BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **17**, No 3
Sofia • 2017 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.1515/cait-2017-0034

Secret Image Enhanced Sharing Using Visual Cryptography

K. Brindha, N. Jeyanthi

School of Information Technology and Engineering, VIT University, Vellore 632014, Tamilnadu, India
E-mails: brindha.k@vit.ac.in njeyanthi@vit.ac.in

***Abstract*:** *In the conventional visual cryptographic scheme, an image is divided into several image shares, which are distributed among the members of a group, and the original image is retrieved by combining the shares of all the members. This secret image becomes accessible to every individual member and there is an inherent risk of any one of the members in the group using the valuable information for illegal purposes as an intruder. To overcome this problem, the proposed algorithm Secret Image Enhanced Sharing using Visual Cryptography* (*SIESVC*) *diligently facilitates any member in the group to retrieve either only a part or the complete secret image based purely on his access privilege rights only.*

***Keywords*:** *Visual Cryptography, Secret Image Enhanced Sharing using Visual Cryptography* (*SIESVC*).

1. Introduction

In the modern networking world, the internet has become the primary medium to transmit confidential information such as net banking transaction, military related data, financial document etc. However, as it is an insecure channel, many security techniques are now being used to make the communication secure and reliable over the network [1, 22]. Cryptography is one of the vital techniques, which not only provides data privacy but also ensures message integrity and authentication. However, the conventional cryptography algorithm such as DES, AES, etc., needs more computation for enciphering and deciphering the data as well as it is liable to many security attacks.

One of the new cryptographic techniques is Visual Cryptography (VC) based on secret sharing developed by Naor and Shamir, which provides more data confidentiality while it requires less computation power only. In this technique, encryption is performed by dividing the secret image into various shares and the original image is obtained by stacking of all the *n* shares. The basic model extended by using General Access Structure Scheme can be used for application, which does not believe in all entity in the process. It is further expanded by sharing of multiple

Unauthenticated
Download Date | 3/22/18 7:39 PM

secrets in a single image [2, 3] and embedding the random noisy image shares in a meaningful cover image, etc. [4].

The application of this technique on information related to Defence, Finance, Banking, etc., enables sharing of the secret information by all the members of the group. All the existing visual cryptography schemes are used to access the entire secret information and not the specific parts alone. This article proposes the Secret Image Enhanced Sharing using Visual Cryptography Scheme, which allows the user to retrieve only a specific part from the secret image based on his user authorization rights. He can access that specific part by superimposing the enciphered image on the received key image share based on his privilege rights.

The remainder of this article is organized as follows. Section 2 describes a review of related work, Section 3 discusses the threats in cloud computing, Section 4 covers the process of proposed algorithm, Section 5 discusses the experimental results and Section 6 concludes the paper.

2. Related work

Naor and Shamir [5] introduced Visual Cryptography technique at the Euro Crypt conference in 1994. It is a modern cryptographic technique, which can decode concealed images without any mathematical computations. Any user who has no knowledge of cryptography algorithm can use it effortlessly without the requirement of any computation complexity. This technique divides the original image into a number of shares, which is called encryption. Later it extracts the original image by superimposing the entire shares one over the other, which is called decryption.

2.1. Basic Visual cryptography scheme

In this scheme, each pixel will be divided into 2 sub pixels. The possible combination in the pixel division is presented in Fig. 1. It indicates three features - Share-1, Share-2 and the superimposition of Share 1on Share 2, which results in the form of entire black or partially black and white pixel.

