International Journal of Soft Computing 11 (6): 374-381, 2016
ISSN: 1816-9503

DOVC: Data Obfuscation Visual Cryptography to Protect Cloud Storage

K. Brindha and N. Jeyanthi
School of Information Technology and Engineering,
VIT University, 632014 Vellore, Tamil Nadu, India

Abstract: In cloud computing model, data are stored in a remote server and retrieved by the data owner whenever and wherever required. But there is no assurance that information stored in the cloud server is protected and not modified by the cloud service provider. Plain text storage is vulnerable to security attacks by both illegitimate users and CSP (Cloud Service Provider). Conventional encryption techniques suffer by computational and storage issues. Hence, protecting a cloud storage space is a complex and primary task to be deployed. Data Obfuscation Visual Cryptography (DOVC) proposes a new data storage scheme in a cloud for storing and retrieving a text file using visual cryptography technique with total data confidentiality.This DOVC storage scheme is more efficient than the conventional cryptographic algorithms because of its less mathematical computations, storage size and time complexity. Experimental results are also supporting the claims.

Key words: Cloud computing, encryption, visual cryptography, data confidentiality, decryption

INTRODUCTION

In the current era of cloud computing, organizations and individuals are increasingly choosing storage services on cloud for saving their documents in the out source storage systems that are managed by various vendors. With the files stored on the offsite storage, organizations and individuals are no longer worried about the size of the computer's hard disk as well as the risk of losing their important documents due to system crash. The various cloud storage service providers such as Amazon, Microsoft, Google, Apple etc., provide different storage services to users for keeping their important documents and files securely on the outsourced storage. Storage service, cost of storage and other additional features differ from one provider to another but they provide certain amount of free space to users.

Generally, users easily store their files in Google drive, Drop box, One drive, Sky drive etc. with their mail id and password. They have to store their important documents such as finance, business, personal records, etc., in cloud database. But the cloud service provider is a business organization and the cloud user has to face its inherent risk of his important information being exposed to his rivals or the unauthorized public. Hence, the prime task for any cloud user is to protect his data before storing it in the cloud. Popular service providers such as Amazon Web Services use 256 bit Advanced Data Encryption Standard (AES) algorithm to protect the user data from external attacks (Wan *et al*., 2012) and Google's cloud storage uses conventional encryption 128 bit AES algorithm to protect data. But the time required for encryption process and storage sizes are more in traditional technique. In this stduy, we propose aDOVC technique for efficient, secure data storage which requires less storage space on cloud and less time complexity for the retrieval of original data using visual cryptography technique.

The DOVC usesdata obfuscation instead of regular encryption process to achieve data confidentiality. When the data is in the hands of a third-party that is a cloud service provider, it is exposed. The novel procedure for obfuscation using visual cryptography proves that information cannot be understood by the cloud and is only decipherable by the user. All the existing visual cryptographic techniques have been so far applied only to image and not for text data. This study clearly shows that this is the first technique that uses visual cryptography as a text data obfuscation technique to achieve data confidentiality on the cloud. A user naturally wants to protect his data on the cloud from unauthorized access. If the resource on which the data is stored is owned by the user himself, existing authentication and authorization measures can protect the data from being disclosed, lost, corrupted or stolen.

Corresponding Author: K. Brindha, School of Information Technology and Engineering, VIT University, Tamil Nadu, 632014 Vellore, India

