Efficiency Privacy Preservation Scheme for Distributed Digital Document using Cache-Cache Mechanism

Shiny Malar F.R.
Dept. Of Computer Science & Engineering
Noorul Islam University, Kumaracoil
Kanyakumari District, India

Jeya Kumar M.K
Dept.Of Computer Application
Noorul Islam University, Kumaracoil
Kanyakumari District, India

ABSTRACT

In data mining, Privacy preservation plays a major role to provide an efficient communication for the users. Several methods have been employed for privacy preservation scheme they are Secured Multiparty Computation (SMC), Data Transformation Technique (DTT) and Cryptographic Technique. Most of the recent works concentrated on SMC and DTT as the data mining sources are mainly distributed in nature. However cryptographic techniques need more overhead for preserving privacy in distributed data mining context. All these existing techniques are worked and concentrated on data sharing and not concerned about the privacy preservation between the participants on distributed data mining. To address these issues more sensitively, in this work, present a privacy preservation scheme using cache-cache mechanism for distributed digital document which includes text, images, etc.,. In the proposed effective privacy preservation scheme for distributed digital document using cache-cache mechanism [PPS-CCM], digital document sharing is done with cache-cache mechanism to reduce the overhead on increasing document sizes. The cache-cache mechanism maintains a cache inside a cache to preserve the details about the users who shared the secret parts of digital document which has been splitted in a scheme of visual cryptography. An experimental evaluation is done with sample set of digital documents and will be processed with the proposed PPS-CCM to estimate the performance of the proposed work in terms of privacy overhead, intensity of cache-cache for digital document sharing, Participant density with an existing texture overlapping and Fourier filtering schemes for color images in visual cryptography.

Keywords

Privacy preservation, Cache-cache mechanism, Digital document (DD), Visual cryptography, distributed data, Secure Multi party computation, Color images.

1. INTRODUCTION

Secure multi party computation is one of a sub field of cryptography. The major goal of the secure multi party computation methods are to enable parties to mutually compute a function over their inputs, while at the same time keeping these inputs are private. In current years, data mining has been analyzed as a hazard to privacy since, the extensive propagation of electronic data preserved by corporations. This has guide to enlarged distress about the isolation of the fundamental data. In modern years, a number of strategies have been presented for adapting or changing the data in such a way so as to conserve privacy. Reviews on some of the strategies used for privacy-preserving data mining are also being examined. Nowadays, online data sharing plays a major role across several application areas to intimate the data to be shared which they want. It is necessary for the user to register their personal information to share their data online for a secure communication. So, there is a great extent of data to be attacked and can also be accessed by some other adversaries. To protect the data to be shared, several techniques have been presented by several authors.

Privacy-preserving data mining has abundant applications in observation which are logically stranded to be “privacy-violating” requests. The solution is to propose methods which persist to be efficient, without confessing security. Some methods for privacy calculation utilize some figure of transformation on the data in organize to achieve the privacy preservation. Classically, such methods decrease the granularity of illustration in order to diminish the privacy. This decrease in granularity results in some defeat of efficacy of data organization or mining algorithms. This is the normal trade-off among information loss and isolation. Some illustrations of such strategies are randomization methods, k-anonymity model and l-diversity, Distributed privacy preservation, Downgrading Application Effectiveness.

To deal with privacy preservation problem, Cache, a common strategy for a class of location-based services that allows users to have the benefit of the services while diminishing the related privacy concerns. Cache obtains a well-explored idea from dispersed systems, explicitly caching, and relates it in the framework of privacy. Cache has two interior ideas: (1) location-enhanced contented can be sometimes pre-fetched in great geographic mass onto a device previous to it is really needed, and (2) the content can be admitted nearby on a device when it is really needed, without relying on any networked services exterior of the device. Thus, relatively than distributing present location on each demand for information, the user only wants to divide common desired content.

Visual Cryptography an encryption method permit obscure is probable only if the appropriate key is abounded by the user. Decryption can be achieved without the interference of the computer. It works on the standard that when an image is dividing into k shares simply the user who contains all the k shares can decrypt the message; any k-1 shares seize by the user does not enclose any practical information. To realize Visual Cryptography in a privacy preservation scheme, transparent sheet should be selected. This paper is well thought-out as follows; Section 2 deals with the review of literature. Section 3 described about the effective privacy preservation scheme for distributed digital document using cache-cache mechanism. Section 4 and 5 offered to Experimental evaluation and result and discussion .Finally the conclusion of this paper in Section 6.