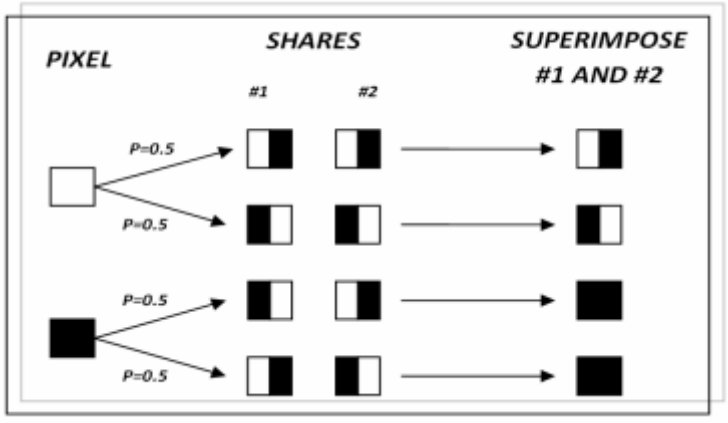


Fig. 1. Coding of Basic visual cryptography

Unauthenticated
Download Date | 3/22/18 7:39 PM

2.2. VC for Gray level images

The traditional VC scheme was limited to black and white images, which is inadequate to real time purposes. Chang-Chou Lin et al. (see [6, 8]) suggested a VC scheme for gray color images by using dithering technique. In this scheme, the gray level image is converted into black and white image shares by dithering technique. Then random noisy shares are created from them by applying traditional VC scheme. However, the drawbacks of this scheme are the increased size of image shares and the poor quality of decoded image.

2.3. VC for Color images

The innovation in VC scheme [9] advanced the quality of the image but it was found inappropriate for the color image. H o u [10] introduced a new aspect on VC for natural color images. In this scheme, the color image is converted into binary images by using primary color RGB or CMY color channels then the traditional VC scheme is applied to each channel. This scheme reduces the size of the image shares but decreases the quality of the decoded image.

2.4. Probabilistic VC scheme

In 2004, Y a n g [12] proposed the probabilistic VC scheme for secret binary image without increasing the size of the image shares. In this scheme, image shares are directly generated by using basic matrices S_1 or S_0. Encryption is accomplished by randomly choosing the column of S_1 or S_0 depending on black or white pixel. However, there is a drawback in this scheme in producing poor quality in the decoded image due to each and every pixel not being recovered properly.

2.5. Extended VC scheme

The traditional VC scheme generates random noisy pixel image shares, which reveal that some secret information is hidden in them. This problem can be overcome by applying the extended VC Scheme. In this scheme, encryption is accomplished by two steps. In the first step, the image is split into image shares and in the next step, the image shares are put into cover images [13-16, 26-28].

In an earlier article, the researcher proposed Secured Document Sharing Using Visual Cryptography (SDSUVC) and DOVC Data Obfuscation Visual Cryptography to protect cloud storage for efficient document storage, which utilizes only less storage space and less time complexity for the document retrieval and it provides data confidentiality [29, 30].

All the existing VC schemes retrieve the complete original image during decryption process. The proposed technique SIESVC (Secret Image Enhanced Sharing using Visual Cryptography) facilitates any member in the group to retrieve either only a part or the complete secret image based purely on his access privilege rights only.

Unauthenticated
Download Date | 3/22/18 7:39 PM

3. Major threats in Cloud computing

The cloud computing is one of the recent emerging techniques which can be utilized by everyone from start-ups to major technological giants like Google, Amazon, etc. In spite of several merits, there are some drawbacks due to inadequacy in its standardization [17, 18]. The various security issues are discussed in the following sub sections.

3.1. Cyber-attacks and hacking of sensitive information

Cloud computing is apparently an improvement of web services such as online storage and web hosting of information such as health record, financial information, credit card details, etc., but it faces attack from cyber thieves and intruders. They are capable of breaking the cloud computing environment and they can also steal and sell the sensitive data to different users.

3.2. Insecure API (Application Programming Interface)

Numerous Cloud Service Providers (CSP) implement API for the customers to collaborate with cloud utilities. Using the interface, CSP does provisioning, monitoring and managing the stored data of the customers. Hackers try to find loopholes in the API to manipulate access control and authentication over the assets. Hence the weak set of API results in security problems related to availability, integrity, confidentiality and accountability [7, 11, 19, 20].

3.3. Nefarious insiders

Most of the IT organizations face the security threats caused by intruders. Counteractants such as antivirus software, intrusion detection system and firewalls are imposed to overcome these threats. Yet significant deterioration to the organization is caused by nefarious insiders. The access rights allowed to an adversary can lead to fraud and stealth of confidential data and great loss to the organization thereby.