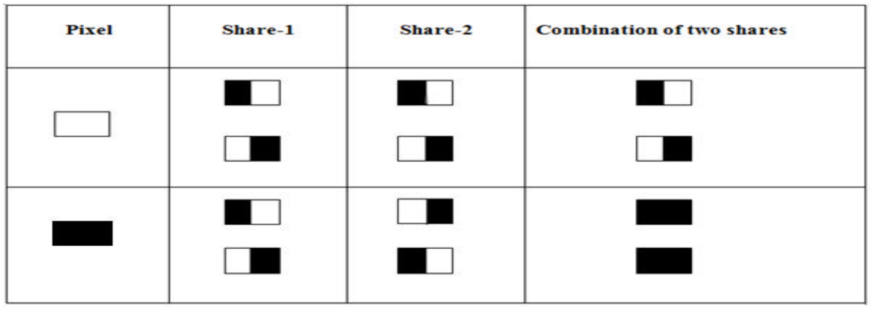

Fig. 1: Encoding and stacking of a pixel

Literature review: Visual cryptography was developed by Moni and Shamir (1995) at the Eurocrypt Conference. Visual cryptography is "a new type of cryptographic technique which can decode concealed images without any mathematical computations." This allows anyone to use the system without any knowledge of cryptography scheme and without need of any computations whatsoever. This technique is very secure and easily implemented. Naor and Shamir's initial model uses binary image which consists of black and white pixels, each pixel is handled individually and it should be noted that the white pixel represents the transparent colour. The visual cryptography technique divides the secret image into 'n' shares called encryption and retrieves the secret image by stacking of 'n' shares. A (2, 2) visual cryptography technique divides the secret image into 2 shares and the original image is retrieved by super imposing the shares one over the other. The secret image is viewed as a collection of black and white pixels. Each share contains collection of 'm' black and white subpixels where each collection represents a particular original pixel. The resulting image can be thought as a $(n\times m)$ Boolean matrix $S = [s_{i,j}]$:

- $s_{i,j} = 1$ if the j-thsub pixel in the i-th share is black
- $s_{i,j} = 0$ if the j-thsub pixel in the i-th share is white

The algorithm in Fig. 1, describes how to encode a single pixel. When a pixel is white, the method chooses one of the two combinations for white pixels and similarly when a pixel is black, it chooses one of the combinations for two black pixels to form the content of the block in the two shares. Then the result of the two stacked pixels is as follows:

- Black and black is black
- White and black is black
- White and white is white

Hence, when stacking two shares, the blocks corresponding to black pixel in the secret image are full black and those corresponding to white pixel are half black and half white which can be represented as grey pixels. As for information security, there are six possible patterns from which every block in a transparency can be randomly chosen, so the secret image cannot be identified from a single transparency. The drawbacks of the basic model are thehuge size of the image (the retrieved secret image is two times larger than the original image) and its optimum quality. Several researchers concentrated in invariant size of image shares (Lin and Tsai, 2003; Ito *et al*., 1999). Yang (2004) developed the probabilistic visual cryptography technique for secret images which consist of white and black pixels (binary image) without pixel expansion. This technique directly uses two basic matrices S_0 and S_1. Shares are generated by using these matrices without any pixel expansion. Encryption is performed by randomly selecting the column of S_0 or S_1 depending on white or black pixel (Yang, 2004). However, the limitation of this model is the quality of the image and certain loss in the recovered image because every pixel is not exactly recovered (Jaafar and Samsudin 2012).

The extended basic model uses grey scale image instead of the binary image. The grey scale image is transformed into black and white image by halftone technique; then each pixel in the binary image is decomposed into 2×2 block of the two shares based on the rule and the secret image is recovered by stacking of the two shares (Blundo *et al*., 2000). For more security purpose, visual cryptographic technique is applied to color images as follows:

- Transform the color image into three halftone images Cyan, Magenta and Yellow
- Decompose the halftone image into 2×2 block shares
- Apply black mask
- Determine the position of Cyan, Magenta and Yellow based on the position of black pixels
- Reconstruct the original image by stacking of all the shares (Hou *et al*., 2003)

Conventional visual cryptography technique generates noisy pixels on shares which indicates that

