Research Journal of Applied Sciences, Engineering and Technology 10(5): 495-503, 2015
DOI:10.19026/rjaset.10.2456
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: June 14, 2014 Accepted: July 19, 2014 Published: June 15, 2015

Research Article

Secured Privacy Preserving Mechanism for Distributed Digital Documents

[1]F.R. Shiny Malar and [2]M.K. Jeyakumar
[1]Department of Computer Science and Engineering,
[2]Additional Controller of Examination, Noorul Islam University, Kumaracoil, Tamil Nadu, India

Abstract: The increasing availability of internet and digital imaging knowledge has given rise to the secret image sharing and visual cryptography. The unauthorized nature of data and sharing control systems, breach their privacy. To address this issue, a very efficient and robust visual cryptography scheme called, securitizing visual cryptography using error transmission technique. First, an efficient color image visual cryptic filtering scheme to improve the image quality on restored original image from visual cryptic shares. Fourier transformation and texture overlapping is applied to normalize the unevenly transformed share pixels on the original restored image. Second, privacy preservation using cache-cache mechanism which maintains cache inside a cache to preserve details about the users who shared the secret parts of digital document which has been split using visual cryptography is presented. Third, to enhance security for distributed file sharing in visual cryptography, binary spanning trees are used. Privacy of file sharing is performed with file block id relating to the participant id using binary trees. Finally, providing security and to achieve good quality of reconstructed image, error transmission technique is introduced. Experimentation carried out with bench mark data sets of real and synthetically generated data sets estimate the performance of Secured Privacy Preserving Mechanism for distributed digital document (SPPM) in terms of visual quality, time taken to read the text, security level.

Keywords: Cache-cache mechanism, error transmission technique, image quality, privacy preservation, visual cryptography

INTRODUCTION

Initially, in Naor and Shamir (1995) have predicted security technique named visual cryptography (Che-Wei and Wen-Hsiang, 2012). In visual cryptography, binary secret image is alternatively arranged into indiscriminate binary patterns, comprising of n shares in k-out-of-n scheme. The 'n' shares are distributed to 'n' participants in a way that each participant share is not known to other participant. With the increasingly and upcoming part of electronic commerce, there is a stronger appeal to solve the crisis related in today's open network environment. The encrypting systems of traditional cryptography mechanism are used to safeguard information security. Privacy-preserving data mining has abundant applications in observation, which are logically standard to privacy-violating requests.

Some methods for privacy factor utilize certain amount of transformations involved on the part of data to achieve privacy. Cache obtains well-explored idea from dispersed systems, explicitly caching and finally relating it in the framework of privacy. One of the few applications involved in visual cryptography is secure multiparty copy right protection. The prime objective of secure multi party computation is to enable parties to mutually compute a function over their inputs, at the same time keeping these inputs as private. In current years, Color image visual cryptic filtering method is presented for deblurring effect on the non-uniform distribution of visual cryptic share pixels. Texture overlapping filters decide which part of input image to be patched with output texture.

Privacy of the owners is preserved using cache-cache mechanism with visual cryptography for distributed digital document. While employing filter mechanism, though pixels were considered the image quality was enhanced using texture overlap and Fourier filtering, this remove the noise present in the image using CMY color model. All information of the users is preserved for distributed digital document using cache-cache mechanism, who shared the secret parts of digital document which has been split using visual cryptography for digital document sharing, between the peer users. The distributed file for distributed data sharing using visual cryptography model further enhances the process of security by deploying distributed key model and binary spanning tree.

LITERATURE REVIEW

In Jin *et al*. (2005) have introduced color visual cryptography scheme. But this method resulted in

Corresponding Author: F.R. Shiny Malar, Department of Computer Science and Engineering, Noorul Islam University, Kumaracoil, Tamil Nadu, India

serious degradation of the images and resulted in low resolution with higher contrast value during the decryption process. In the same year, an extended scheme called the Visual Secret Sharing (VSS) was presented by Yang and Chen (2005). This method also known as one of the most secure methods that hide a secret image that breaks further into images called as the shadow images. Further, using the shadow images, they are decrypted by the human perception.

