveness of E-Learning :An Explorative Reviews of the Defraction Methodologies and Factors to Promote E-Learning Effectiveness, The Electronic Journal of E-Learning, Vol.13,Issue:4, pp. 278-290.
- [7] Ren-Junn Hwang(2000), A Digital Image Copyright Protection Scheme Based on Visual Cryptography , Tamkang Journal of Science and Engineering, Vol.3, No.2, pp. 97-108.
- [8] ParagChattenjee and Asoke Nath (2014), Massive Open Online Courses (MOOC,s) in Education – A Case Study in Indian Contest and Vision of Abiquitos Learning, IEEE International Conference on MOOC Innovation And Tech in Education,
- [9] Lakshmeeswari G and Shubham Goel (2016), Anti – Phishing Frame – Work applying Visual Cryptography Mechanism, Int. Journal of Current Engineering and Technology, Vol. 1, No. 6.
- [10] Sejal V Gawande and Prasant R Deshmukh(2016), Secret Image Sharing Schemes: A Review, Int. Journal of Computer Science and Mobile Computing, Vol.5, No.2, pp. 150-153.
- [11]Rajendra Prasad M, Lakshman Naik, Dr.Bapuji V,(2013), Cloud Computing :Research Issue and Implication, Int.Journal of Cloud Computing and Services, Vol.2, No.2, pp. 134 -140.