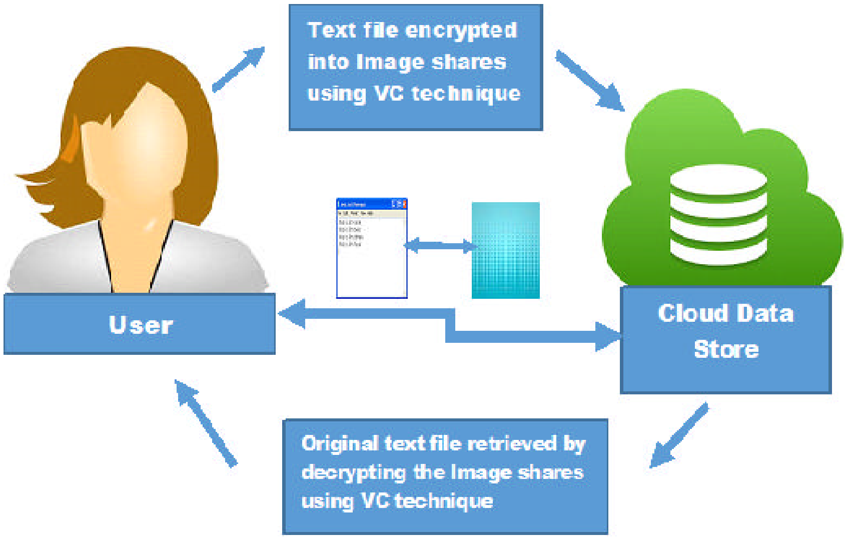
Text file encrypted into Image shares using VC technique
User
Cloud Data Store
Original text file retrieved by decrypting the Image shares using VC technique

Fig. 2: Storing and retrieving a text file using VC technique

some hidden secret image are on a share. This can be avoided by extended visual cryptography technique. Encryption is performed by two phases. In the first phase, the secret image is divided into shares and in the second phase the secret shares are embedded into meaningful cover images. No one can easily identify the secret data embedded in an image (Lee and Chiu, 2012; Jaya, 2013).

The secret image is encrypted at hierarchical levels. Four shares are generated based on two hierarchical levels. Key share is created by using any three shares from among the four using soft computing technique. Finally one of the two resultant shares is stored in database and the other one is passed to the recipient (Chavan *et al*., 2014). The following study proves that the same visual cryptographic technique can be effectively applied for text data to achieve total data confidentiality and security.

MATERIALS AND METHODS

Data storage on cloud: DOVC technique mainly deals with using visual cryptography to protect text data in the cloud instead of using encryption techniques. All the current research in the domain of cloud computing security is focused on using some encryption techniques for sending and retrieving data. The DOVC approach is to avoid using standard encryption techniques. Instead we use visual cryptography for uploading and downloading data. The user has some secret information in a simple text file that is to be uploaded to the cloud. If the secret information is in another format, it must be converted into text file. The overall concept of the system is simple; instead of uploading an unencrypted file, it must be converted into image shares and uploaded into the cloud. Later the downloaded image shares must be converted into a text file using Visual Cryptography technique as shown in Fig. 2. The following steps are to be performed for uploading a text file into a cloud and downloading the text file from the cloud.

Uploading a secured text file:

- Select the text file which is to be uploaded
- Convert the text file into image shares using the DOVC technique
- Encrypt (text-file) = Image-share 1 and 2
- Upload them on a cloud
- Select the image shares which are to be downloaded
- Download them from the cloud
- Stack them using DOVC technique and get the original text file
- Decrypt (image-share 1 and 2) = Text-file

When the user wants to upload a text file which contains some secret information, it must be encrypted by DOVC encryption technique. Every line from a text file must be read and each character is extracted based on its position and then converted into ascii value and this value is converted into a pixel using SetRGB() method in java. The resultant pixel is stored in the relevant co-ordinate (x, y) postion in the buffered image. The (x, y) indicates the line of the text file and the position of the character in the line, respectively. Each and every pixel in a line is stored in image 1 and 2 alternately. This process is repeated until the file comes to an end. Finally, the the image shares must be uploaded into a cloud as shown in Fig. 3.