Zhou *et al*. (2006) have presented a new mechanism referred to as the halftone visual cryptography, that encode a binary image secretly into n halftone shares with the help of two algorithms referred to as the void and cluster. He *et al*. (2007) have proposed a cheating method in Visual Cryptography schemes. The cheating method exploits the cheater with equal form of black and white sub pixels of the shares belonging to the honest participants. Chin-Chen *et al*. (2009) was introduced extended a self-verifying visual secret sharing scheme, which can be applied to both grayscale and color images for secure hashing. Since the set of shadows and the reconstructed secret image are generated by simple Boolean operations, no computational complexity and no pixel expansion occur in our scheme. Experimental results verify that each shadow generated by our scheme is a noise-like image and eight times smaller than the secret image.

InKoo *et al*. (2011) have presented the idea of pixel synchronization and error diffusion to produce good quality images. Ka and Do (2011) have study the optimality to be arrived using a filter bank set up where the images are acquired from multi channel method which included robust reconstruction in the presence of noise. Luisier *et al*. (2011) have proposed a technique to optimize thresholding algorithms for removing the noise which was completely corrupted by poission-gaussian.

In Chopra and Pal (2011) have provided with an enhanced image compression algorithm with the help of slope intercept representation and comparison was made to evaluate the wavelet based model which also results in the improvement of the decibels level. Gunging *et al*. (2011) have obtained high resolution images by adapting compressive measurement and optimization reconstruction which results in the improvement of transmission and memory space.

In the same year, Yun-Fu *et al*. (2011) have presented a method to obtain high quality inverse halftone images from halftone images. The algorithm applied to obtain good quality an image was the mean square least value to obtain a good relationship between the current position and its successive neighborhood values. The results obtained showed better visual quality and improvement in the PSNR ratio with better memory consumption. Egil *et al*. (2011) presented a minimization algorithm on the basis of graph cuts in order to minimize the energy.

In order to improve the quality of image, the digital document given as input are divided into shares using DFT and texture overlapping by maintaining the privacy of the individual shares using cache-cache mechanism with security provided using error transmission technique and distributed individually.

METHODOLOGY

Secured privacy preserving mechanism for distributed digital documents is efficiently designed to improve the quality of share obtained using visual cryptography, to provide privacy for distributed digital document using cache-cache mechanism and to reduce the error using error transmission technique. The SPPM is processed under four set of phases.

Figure 1 shows the conceptual framework of SPPM. The first phase describes the process of improving the image quality using Fourier transform and texture overlapping. The second phase preserves the privacy of the shares obtained using cache- cache mechanism. The third phase provides secure distribution of digital document to different levels using binary spanning trees. The fourth phase describes the process of enhancing the visual quality of the image and removing the error occurred during transmission using error transmission technique.

Fourier filtering and texture overlapping for visual cryptographic images: The first step concentrates on enhancing the quality of digital document image by applying Fourier transformation and texture overlapping. A color image visual cryptic filtering scheme presents a deblurring effect. The Fourier Transform of an image is carried out using Discrete Fourier Transform (DFT) method which allows spectral data to be reverse transformed producing an image. After eliminating blurring effects on the pixels, Fourier transformation is applied to normalize the unevenly transformed share which improves the quality of restored visual cryptographic image to its optimality. The total number of frequencies corresponds to the total number of pixels in the spatial domain image where the image in the spatial and Fourier domain is of the equal size.

In addition the overlapping portion of the two or multiple visual cryptic shares is filtered out with homogeneity of pixel texture property on the restored original image. Texture overlapping filters decides which parts of the input image to be patched into the output texture. After finding a good patch offset between two inputs, the best patch seam is computed. The two overlapped visual cryptic shares images are copied to the output, cut by max-flow/min-cut algorithm and then stitched together along optimal seams to generate a new output.