2. LITERATURE REVIEW

A number of novel methods for visual cryptography have been presented recently a lot in the literature. An important issue in secure multi-party computation is the definition of security. Initially the SMC was suggested by Andrew C. Yao as solution to the millionaire's problem in the year 1982 [1]. The blind signatures can be applied to one of the key problem domains, which are protocols for privacy preserving electronic cash. This idea of the blind signatures as a form of multi party computation was offered by D. Chaum [2] in the year 1982. In 1983, Manuel Blum [3] has proposed Extends the Diffie-Hellman key exchange protocol to subjective multi-party computations. A method for ensuring that a random coin-flip is exactly computed by multiple parties via an anxious phone line is presented. Theoretical analysis guarantees that the outcome of the coin-flip will be accidental. In 1986 [4], A. Yao was extended their earlier work that formalizes the notion of secure multiparty protocols for secret sharing. In the first solution in 1987, Goldreich, Micali and Wigderson [5] showed that in a synchronous system with cryptography a majority of honest processes can simulate a centralized trusted third party. In 1988 [6], Michael Ben-Or and Avi Wigderson have Proves completeness theorems about multi-party protocols in the information theoretic sense. More than half of the co-owners must work together to ever learn final information or output, if everyone should act truthfully. In the same year, David Chaum, Claude Cropeau, and Ivan Damgard have predicted entirety theorems for secure multiparty protocols in spite of computational power. More than three co-owners must join together to break any realistic multiparty protocol [7].

In 1993[8], Michael Ben-Or, Ran Canetti, and Oded Goldreich have predicted the concept of asynchronous multiparty computation and examines security issues surrounding it. A protocol for securely accumulating the results of computation accross multiple parties using a quasi-commutative one way hash function was introduced by Josh Cohen Benaloh and Michael de Mare in the year 1994 [9].In 1996 [10], Ran Canetti, Uri Feige, Oded Goldreich, and Moni Naor have Identified the shortcoming in previous multi-party computation work arrising from the introduction of adaptive adversarys, who choose to corrupt involved parties dynamically during the computation. In 2000 by researchers from different groups used the title "Privacy Preserving Data Mining" [11, 12]. The best contrast k-out-of-n scheme to progress the dissimilarity loss problem in the reconstructed images is proposed in [13]. The visual color cryptography are also has been processed using the progressive technique [14]. The progressive mechanism views also be done with the sensitive images [15] and has been processed across the data on pattern recognition process.

Many of the protocols based on encryption use the idea introduced by Yao [16]. After decrypting the image using visual cryptographic technique, the secrets sharing schemes are processed with aspect ratio invariant [17] with minimal n umber of pixel expansion. The visual cryptography schemes are also be integrated with the Halftone mechanism [18] and the decrypted images are halftone and processed. The visual cryptography schemes are used with homogeneous secret set of images using Cheating Prevention Scheme [19]. Halftone visual cryptography is also being done with error diffusion [20]. The visual cryptography schemes are also being done with the optimal threshold values [21]. In their cheating method, the cheater needs to know the exact distribution of black and white sub pixels of the shares of honest participants. Based on this characteristic, they proposed a cheat-preventing method to prevent the cheater [22] from obtaining the distribution by cache replacement algorithms [23]. The hierarchical error diffusion [24] and Distributed hash table (DHT) algorithms [25] have been planned to progress the explore effectiveness by planning the catalog of a file to an exclusive peer based on predefined hash functions for network sharing environment.In this work, for a privacy preservation scheme in a digital document sharing environment used cache-cache mechanism, which provides a secure communication over the network.

3. EFFECTIVE PRIVACY PRESERVATION SCHEME FOR DISTRIBUTED DIGITAL DOCUMENT USING CACHE-CACHE MECHANISM

The proposed privacy preservation mechanism is efficiently designed for distributed digital document sharing using cache-cache meachanism. The proposed effective privacy preservation scheme for distributed digital document using cache-cache mechanism [PPS-CCM] comprises of two operations. The first operation implies the process of converting the digital document includes text, image, etc., into image and split the converted image using visual cryptography scheme. The second operation is to perform the privacy preservation mechanism using cache-cache to attain a secure digital document sharing across distributed data mining. The process of the proposed PPS-CCM is shown in figure 1.