3.4. Vulnerability in Shared technologies

The main objective of cloud system is source sharing. Accesses to servers, disk partition, infrastructure, etc. are shared among numerous clients. Yet the Cloud Service Provider (CSP) intends to ensure that the clients cannot access each other’s data domain [21, 23].

3.5. Data leakage/loss

There are various reasons for data leakage or loss during cloud computing. The information in the cloud store may be deleted, altered or corrupted during some process and insufficient authorization, authentication and audit authority can lead to data leakage or loss.

Unauthenticated
Download Date | 3/22/18 7:39 PM

4. Preliminaries of the proposed system

The proposed system uses predicate encryption technique for protecting secret information and Least Significant Bits (LSB) encoding algorithm is used to embed the encrypted data to avoid the data modification. Hence, in this section the proposed system's special features and merits are discussed.

4.1. Predicate encryption

Predicate encryption is a special type of asymmetric encryption system and it was contributed by Dan Boneh and others (see [23]). One of the main feature of this algorithm is that the intended recipient can decrypt only part of the encrypted message received from the sender based on his privilege rights [24]. In predicate encryption, an encrypted message is associated with feature y and a private key associated with a predicate f and the recipient who has a private key associate with feature f can decrypt an encrypted message associated with y, if $f(y) = 1$. It is a way to limit the decryption.

4.2. Least Significant Bits encoding

The LSB encoding is a simple technique to embed the secret information into cover image. This technique replaces the position of bits in the cover image with secret image. In case of 24-bit color image, three bits of information in every pixel are replaced with information of secret image. The changes in the LSB cannot make much change in the appearance of the image. This encoding protects the integrity of the information.

5. Proposed SIESVC (Secret Image Enhanced Sharing using Visual Cryptography) technique architecture

The proposed technique SIESVC secures the cloud data storage by protecting the security key components such as integrity, confidentiality and access control and it involves three phases.

- Predicate encryption
- Embedding in cover image
- Predicate decryption

5.1. Predicate encryption

The proposed SIESVC technique can be used to implement predicate encryption for storing secret data on the cloud. Initially the random noise image share is created which is of the same size as that of the secret image. Based on the user privilege rights, the portion of the secret image is selected. Each and every pixel is retrieved from both random noise image and user key image. If both the pixels are same position then the pixel of random noise image share is XOR with the pixel of the user key image. This process is repeated for all the pixels in both the images.

Unauthenticated
Download Date | 3/22/18 7:39 PM

Finally, the encrypted image is obtained. Thus, the secret image is protected and it ensures the confidentiality.

Algorithm for Creation of Encrypted Image

Input: Secret_Image
Output: Encrypted Image

1. Size(Secret_Image) = Size(Random noise Image)
2. Retrieve the Secret token image with minimum coordinates (x_{min}, y_{min}) and maximum coordinates (x_{max}, y_{max}) based on users' privilege rights
3. Repeat I = (x_{min}, y_{min}) to (x_{max}, y_{max})
4. Select pixel X of secret token image with coordinates (x,y)
5. Select pixel X′ of random noise image with coordinates (x′, y′)
6. If (x==x′) and (y==y′)
7. (x,y) $\oplus$ (x′,y′)
8. Final resultant image is the encrypted image

Fig. 2. Algorithm for creation of Encrypted image

5.2. Embedding in Meaningful share

The encrypted image looks like the random noise image shares which can be attracted by attacker's attention. Hence the proposed SIESVC technique can be used to hide the encrypted image and the random noise image share by a cover image. The LSB encoding technique is used to cover the secret image. Hence data integrity is ensured during the data transmission.

Algorithm for embedding in Meaningful Share

Input: Encrypted_image, Random noise Share
Output: Embedding Encrypted_image, Random noise share with Meaningful cover image

1. Size (Cover_image$_1$) = Size(Cover_image$_2$)
2. Embedding Encrypted_image, Random noise image with cover image using LSB encoding
3. Final resultant image embed with secret information

Fig. 3. Algorithm for embedding in Meaningful share

5.3. Predicate decryption

The proposed SIESVC technique implements predicate decryption, which reduces the processing time of decryption. It can render protection against illegal access and loss of data. Predicate encryption allows decrypting only the part of the image based on the user's privilege rights. Hence, it ensures the access control of the legal user.