When filtering an overlapped texture, the generated texture should be perceptually similar to the original image which has been formalized as a Markov Rando

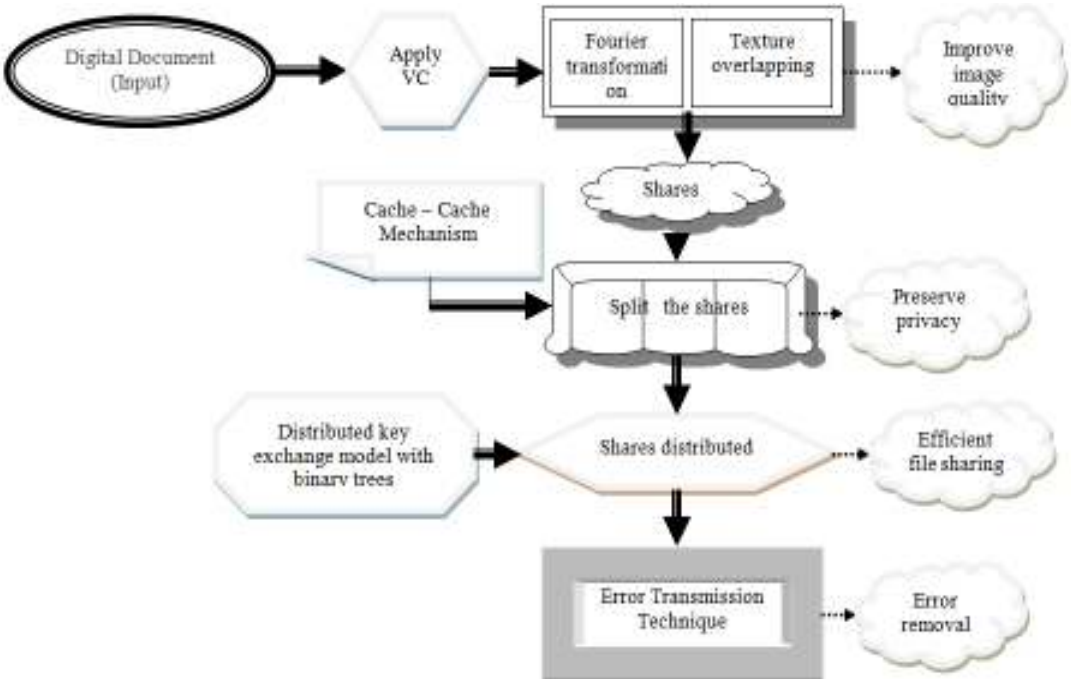


Fig. 1: Architecture of SPPM

Field (MRF). The application of MRF provides with accurate determination of perceptual effect whereas in other methods, the path size is determined in priori. The texture overlap filtering technique used determines the optimal patch for any offset between the two textures, input and output respectively. Finally the performance measure checks this flexibility for different offsets.

For a square image of size N*N, the two-dimensional DFT is shown in the Eq. (1):

$$F(x, y) = \sum_{p=0}^{N-1} \sum_{q=0}^{N-1} f(p, q)\, e^{-y2\pi\,(xp/N+yp/N)} \quad (1)$$

where, f (p, q) denotes the spatial domain of the image. The exponential term is the basic function corresponding to each point F (x, y) in the Fourier space. The value of each point F (x, y) is calculated by multiplying the spatial image with the corresponding base function and adding the result.

Similarly, the Fourier image is re-transformed to the spatial domain.

Cache-cache mechanism for file sharing in VC: The process of preserving privacy using cache-cache to attain a secure digital document sharing across distributed data mining. Given digital document includes text, image, etc., which is converted into an image for sharing with other users present in the distributed network environment in a secure manner. Once the digital document is converted into an image, visual cryptography is applied to split the given image into different parts. Each original image pixel presents n shares of the image, one for each transparency. Each share image comprises of m black and white sub-pixels.

To improve the quality of image and to reduce the noise present in the image using conventional visual cryptography mechanism, the Cache-Cache (CC) mechanism is used with the visual cryptography process for preserving privacy of the respective share holders. The CC mechanism maintains the information about the users who share the splitted parts of the image and at the same time share the image without disclosing the privacy data. The CC mechanism uses cache to fetch the needed information of the system based on the user shares. The splitted images are distributed to the user to the required user who eventually want and share in a secure manner by verifying it with the cache storage.