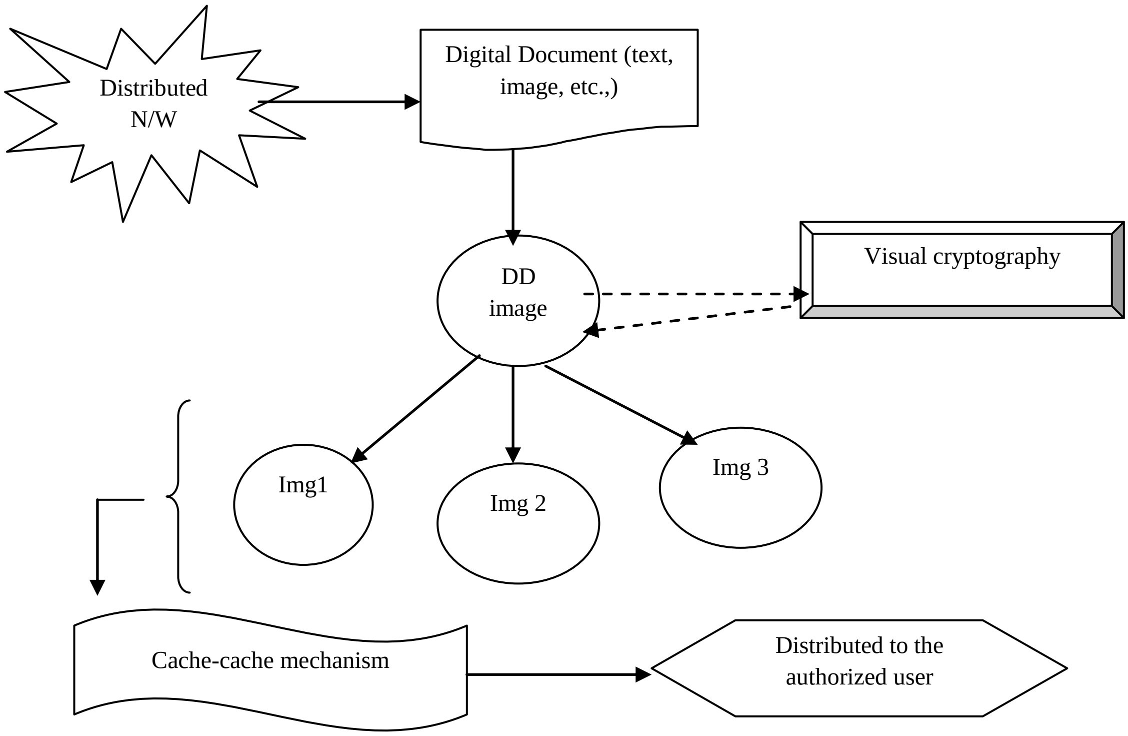

Figure 1: Process of PPS-CCM

The first phase describes the process of changing the given digital document into image. Then use a visual cryptography mechanism into the converted image to split the image into different parts. Given an image, the pixels contained in it are split into further blocks. The pixels are divided into 2 * 2 black and white sub pixels. In order to encode the secret we have to split the actual image into n different shares in such a way that n different shares consists of equal number of white and black blocks. If a pixel is divided into two halves, then the one half refers to the black portion and the other half represents the white portion.

The second phase describes the process of privacy preservation scheme for a image which has been splitted based on visual cryptography and distributed to the user based on the cache-cache mechanism (CCM). The CCM describes the process of maintaining the user's privacy information in the cache which has been hold by another cache. Thus based on CCM, it is easy to identify the users who are keeping the splitted part of the image done by visual cryptography.

From the figure3.1, the process of the proposed PPS-CCM is explained briefly under subsections. At first, the given digital document is converted into an image and the visual cryptography mechanism is applied to the image to obtain the splitted parts of the converted image. Then apply cache-cache mechanism to the given image to perform the privacy preservation scheme in a reliable manner.

3.1 Visual Cryptography scheme for a Digital Document

Given a digital document includes text, image, etc., it is converted into an image for sharing the image with the other users present in the distributed network environment in a secure manner. After converting into an image, visual cryptography mechanism is applied to split the given image into different parts. The visual cryptography mechanism to a digital document is shown in figure 2.