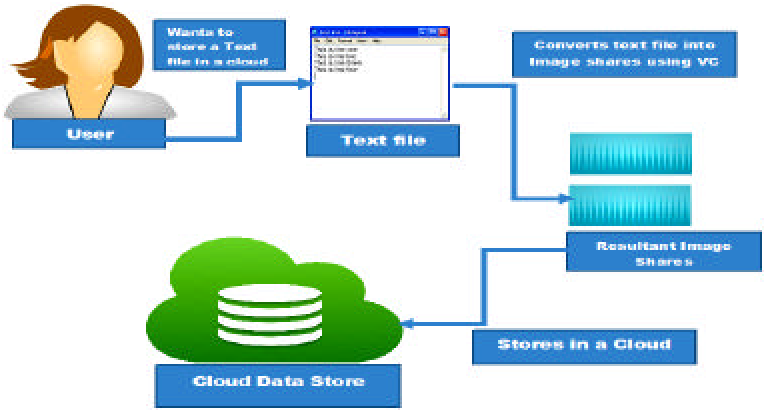
Wants to store a Text file in a cloud
User
Text file
Converts text file into Image shares using VC
Resultant Image Shares
Stores in a Cloud
Cloud Data Store

Fig. 3: DOVC decryption process

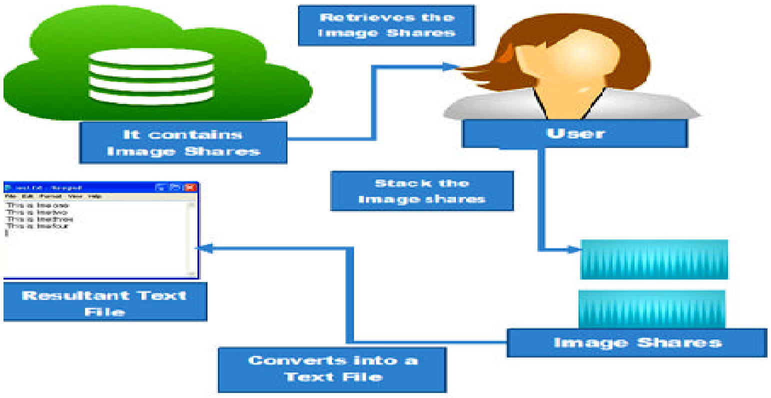

Fig. 4: DOVC encryption process

Algorithm: For Encryption of text file into image shares

Input: Secret file

Output: Image Shares

- Read the secret text file
- Intitialize the two images shares Image-Share1, Image-Share2 with png format
- Transfer all the data from the secret file into buffer
- Compute the width and height of the image shares based on the content of secret file
- Width of the image shares = Maximum number of characters in a line from the file
- Height of the image shares = Number of lines in the secret file
- Read a line from the buffer
- Extract each character from the line based on its position
- Findascii value for the character
- Compute the individual pixel by passing ascii value to SetRGB method in java
- Store each and every pixel in a line in Image-Share1 and Image-Share2 alternately
- Place the pixel on the image shares based on its x, y co-ordinates where x, y indicates the line number and the position of the character in thatlinerespectively
- This process is repeated till the end of the secret file

- Finally save the image shares such as Image-Share1, Image-Share2 stored in (.png) format using ImageIo.write method in java

Decryption process: When the user wants to download the image shares which contain some secret information, they must be decrypted by DOVC technique. Every line from the image shares which is in .png format must be read and every pixel from a line must be extracted using getRGB Method. Each pixel must be converted into hexa code and the resultant character stored in a string buffer. This process is repeated until the file comes to an end. Finally, all the contents of the buffer must be transferred into a text file as shown in Fig. 4.

Algorithm: For decryption of text file from image shares

Input: Image shares

Output: Secret file

- Read image shares Image-Share1.png, Image-Share2.png
- Initialize the string buffer
- Extract each and every pixel from the lines in the image shares using getRGB() method
- Compute ascii value for the extracted pixels
- Find relevant characterfor each asciivalue and store them in a buffer
- Finally transfer the content of the buffer into a text file “Text.txt” using filewriter method in java

RESULTS AND DISCUSSION

The proposed DOVC algorithm has been implemented in Java and various experimental tests have been carried