Distributed file sharing using binary trees: The process of an efficient and secure file sharing is use binary spanning trees. Group dynamics is also achieved with distributed key exchange model, based on the principal operation of minimum spanning tree variants. After maintaining the participants' information regarding their data preservation in cache, it is necessary to share the distributed data and file with them. For each user and file, a unique id is assigned for the process. With the file block id and participant id, a tree is constructed. Based on the construction of tree, the spanning tree is applied to enhance the privacy preservation scheme.

The process of an efficient and secure ,distributed file and data sharing to each and every co-owner by using binary spanning tree is represented next. To avoid the adversary attack, unique id is assigned to both the

users and shared image data, which is again used for constructing binary spanning tree to share the images in a reliable manner. Minimum spanning tree is the set of edges E_{span} denoted in Eq. (2), such a way that:

$$C = \sum (Cij \mid V\ eij \in E_{span}) \quad (2)$$

where, e denotes the edges that connect all the vertices V of communication, following from direction i to j. Finally, improved visual quality of reconstructed image is obtained using error transmission technique. In error transmission technique the error value is dispersed on a partial basis to the adjacent pixels as given below in Eq. (3):

$$E_g = \sum D_j \text{ where } j = 1.4 \quad (3)$$

where,

D1 = P (a, b) - P (a + 1, b)
D2 = P (a, b) - P (a - 1, b + 1)
D3 = P (a, b) - P (a, b + 1)
D4 = P (a, b) - P (a + 1, b + 1)

where, D1, D2, D3 and D4 denotes the directions of each gradient, P (a, b) is pixel at position a, b and E_g is the sum of gradients. Finally, original image is reconstructed by loading the shares.

The spanning tree is used to determine the location of file and the participant with respect to its id. Minimum Spanning Cluster Tree is constructed for each sub tree. The algorithm is modified in order to generate k clusters with k number Minimum Spanning Clustering Tree (MSCT). Using the MSCT the cluster membership of file id relating to the participant id can be easily identified. In this way, file sharing is performed using cache-cache mechanism to reduce the overhead on increasing file sizes. Privacy of file sharing is done with file block id relating to the participant id using binary trees. Group dynamics is handled effectively and shares are distributed with distributed key exchange model, based on the principal operation of minimum spanning tree variants.

Improving visual quality of reconstructed image using error transmission technique: The process of removing the error occurrence from the shares distributed using error transmission technique, a kind of half toning in which the quantization residual is spread to adjacent pixels that have not yet been practiced. Error Transmission technique has the trend to improve edges in an image. When an image has a conversion from light to dark the error transmission algorithm likely creates the next pixel as black. Dark to light conversions be liable to effect in the next created pixel being white. This engenders an edge improvement result at the cost of gray level imitation accuracy. This proves results as error transmission containing an advanced obvious decision than halftone techniques.

Algorithm:

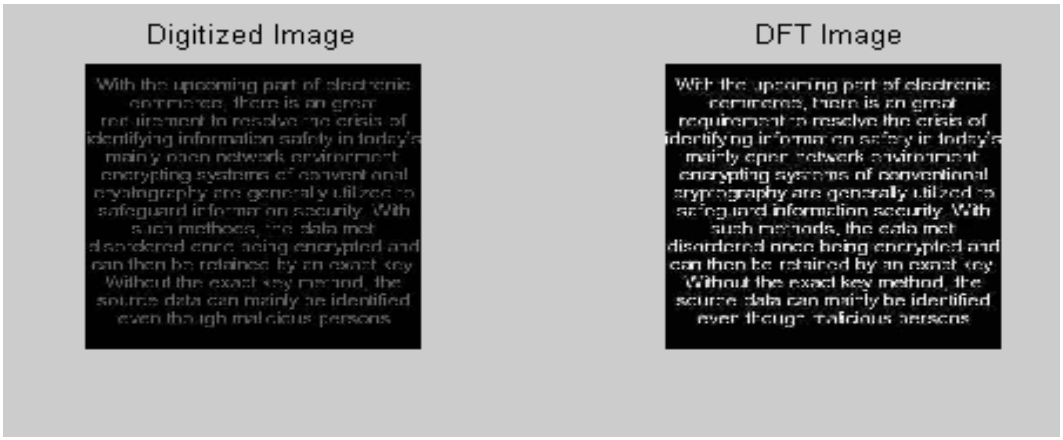
//Process of VC for digital document
Initialization
Let e be an edge in the MST constructed from S and W_e be the weight of e
Let σ be the standard deviation of the edge weights and n_c be the number of clusters
Let n be the root number for binary tree and let T be the error value and N*N denote the size of pixel
Input: Digital Document (DD), Image I, Cache, S the point set with file id relating to participant id, spatial domain image, covering image
For each square image of size M * M, two dimensional DFT is processed to yield F (x, y) using Eq. (1).
//Process of Cache-cache mechanism
Convert DD to image I and apply VC to image I
Split image I into i1, i2,….., in and preserve splitted parts of image
Apply Cache-Cache mechanism and partition the image
Distribute image to different users
For each user Ui
Register personal information in cache
Register User holds which parts of the images
End for
Output: User share image without disclosing their privacy data
//File sharing with multiple participants
For each user U and shared file
Obtain user id Uid and fid and build MST from S
Determine average weight of W and standard deviation σ of all edges
Repeat
For each e ∈ MST
If (We>$\hat{W}$ + σ) or (Current longest edge e)
Remove e from MST which result T', a new disjoint sub tree
ST = ST U {T''} //T' is new disjoint sub tree
nc = nc + 1; n = n + 1;
Tree (T', n) //Construction of Minimum spanning clustering Tree
{Endif} {End for}
Until nc = k
Return k Minimum spanning clustering tree
Output: k number of clusters with binary tree
//Error Transmission technique
For each N*N pixel
If (adjPixels in right)
{Disperse Error Value (T)}
{End if}
If (adjPixels notin right)
{Retain error value}{End if}{End for}

Experimental evaluation: The experimental simulation is conducted using image processing software package (MATLAB). The digital document and color secret image is given as input. This is

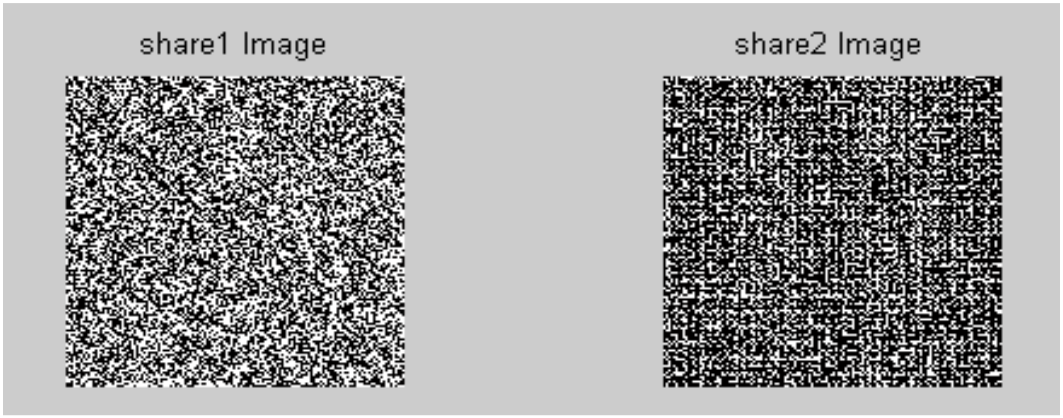
converted into RGB digitized image and is stored in MATLAB as an M- by-3 N-by-3 data array that defines red, green and blue color components for every individual pixel. The color of each and every pixel is defined by the combination of the red, green and blue intensities stored in each and every color plane at the pixels location. Input digital image and secret images are superimposed into digitized image then DFT is applied to improve the clarity of image. VC is applied to DFT images and split the number of shares into secret image and distribute to all participants involved in communication.