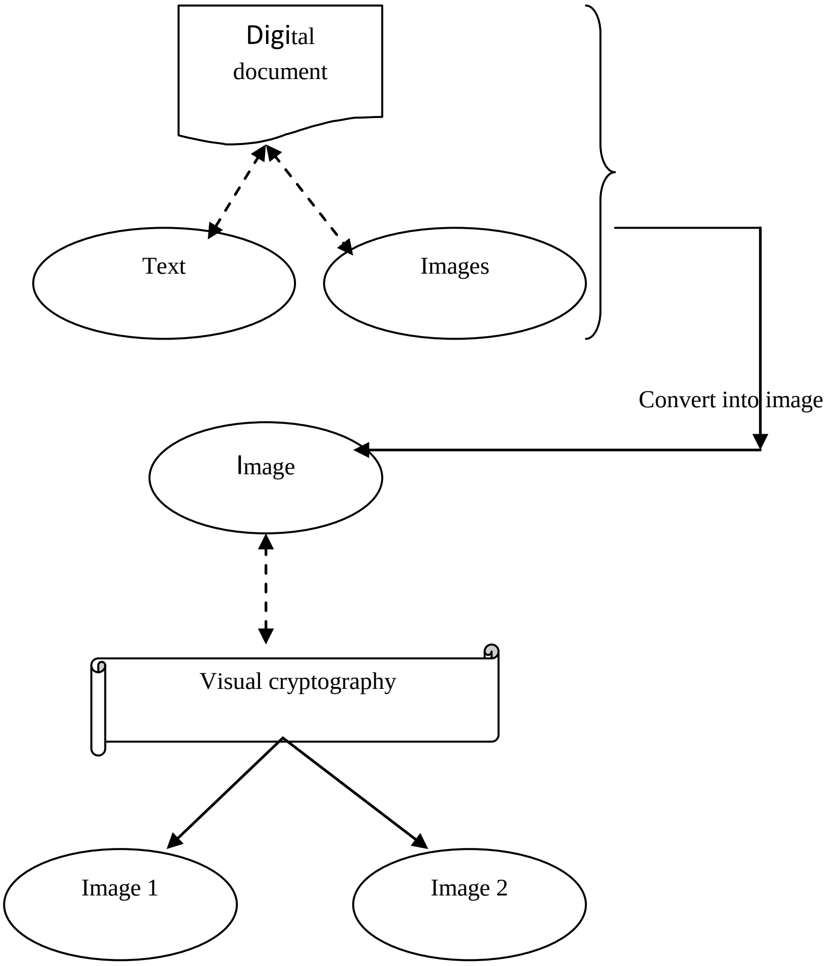

Figure 2: Process of VC in digital document

Every digital document can be presented as an image, and then that the image is simply be a set of black and white pixels i.e. it is generalized to be a binary image. Each original image pixel presents in n shares of the image, one for each transparency. Each share image comprises of m black and white sub-pixels. For every share of sub-pixels is printed on the transparency in close proximity, the resulting construction can be presented by a Boolean matrix $M = (m_{ij})_{n\times m}$ where $m_{ij} = 1$ if and only if the j-th sub-pixel of the i-th share is black. Normally, R_0 refer to the built M when the pixel in the exact image is white, and probably R_1 refers to the pixel in the exact image is black.

The visual cryptography for a given image can be clearly illustrated by a 2 out of 2 visual cryptographic scheme. Define the 2*2 matrices:

$$M_o = \begin{pmatrix} 1\,1\,0\,0 \\ 1\,1\,0\,0 \end{pmatrix}$$

$$M_1 = \begin{pmatrix} 1\,1\,0\,0 \\ 0\,0\,1\,1 \end{pmatrix}$$

The six patterns of shares created based on the above matrices are shown in figure 1. Note that one pixel of the original image now corresponds to four pixels in each share. A visual cryptography scheme

1) If the pixel of the exact image is white, arbitrarily pick the same pattern 0 of four pixels for both shares.

2) If the pixel of the exact image is black, pick a complementary pair of patterns, i.e., the patterns from the same column.

The procedure below described the process of VC in digital document

Step 1: Digital Document (DD) as input.

Step 2: Convert DD into image i

Step 3: Apply VC to image i

Step 4: Split the image i into i1, i2... in

Step 5: Preserve the splitted parts of image i1, i2…in

Step 6: End

Step 7: Splitted parts of DD as images (output)

As an input, digital document is given. The next step is to convert the digital document into an image. The visual cryptographic technique is used to encode the image by splitting up into different parts. The image is splitted based on pixels presents. These splitted parts of the image are shared by the user using cache-cache mechanism for privacy preservation scheme.

3.2 Cache- Cache Mechanism for Privacy Preservation Scheme

The Cache-Cache mechanism is used here with the visual cryptography process for privacy preservation mechanism. The Cache-Cache mechanism will maintain the information about the users who share the splitted parts of the image and the Cache-Cache share the image without disclosing the privacy data. The Cache-Cache mechanism uses cache itself to fetch the needed information of the system based on the user shares. The splitted image are distributed to the user whoever want a share in a secure manner by verifying it with the cache storage.