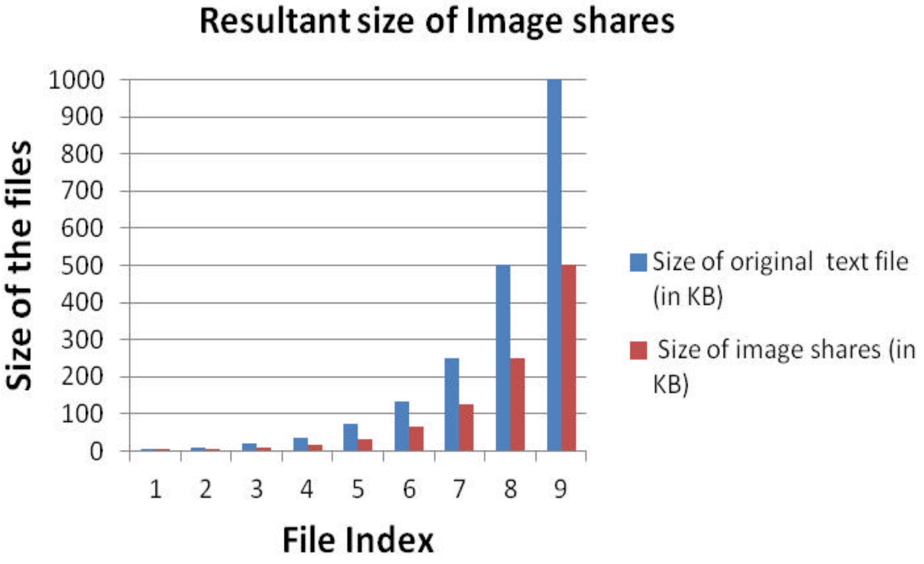

Fig. 5: Comparison of sizes of text files and image shares during encryption

out using a laptop with the configuration of 2.40 GHz, Intel core i3 processors with 4GB RAM on Windows 7 Professional Version 2. The algorithm is evaluated in various sizes of text files 5, 10, 19, 37, 133, 250, 500 and 1000 kb. The cloud service provider such as Amazon, Google drive, etc., are used to protect the data using the conventional encryption algorithm AES (Advanced Encryption Standard). Hence, the performance of algorithm is tested with parameters like size of the image shares and execution time for DOVC encryption and decryption technique with symmetric encryption algorithm AES with 128 bit key.

The test result of the sample text file for the proposed DOVC technique is as follows: the sample2.txt text file which is of size 19 kb and contains 19024 characters and converted into image shares of size 1.14 kb which contain 9512 pixels during DOVC encryption process. The resultant image shares are decrypted to obtain the original text file using DOVC technique. This technique has been tested with various text files and it is found that the size of the image share is very less when compared with the original file during the encryption process. Table 1 depicts the various size text files compared with image shares and Fig. 5 and 6 compares the size of the original text file with that of image shares. Based on the experimental result, the size of the decrypted file is found to be the same as that of the original text file.

The execution time is considered as the time taken to convert the text file into image shares during encryption and the image shares into the text file during decryption.

Table 1: Result of size of image shares during DOVC encryption technique

Size of original text file (kb)	Size of image shares (kb)
5	2
10	5
19	9
37	18
73	32
133	67
250	125
500	250
1000	500

Table 2: Execution time for encryption in DOVC and AES

Size of original text file (kb)	Execution time for DOVC (msec)	Execution time for AES (msec)
5	60	281
10	68	286
19	82	300
37	98	320
73	125	335
133	171	350
250	190	360
500	200	375
1000	213	390

The throughput of the encryption scheme is calculated as the result of the size of the image shares in kilo bytes divided by the execution time. Similarly the throughput of the decryption scheme is calculated as the result of the size of decrypted text file in kilo bytes divided by the execution time. These results are compared with the results of traditional AES algorithm with 128 bit key. Table 2 compares the encryption time for DOVC technique with that of AES and Fig. 7 shows the execution time for both the algorithms.