Unauthenticated
Download Date | 3/22/18 7:39 PM

Algorithm for Predicate Decryption

Input: Embedded meaningful share
Output: Secret Image

1. Remove the cover image by extracting the LSB technique
2. Repeat I = (x_{min}, y_{min}) to (x_{max}, y_{max})
3. Select pixel X of secret token image with coordinates (x, y)
4. Select pixel X′ of random noise image with coordinates (x′, y′)
5. If (x==x′) and (y==y′)
6. (x,y) ⊕ (x′,y′)
7. Obtain the final resultant image based on the user's privilege

Fig. 4. Algorithm for Predicate decryption

Let us consider an image SI which contains secrets S_1, S_2 and S_3. The random noise image share is created. The size of the random noise image share is same as that of the secret image. The secret token image is generated from the original image based on the user privilege rights. The Predicate encrypted image obtained by the secret token image is XOR with random noise share image. These random noise shares can be easily attract the attention of intruders but this can be avoided by the resulting shares being embedded into cover images and then passed among groups of users. Suppose user1 has the privilege rights to access the secret S_1. After decryption he can view the S_1 only and the remaining secrets are hidden and blank. Fig. 5 denotes the architecture of SIESVC technique.

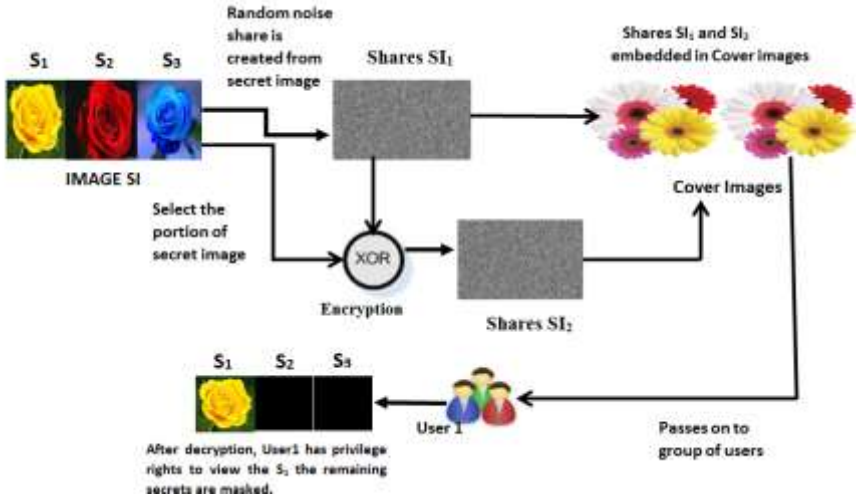
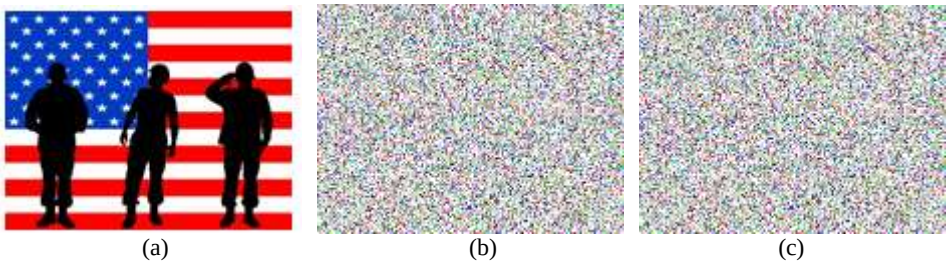


Fig. 5. Secret image enhanced sharing using Visual Cryptography technique

6. Result analysis

The proposed SIESVC technique has been tested with various sample images. The secret image is encrypted using the predicate key token image with the random noise image share. The secret image, the predicate key token image and the encrypted image shown in Fig. 6a-c.