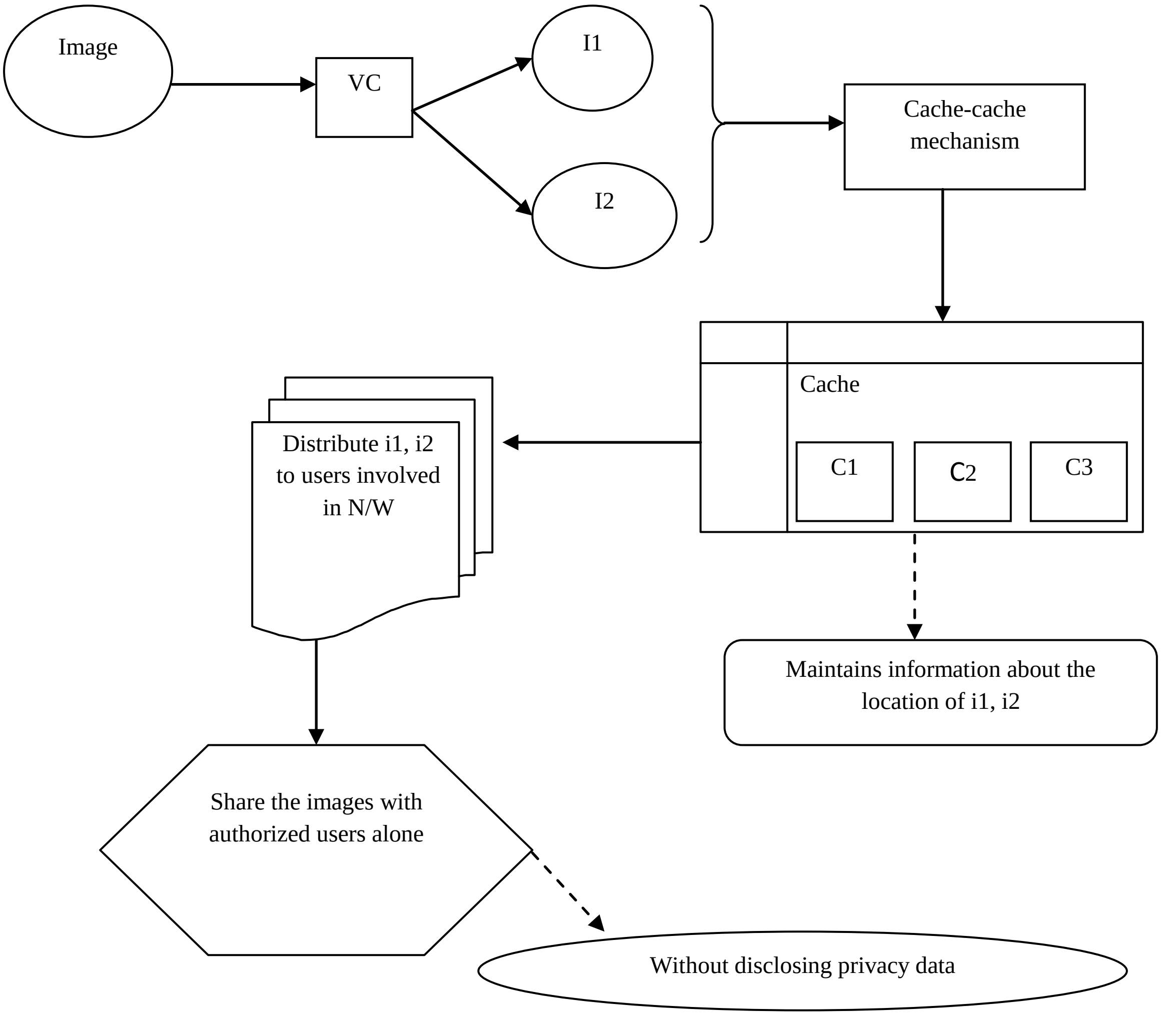
Image
VC
I1
I2
Cache-cache mechanism
Cache
C1
C2
C3
Distribute i1, i2 to users involved in N/W
Maintains information about the location of i1, i2
Share the images with authorized users alone
Without disclosing privacy data

Figure 3: Process of CCM for privacy preservation scheme

The process of cache-cache mechanism is to maintain information about the user who is having the splitted parts of the images which are partitioned by visual cryptography. The procedure below describes the process of the cache-cache mechanism for privacy preservation scheme of digital document.

Input: DD, cache, image

Step 1: Procedures followed in section 3.2

Step 2: The cache-cache mechanism uses cache inside a cache

Step 3: After partitioning of images,

Step 4: Distribute the image into different types of user involved in the network Communication

Step 5: End

Step 6: For each User Ui

Step 7: Register the personal information in cache

Step 8: Register which splitted part of an image user holds

Step 9: End For

Step 10: User share the image without disclosing their privacy data

Step 11: End

The above figure3 presents the CCM for privacy preservation scheme. The cache maintains the details about the image and the user who is sharing the image part with put disclosing their privacy data. By using CCM, the privacy preservation scheme is efficiently achieved.

4. EXPERIMENTAL EVALUATION

In this paper, the experimental simulation is conducted by using the image processing software package (MATLAB). The digital document is given as input which includes text, image etc. The digital document is converted into RGB image and is stored in MATLAB as an M- by- N-by-3 data array that defines red, green, and blue color components for every individual pixel. The color of each and every pixel is defined by the combination of the red, green, and blue intensities stored in each color plane at the pixel's location.