The encryption time for AES algorithm increases only marginally corresponding to the increase in the size of the

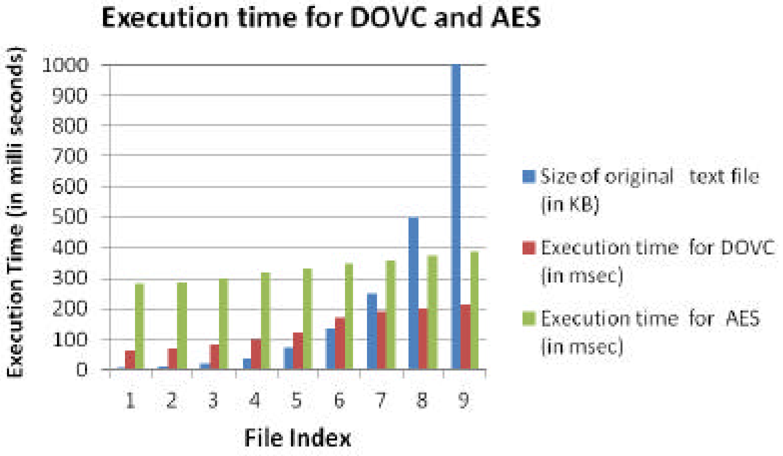

Fig. 6: Comparison of execution time for DOVC and AES encryption

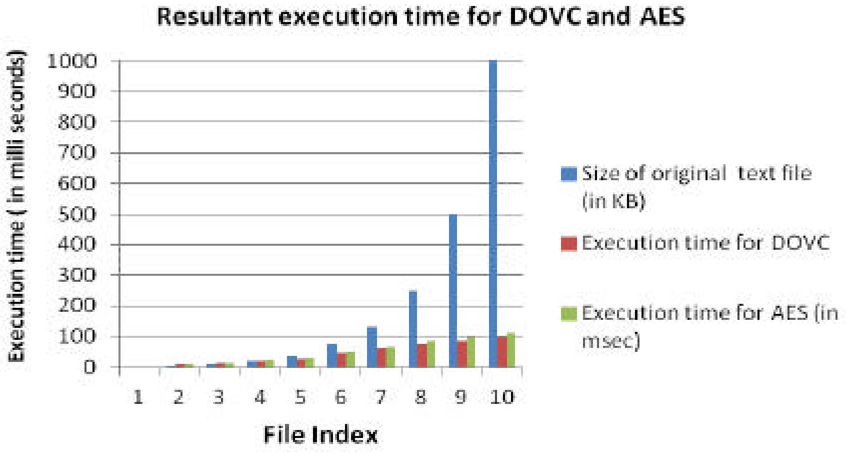

Fig. 7: Comparison of execution time for DOVC and AES decryption

Table 3: Execution time for decryption in DOVC and AES

Size of original text file (kb)	Execution time for DOVC (msec)	Execution time for AES (msec)
5	11	11
10	13	14
19	20	22
37	29	31
73	46	50
133	62	67
250	75	85
500	87	99
1000	98	109

text file. The time required for encryption in DOVC technique is less when compared with that of standard AES algorithm. This result is shown in Fig. 7. Table 3 compares the execution time for decryption process in DOVC technique with the same in the AES algorithm. The decryption time of DOVC technique is less when compared with that of AES algorithm Fig. 8 shows the resultant execution time for both the algorithms.

Table 4: Result of size of encrypted files in DOVC and AES

Size of original text file (kb)	Size of encrypted file in DOVC (kb)	Size of encrypted file in AES (kb)
5	2	5
10	5	10
19	9	19
37	18	37
73	32	73
133	67	133
250	125	250
500	250	500
1000	500	1000

Table 4 compares the size of the encrypted file in the DOVC technique with that of the standard AES algorithm. The sizes of the image shares in DOVC are very much reduced when compared with those in the AES algorithm. Figure 9 shows the resultant size of the encrypted file in the DOVC and the AES algorithms. Table 5 compares the throughput of encryption and decryption process in