Unauthenticated
Download Date | 3/22/18 7:39 PM



(a) (b) (c)

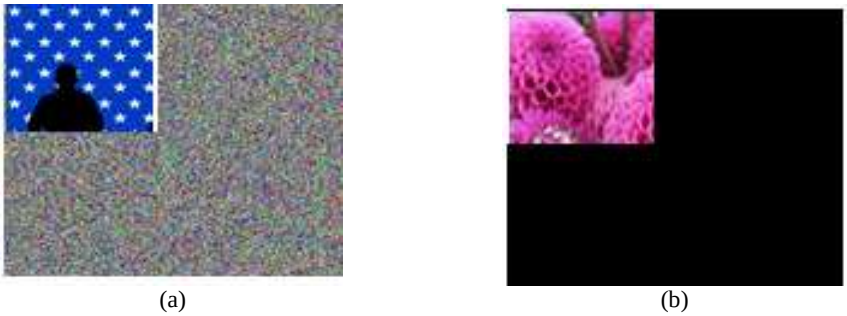
Fig. 6. Secret Image (114×154) (a); Predicate key token image (114×154) (b); Encrypted image (114×154) (c)

The predicate key token image and the encrypted image are embedded in the cover image using LSB encoding shown in Fig 7a and b.

(a) (b)

Fig. 7. Cover image (114×154) (a); Cover image (114×154) (b)

The original image (50×50) and its masked image after decryption are shown in Fig. 8a and b.



(a) (b)

Fig. 8. Part of the original image (114×154) (a); Masked Image (114×154) (b)

The result is compared with predicate encryption and decryption of various size of retrieval images of the original image size (500×500). The Table 1 indicates the time taken for the execution of predicate encryption and decryption for various sizes of retrieval images.

Unauthenticated
Download Date | 3/22/18 7:39 PM

Table 1. Execution time for predicate encryption and decryption

Retrieval Image Size	Execution time for encryption (ms)	Execution time for decryption (ms)
Size 1 (50×50)	70	65
Size 2 (50×75)	90	83
Size 3 (75×75)	150	140
Size 4 (100×100)	250	220
Size 5 (150×150)	350	330
Size 6 (250×250)	400	380
Size 7 (350×350)	550	510
Size 8 (500×500)	650	603

The comparison of the time taken for the execution of predicate encryption and decryption with various sizes of retrieval images are shown in Fig. 9.

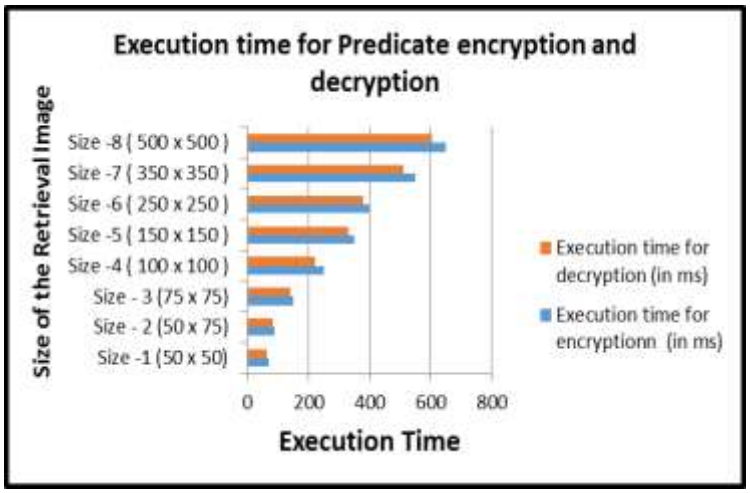


Fig. 9. Execution time for predicate encryption and decryption

The execution time taken predicate encryption and decryption decreases when the size of the retrieval image is decreased are shown in graph.

7. Security analysis

In this section, the security parameters of Secret Image Enhanced Sharing using Visual Cryptography technique will be discussed and then the performance of each operation is analysed.

7.1. Data confidentiality

Data confidentiality refers to the protection of secret data during its storage in data store or data transfer from one location to another. The proposed approach uses Visual Cryptography technique, which encrypts the secret image based on the user privilege rights into random noisy image share using predicate encryption. The

Unauthenticated
Download Date | 3/22/18 7:39 PM

random noisy share cannot reveal information to others. Hence, this approach ensures data confidentiality using predicate encryption.