During the experiment, digital document is taken as input image. Here we used (2, 2) VCS scheme and consider the Lena color image of size 256 X 256 for experimental results. This input image is multiplied in a pixel-by-pixel model. In the encryption process every secret pixel is splitted into two shares. Each share belongs to the corresponding share image. In the decryption process the two corresponding shares are joined together by using OR operation to retrieve the secret pixel. For privacy preservation scheme, CCM is used to maintain all the details about the splitted image and the user for a secure communication. The performance of the proposed PPS-CCM is measured in terms of

- Privacy overhead,
- Intensity of cache-cache for digital document sharing,
- Participant density

5. RESULTS AND DISCUSSION

In this section, some experimental results to illustrate the effectiveness of the proposed PPS-CCM. The scheme proposed generates high quality of secured decrypted share using cache-cache mechanism. To evaluate the performance of the proposed PPS-CCM, it is illustrative to compare the proposed methods with previous texture overlapping and Fourier filtering schemes for color images in visual cryptography. VC can be indulged as a particular case in our proposed PPS-CCM methods, which means no visual information is carried by the share.

In existing texture overlapping and Fourier filtering schemes for color images in visual cryptography, shares carry visual information and there is a transaction among the contrast of the restructured image and the contrast of the share image. This transaction is analogous to the transaction among the distinction of the renovated image and the privacy preservation scheme of the proposed PPS-CCM methods. Compared with the existing texture overlapping and Fourier filtering schemes for color images in visual cryptography (TOFS), the proposed PPS-CCM method achieves better privacy preservation scheme. The below table and graph describes the performance of the proposed PPS-CCM method.

Table 1. Participant density vs. Privacy overhead

Participant Density	Privacy overhead	
	Proposed PPS-CCM	Existing TOFS
10	5	15
20	8	18
30	12	25
40	16	34
50	19	40

Table 1 described the privacy overhead occurred when more number of participants involved. The outcome of the proposed effective privacy preservation scheme for distributed digital document using cache-cache mechanism [PPS-CCM] is compared with an existing texture overlapping and Fourier filtering schemes for color images in visual cryptography (TOFS).

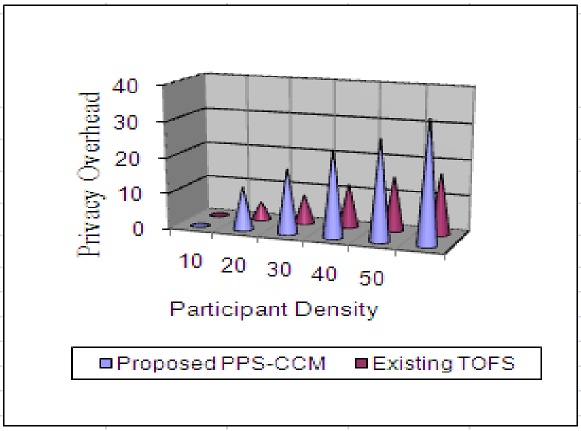

Figure 4: Participant densities vs. Privacy overhead

Figure 4 described the process of privacy overhead arise when more number of participants involved in a secure communication. The proposed PPS-CCM used VC mechanism for image decryption in a reliable manner. After decrypting the given image, the proposed used cache-cache mechanism for privacy preservation scheme i.e., cache maintains a cache inside for maintaining the privacy data of the user and the details of the location of the image i.e., which user keeps the image which is splitted by VC method. The privacy overhead is measured in terms of number of lost information which could be done by adversaries. When participant density increases in some amount, the privacy overhead in the proposed PPS-CCM is less since it maintained a cache inside a cache for maintaining the location of the image by the user. The variance in the privacy overhead is 40-

50% low in the proposed PPS-CCM compared to an existing TOFS.

Table 2. No. of images vs. Intensity of cache

No. of images	Intensity of cache-cache for digital document sharing	
	Proposed PPS-CCM	Existing TOFS
2	12	5
4	18	8
6	24	12
8	28	15
10	34	17

Table 2 described the intensity of cache maintained when more number of image are splitted by VC. The outcome of the proposed effective privacy preservation scheme for distributed digital document using cache-cache mechanism [PPS-CCM] is compared with an existing texture overlapping and Fourier filtering schemes for color images in visual cryptography (TOFS).