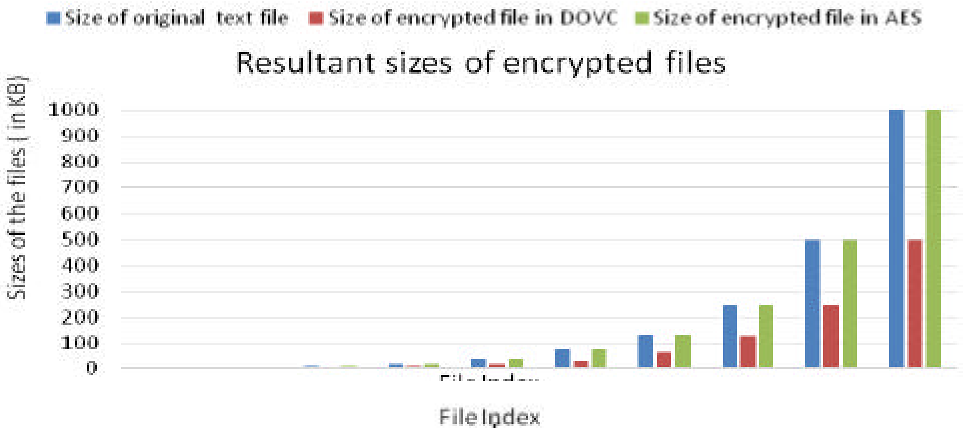

Fig. 8: Comparison of sizes of files during DOVC and AES encryption

Table 5: Encryption and decryption throughput in DOVC and AES

Size of original text file (kb)	Execution time for DOVC encryption (msec)	Execution time for AES encryption (msec)	Execution time for DOVC decryption (msec)	Execution time for AES decryption
5	60	281	11	11
10	68	286	13	14
19	82	294	20	22
37	98	296	29	31
73	125	297	46	50
133	171	298	62	67

DOVC with standard AES. The encryption and decryption speed of DOVC is high compared to that of AES. Speed of the encryption and decryption process is measured by using throughput. Throughput in DOVC and AES is specified:

- Encryption throughput (kb/msec) = ∑Text File/∑ Encryption execution time
- Encryption throughput (DOVC) = 277/604 = 0.4586 msec bit^{-1}
- Encryption throughput (AES) = 277/1752 = 0.1581 msec bit^{-1}
- Decryption throughput (KB/msec) = ∑ Text File/∑ Decryption execution time
- Decryption Throughput (DOVC) = 277/181 = 1.53 msec bit^{-1}
- Decryption Throughput (AES) = 277/195 = 1.42 msec bit^{-1}

Security: The security of visual cryptography techniqueis based upon randomness (Thien and Lin, 2002), more specifically, the randomness with which the image shares are created based on the black and white pixel patterns. This is the core security concept within visual cryptography. This means that while the shares are separate no cryptographic analysis will yield the original secret based on analysis of one of the shares. Therefore, sconsidering a 2 out of 2 visual secret sharing scheme for simplicity, one can easily draw an analogy to the one time pad cipher. One share acts as cipher text and the other share acts as the secret key. This is similar to a one time pad as each pixel on the cipher text is decoded by using the equivalent pixel on the secret key.

Complexity of DOVC: Many of the existing schemes in visual cryptography result in size of shares growing very large, depending on the image type and size. Typically as the contrast improves, the share size also increases quite dramatically. This increases the image processing time which leads to overall increase in the complexity of the schemes. It reduces the overall potential for a practical application of the existing schemes. Share sizes become completely unmanageable, specifically when high resolutions are used to share information. All the existing schemes state that hiding only a small amount of information within the shares has proven to be effective. However, if a larger amount of data is required to be shared, the share size becomes large and difficult to manage. Tracking this complexity has been a real challenge within VC. There are a number of schemes which present near optimal solutions for share sizes (Nung and Shin, 2005, 2006; Yang and Chen, 2007). The proposed DOVC technique can hide large amount of text data with less effort and time complexity but without any loss of information and confidentiality.