7.2. Data integrity

Data integrity refers to the proper transmission and storage of data. Data integrity is preserved by the authenticated user. The encrypted images are in the form of random noisy shares. During transmission, there is a possibility to modify the content in the random noisy image shares. In this technique, the encrypted image share and the predicate token image are embedded in meaningful cover images. This incapacitates the intruders to modify the information in the encrypted data. Hence, this approach ensures data integrity.

7.3. Access control

Access control refers to the user access to the information based on his rights. In this technique, the predicate token image is created based on the user's privilege rights. The user can access only part of the image and the remaining portion of the image is masked. Hence, this technique ensures access control rights.

8. Conclusion

Many of the existing schemes in Visual Cryptography result in the 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 challenge within VC. The proposed SIESVC technique can hide large amount of secret and the user can access only part of data based on his access rights with less effort and time complexity but without any loss of information, confidentiality and data integrity.

This technique ensures total privacy, security, confidentiality and integrity without the complication of pixel expansion or change in the quality of the image. The end-user has the benefit of retrieving the image with less computational effort. The SIESVC technique has been successfully applied to image shares with defined boundaries only. Further work can be carried out on portions of image with any type of boundaries in future.

References

1. J e y a n t h i, N., N. C. S. N. I y e n g a r. An Entropy Based Approach to Detect and Distinguish DDoS Attacks from Flash Crowds in VoIP Networks. – International Journal of Network Security, Vol. **14**, 2012, No 5, pp. 257-269.

Unauthenticated
Download Date | 3/22/18 7:39 PM

2. W u, H. C., C. C. C h a n g. Sharing Visual Multi-Secrets Using Circle Share. – Computer Standards & Interfaces, Vol. **28**, 2005, No 1, pp. 123-135.
3. S h y u, S. J., S. Y. H u a n g, Y. K. L e e, R. Z. W a n g, K. C h e n. Sharing Multiple Secrets in Visual Cryptography. – PatternRecognition, Vol. **40**, 2007, No 12, pp. 3633-3651.
4. S a r d a n a, A. Multiple Secrets Sharing with Meaningful Shares. – In: International Conference on Advances in Computing and Communications, Berlin, Heidelberg, Springer, July 2011, pp. 233-243.
5. N a o r, M., A. S h a m i r. Visual Cryptography. – In: Proc. of Advance in Cryptology (EUROCRYPT'94), Lecture Notes in Computer Science, Springer-Verlag, Vol. **950**, 1995, pp. 1-12.
6. M a n d a l, S. N., S. D u t t a, R. S a r k a r. Block Based Symmetry Key Visual Cryptography. – International Journal of Computer Network and Information Security, Vol. **4**, No 9, pp. 10-19.
7. T h a n d e e s w a r a n, R., S. S u b h a s h i n i, N. J e y a n t h i, M. A. S a l e e m D u r a i. Secured Multi-Cloud Virtual Infrastructure with Improved Performance. – Cybernetics and Information Technologies, Vol. **12**, 2012, No 2, pp. 11-22.
8. L i n, C h a n g-C h o u, W e n-H s i a n g T s a i. Visual Cryptography for Gray-Level Images by Dithering Techniques. – Pattern Recognition Letters, Vol. **24**, 2003, No 7, pp. 349-358.
9. M o n d a l, U. K., S. N. M a n d a l, J. P. C h o u d h u r y, J. K. M a n d a l. A New Approach to Cryptography. – In: Proc. of International Conference Systematics, Cybernatics & Informatics (ICSCI'08), 2008, pp. 1-12.
10. H o u, Y o u n g-C h a n g. Visual Cryptography for Color Images. – Pattern Recognition, Vol. **36**, 2003, No 7, pp. 1619-1629.
11. J e y a n t h i, N., N. C. S. N. I y e n g a r. Escape-On-Sight: An Efficient and Scalable Mechanism for Escaping DDoS Attacks in Cloud Computing Environment. – Cybernetics and Information Technologies, Vol. **13**, 2013, No 1, pp. 46-60.
12. Y a n g, C. N. New Visual Secret Sharing Schemes Using Probabilistic Method. – Pattern Recognition Letter, Vol. **25**, 2004, No 4, pp. 481-494.
13. J a a f a r, A., A. S a m s u d i n. A Survey of Black and White Visual Cryptography Model. – International Journal of Digital Content Technology and its Applications (JDCTA), Vol. **6**, 2012, No 15, pp. 237-249.
14. J e y a n t h i, N., P. C. M o g a n K u m a r. A Virtual Firewall Mechanism Using Army Nodes to Protect Cloud Infrastructure from DDoS Attacks. – Cybernetics and Information Technologies, Vol. **14**, 2014, No 3, pp. 71-85.
15. B l u n d o, C., A. D e S a n t i s, M. N a o r. Visual Cryptography for Grey Level Images. – Information Processing Letters, Vol. **75**, 2000, No 6, pp. 255-259.
16. L e e, K a i-H u i, P e i-L i n g C h i u. An Extended Visual Cryptography Algorithm for General Access Structures. – IEEE Transaction on Information Forensics and Security, Vol. **7**, 2012, No 1, pp. 219-229.
17. J a y a. Securing Cloud Data and Cheque Truncation System with Visual Cryptography. – International Journal of Computer Applications, Vol. **70**, 2013, No 2, pp. 16-21.
18. **https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf**
19. **https://arxiv.org/pdf/1512.01701**
20. **http://securitylabs.websense.com/content/Blogs/3402.aspx**
21. B o l d y r e v a, A., V. G o y a l, V. K u m a r. Identity-Based Encryption with Efficient Revocation. – In: Proc. of 15th ACM Conference on Computer and Communications Security, 2008, pp. 417-426.
22. J e y a n t h i, N., R. T h a n d e e s w a r a n, J. V i n i t h r a. RQA Based Approach to Detect and Prevent DDoS Attacks in VoIP Networks. – Cybernetics and Information Technologies, Vol. **14**, 2014, No 1, pp. 11-24.
23. B o n e h, D., B. W a t e r s. Conjunctive, Subset, and Range Queries on Encrypted Data. – Theory of Cryptography, Springer, 2007, pp. 535-554.
24. K a t z, J., A. S a h a i, B. W a t e r s. Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products.– In: Lecture Notes in Computer Science, Vol. **4965**, Springer, EUROCRYPT, 2008, pp. 146-162.