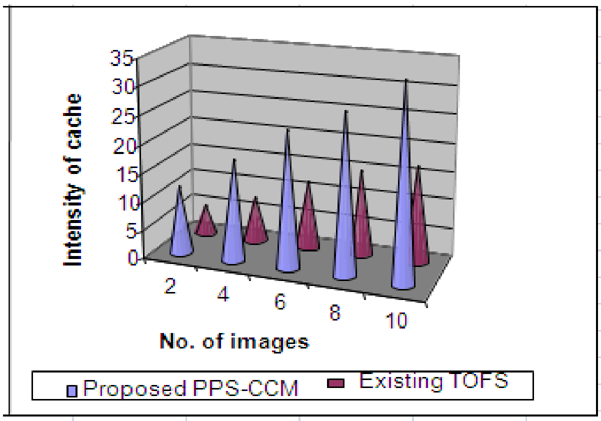

Figure 5: No. of images vs. Intensity of cache

Figure5 described the process of intensity of cache maintained by the cache using cache mechanism. The proposed PPS-CCM used VC mechanism for image decryption done in a reliable manner. After decrypting the given image, the proposed used cache-cache mechanism for privacy preservation scheme i.e., cache maintains a cache inside for maintaining the privacy data of the user and the details of the location of the image i.e., which user keeps the image which is splitted by VC method. The intensity of cache is measured in terms of number of information maintained by each cache. When participant density and the image splitter by VC method increases in some amount, the intensity of cache in the proposed PPS-CCM is high since it used a cache inside a cache for maintaining the location of the image by the user. The variance in the intensity of cache is 45-50% high in the proposed PPS-CCM compared to an existing TOFS.

Table 3. Participant density vs. Privacy preservation rate

Participant Density	Privacy preservation rate (%)	
	Proposed PPS-CCM	Existing TOFS
10	15	2
20	20	9
30	28	13
40	39	17
50	45	19

Table 3 described the privacy preservation performance scheme when more number of participants involved. The outcome of the proposed effective privacy preservation scheme for distributed digital document using cache-cache mechanism [PPS-CCM] is compared with an existing texture overlapping and Fourier filtering schemes for color images in visual cryptography (TOFS).

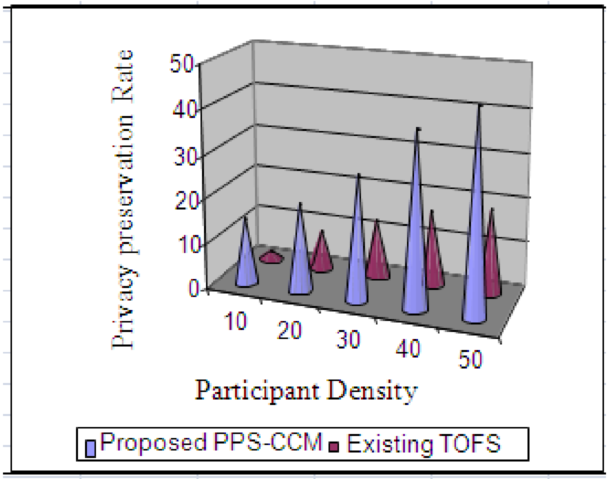

Figure 6: Participant densities vs. Privacy preservation rate

Figure 6 described the process of privacy preservation rate when more number of participants involved in a secure communication. The proposed effective privacy preservation scheme for distributed digital document using cache-cache mechanism used VC mechanism for image decryption in a reliable manner. The CCM maintains a cache inside for maintaining the privacy data of the user and the details of the location of the image i.e., which user keeps the image which is splitted by VC method. The privacy overhead is measured in terms of number of lost information which could be done by adversaries. When participant density increases in some amount, the privacy preservation rate in the proposed PPS-CCM is less since it maintained a cache inside a cache for maintaining the location of the image by the user. The variance in the privacy preservation is 70-80% high in the proposed PPS-CCM compared to an existing TOFS.

Finally, it is being known from the experimental results is that the proposed PPS-CCM efficiently achieved the privacy preservation scheme for digital document sharing in a distributed data mining process. The privacy preservation is done through cache which maintains the details about the location of the image after which has been splitted into diverse part of the image by VC mechanism.

6. CONCLUSION

The previous methods for color visual cryptography for privacy preservation scheme to digital document are not satisfactory in terms of producing either meaningless shares or meaningful shares with low visual quality, leading to loss of privacy data while sharing. In the existing texture overlapping and Fourier filtering schemes for color images in visual cryptography (TOFS) of color VC the quality of images being re-established depends on error dispersion, other image degradations due to shadowing, alteration and overlapping were not gripped in it. The proposed effective privacy preservation scheme for distributed digital document using cache-cache mechanism [PPS-CCM] enhances the privacy preservation scheme by using the cache-cache mechanism which maintains all the details about the location of the image without disclosing the privacy data of the user. The proposal in our work improves the image quality on restored original image from visual cryptic shares by presenting an efficient color image visual cryptic scheme and the privacy preservation of digital document sharing is also being done at the network environment in a secure manner.

7. REFERENCES

[1] C. Yao. Protocols for secure computations (extended abstract). In 23rd Annual Symposium on Foundations of Computer Science. IEEE, 1982.

[2] D. Chaum. Blind signatures for untraceable payments. In Proceedings of Advances in Cryptology, pages 199-203. Plenum Press, 1982.