Time complexity of DOVC encryption process: Time required for conversion from text file to image shares = 2×n+3×n+12. Overall complexity of the encryption process = O(n).

Time complexity of DOVC decryption process: Time required for conversion from image shares into a text file = 2×n+n+5. Overall complexity of the decryption process = O(n). The time complexity of the AES algorithm is linear in terms of number of keys O(n) but exponential in terms of length of key O(2^n) (Stallings, 2003). Hence, the DOVC technique requires less time complexity when compared with currently used encryption technique AES in cloud domain.

CONCLUSION

We intend to present a novel technique to achieve data confidentiality in the cloud computing environment. The cloud service provider is considered untrustworthy and the data must be concealed not only from an outside attack but also from the provider. No one must be able to extractany meaningful information from the data. In this study we use visual cryptography technique to protect the data on the cloud avoiding the standard encryption techniques, yet we can achieve strong privacy and confidentiality of the data. The traditional visual cryptography technique has so far assured confidentiality only to image file. Here the DOVC technique proposes data confidentiality for the text file using visual cryptography technique and proves to be more efficient than the current cloud storage encryption technique such as AES in terms of storage size, time consumption and overall speed. The existing algorithm AES needs the overhead associated with key management as well as the protection of the secret key whereas the DOVC requires neither. To put it in a nutshell, the DOVC technique proves to be better than the AES technique in providing efficient confidentiality, privacy and data security.

REFERENCES

Blundo, C., A. de Santis and M. Naor, 2000. Visual cryptography for grey level images. Inform. Process. Lett., 75: 255-259.

Chavan, P.V., D. Atique and D. Malik, 2014. Design and implementation of hierarchical visual cryptography with expansion less shares. Int. J. Network Secur. Appl., 6: 91-102.

Hou, Y.C., 2003. Visual cryptography for color images. Pattern Recognit., 36: 1619-1629.

Ito, R., H. Kuwakado and H. Tanaka, 1999. Image size invariant visual cryptography. IEICE Trans. Fundam., E82-A: 2172-2177.

Jaafar, A. and A. Samsudin, 2012. A survey of black-and-white visual cryptography models. Int. J. Digital Content Technol. Appl., 6: 1-12.

Jaya, J., 2013. Securing cloud data and cheque truncation system with visual cryptography. Int. J. Comput. Appl., 70: 16-21.

Lee, K.H. and P.L. Chiu, 2012. An extended visual cryptography algorithm for general access structures. IEEE Trans. Inform. Forensics Secur., 7: 219-229.

Lin, C.C. and W.H. Tsai, 2003. Visual cryptography for gray-level images by dithering techniques. Pattern Recognit. Lett., 24: 349-358.

Moni, N. and A. Shamir, 1995. Visual Cryptography Advances in Cryptology-Eurocrypt'94. Springer, Berlin, Germany,.

Nung, Y.A.N.G.C. and T.C.H.E.N. Shih, 2005. Size-adjustable visual secret sharing schemes. IEICE. Trans. Fundam. Electron. Commun. Comput. Sci., 88: 2471-2474.

Nung, Y.A.N.G.C. and T.C.H.E.N. Shih, 2006. New size-reduced visual secret sharing schemes with half reduction of shadow size. IEICE. Trans. Fundam. Electron. Commun. Comput. Sci., 89: 620-625.

Stallings, W., 2003. Cryptography and Network Security Principles and Practice. 3rd Edn., Prentice-Hall of India Pvt. Ltd., India.

Thien, C.C. and J.C. Lin, 2002. Secret image sharing. Comput. Graph., 26: 765-770.

Wan, Z., J. Liu and R.H. Deng, 2012. HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing. IEEE Trans. Inform. Forensics Secur., 7: 743-754.

Yang, C.N. and T.S. Chen, 2007. Extended visual secret sharing schemes: Improving the shadow image quality. Int. J. Pattern Recognit. Artif. Intell., 21: 879-898.

Yang, C.N., 2004. New visual secret sharing schemes using probabilistic method. Pattern Recognit. Lett., 25: 481-494.