Unauthenticated
Download Date | 3/22/18 7:39 PM

25. J a y a, A. S a r d a n a. Multiple Secrets Sharing with Meaningful Shares. – In: International Conference on Advances in Computing and Communications, Heidelberg, Springer, 2011, pp. 233-243.
26. Y a n g, C h i n g-N u n g T s e-S h i h C h e n. Size-Adjustable Visual Secret Sharing Schemes. – IEICE Transactions on Fundamental of Electronics, Communication and Computer Science, Vol. **88**, 2005, No 9, pp. 2471-2474.
27. Y a n g, C h i n g-N u n g, T s e-S h i h C h e n. New Size-Reduced Visual Secret Sharing Schemes with Half Reduction of Shadow Size. – IEICE Transactions on Electronics, Communication and Computer Science, Vol. **89**, 2006, No 2, pp. 620-625.
28. Y a n g, C h i n g-N u n g, T s e-S h i h C h e n. Extended Visual Secret Sharing Schemes: Improving the Shadow Image Quality. – International Journal of Pattern Recognition and Artificial Intelligence, Vol. **21**, 2007, No 5, pp. 879-898.
29. B r i n d h a, K., N. J e y a n t h i. Secured Document Sharing Using Visual Cryptography to Protect Cloud Data Storage. – Cybernetics and Information Technologies, Vol. **15**, 2015, No 4, pp. 111-123.
30. B r i n d h a, K., N. J e y a n t h i. DOVC: Data Obfuscation Visual Cryptography to Protect Cloud Storage. – International Journal of Soft Computing, Vol. **11**, 2016, No 6, pp. 374-381.

Unauthenticated
Download Date | 3/22/18 7:39 PM