[3] Manuel Blum. Coin flipping by telephone a protocol for solving impossible problems. SIGACT News, 15(1):23-27, 1983.

[4] A. Yao. How to generate and exchange secrets. In Proceedings of the twenty-seventh annual IEEE Symposium on Foundations of Computer Science, pages 162-167. IEEE Computer Society, 1986.

[5] O. Goldreich, S. Micali, and A. Wigderson. How to play ANY mental game. In Proceedings of the nineteenth annual ACM conference on Theory of computing, pages 218-229. ACM Press, 1987.

[6] Michael Ben-Or and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In Proceedings of the twentieth annual ACM symposium on Theory of computing, pages 1-10. ACM Press, 1988.

[7] David Chaum, Claude Cropeau, and Ivan Damgard. Multiparty unconditionally secure protocols. In Proceedings of the twentieth annual ACM symposium on Theory of computing, pages 11-19. ACM Press, 1988.

[8] Michael Ben-Or, Ran Canetti, and Oded Goldreich. Asynchronous secure computation. In Proceedings of the twenty-fifth annual ACM symposium on Theory of computing, pages 52-61. ACM Press, 1993.

[9] Josh Cohen Benaloh and Michael de Mare. One-way accumulators: A decentralized alternative to digital signatures. Lecture Notes in Computer Science, 765:274-286, 1994.

[10] Ran Canetti, Uri Feige, Oded Goldreich, and Moni Naor. Adaptively secure multi-party computation. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pages 639-648. ACM Press, 1996.

[11] R. Agrawal and R. Srikant. Privacy-preserving data mining. In Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data, May 16-18, 2000, Dallas, Texas, USA, pages 439–450. ACM, 2000.

[12] Y. Lindell and B. Pinkas. Privacy preserving data mining. In Advances in Cryptology (CRYPTO'00), volume 1880 of Lecture Notes in Computer Science, pages 36–53. Springer-Verlag, 2000.

[13] InKoo Kang, Member, IEEE, Gonzalo R. Arce, Fellow, IEEE, and Heung-Kyu Lee, Member, IEEE," Color Extended Visual Cryptography Using Error Diffusion," IEEE Transactions on image processing, vol. 20, no. 1, pp. 132-145, January 2011.

[14] D. Jin, W. Q. Yan, and M. S. Kankanhalli, "Progressive color visual cryptography," J. Electron. Imag., vol. 14, no. 3, p. 033019, 2005.

[15] W. P. Fang and J. C. Lin, "Progressive viewing and sharing of sensitive images," Pattern Recogniti. Image Anal., vol. 16, no. 4, pp. 632–636, 2006.

[16] A. C. Yao. How to generate and exchange secrets. In Proceedings of the entyseventh annual IEEE Symposium on Foundations of Computer Science, pages 162–167. IEEE Computer Society, 1986.

[17] C. N. Yang and T. S. Chen, "Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion," Pattern Recogniti. Lett., vol.26, pp. 193–206, 2005.

[18] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography,"IEEE Trans. Image Process., vol. 18, no. 8, pp. 2441–2453, Aug. 2006.

[19] D.S. Tsai, T.H. Chen, G. Horng, "A Cheating Prevention Scheme for Binary Visual Cryptography with Homogeneous Secret Images," Pattern Recognition, Vol. 40, No. 8, pp. 2356-2366, 2007.

[20] Zhongmin Wang, Gonzalo R. Arce,, and Giovanni Di Crescenzo ,"Halftone Visual Cryptography Via Error Diffusion",IEEE Transactions on information forensics and security, Vol. 4, No. 3, 383-395, September 2009.

[21] Zhen He ,"Hierarchical Error Diffusion", IEEE Transactions on image processing, Vol. 18, No. 7, pp. 1524-1534, July 2009

[22] Dash,A. Demsky,B., "Integrating Caching and Prefetching Mechanisms in a

DistributedTransactionalMemory", IEEE Transactions on Parallel and Distributed Systems, **Volume:** 22 , Issue: 8¸ 2011

[23] Kharbutli,M. , Yan Solihin et. Al., "Counter-Based Cache Replacement and Bypassing Algorithms", IEEE Transactions on Computers, **Volume:** 57 , Issue: 4¸ April 2008

[24] C. Blundo, P. D.Arco, A. De Santis, and D. R. Stinson, "Contrast Optimal Threshold Visual Cryptography Schemes" , SIAM J. on Discrete Math. 16, pp. 224-261, 2003.

[25] Wang,C. Xiao, L. et. Al., "DiCAS: An Efficient Distributed Caching Mechanism for P2P Systems", IEEE Transactions on Parallel and Distributed Systems, **Volume:** 17 , Issue: 10¸ oct., 2006