(a) Input image

(b) Shares obtained



(c) Applying DFT and texture overlapping



(d) Applying cache-cache

(e) Applying error transmission technique

Fig. 2: Process of secured privacy preserving mechanism for distributed digital documents

RESULTS AND DISCUSSION

A digital document as shown in Fig. 2a is given as input. Visual cryptography is applied to the digital document. The obtained output is share in the form of image as shown in Fig. 2b. The noise present in the image degrades the quality of the image. To remove the noise present in the image, Visual cryptography is used. The shares obtained using traditional visual cryptography methods contains higher noise level and in order to improve the quality of image, noise filters are applied.

Figure 2c shows the results of different level of shares obtained using DFT and texture overlapping. The privacy of individual shares obtained are preserved using cache-cache mechanism and the sample resultant share is illustrated in Fig. 2d. The shares obtained are then distributed to different level (owner, distributor, retailer) using binary spanning tree. Possibility of error occurrence in the shares to be distributed, to different levels makes the system more tedious. To remove the error present in the shares, error transmission technique is applied and shares are distributed to different levels of users as shown in Fig. 2e.

For efficient file sharing approach, cache-cache mechanism is used to maintain all the details about the image being split and the details regarding the user for secure communication. To enhance the privacy preservation, binary spanning trees are performed with file block id relating to the participant id. While reconstructing the secret image, an error transmission technique is used to obtain a good visual quality of the image. The performance of Secured Privacy Preserving Mechanism for Distributed Digital Documents is measured in terms of:

- Visual quality
- Security level
- Time taken to read text
- Error rate
- Privacy overhead

Performance measure of visual quality: Table 1 describes the visual quality of the image for varied number of shares obtained for digital document. The outcome of visual quality using Secured Privacy Preserving Mechanism for distributed digital Documents (SPPM) is compared with existing three methods Copyright Protection using Visual Cryptography (CP-VC), Embedded Extended Visual Cryptography (EVCS) and Visual Cryptography using Error Diffusion (VC-ED).

Figure 3 describes the visual quality of the image with varied number of share levels. The visual quality is measured in terms of %. An increase in number of shares causes an increase in visual quality of image. From the figure it is evident that the visual quality of image is high in Secured Privacy Preserving Mechanism (SPPM) because of application of error transmission technique which secures the image shares resulting in enhanced visual quality when compared to three other methods CPVC, EEVC and VCED with a variance of 20-25% when compared with CPVC.

Performance measure of security level: Table 2 describes the security level of the secret image when the density of participants increases. The outcome of security using Secured Privacy Preserving Mechanism for distributed digital documents (SPPM) is compared with existing three methods CP-VC, EVCS and VC-ED.

Table 1: No. of shares vs. visual quality

No. of shares	Visual quality (%)			
	SPPM (proposed)	Existing methods		
		CP-VC	EVCS	VC-ED
2	62	40	28	25
4	66	43	33	31
6	70	47	37	37
8	73	51	42	40
10	77	54	47	45
12	80	58	50	48

Table 2: Participant density vs. security level

Participant density	Security level (%)			
	SPPM	CP-VC	EVCS	VC-ED
5	50	40	33	30
10	54	43	37	30
15	60	47	42	32
20	65	52	46	38
25	72	56	49	40
30	75	60	52	45

Table 3: Participant density vs. tame taken to read text

Participant density	Time taken to read text (sec)			
	SPPM	CP-VC	EVCS	VC-ED
5	10	16	18	20
10	15	22	23	25
15	18	28	27	30
20	23	35	32	35
25	27	37	35	38
30	30	42	40	42

Figure 4 describes the security level of the image sharing in visual cryptography. The security level of image is measured in terms of number of lost information which can be performed by adversaries. When participant density increases to some extent, the security level in SPPM is high as it maintained binary spanning tree and group management key for sharing the information with the users. When compared to other three methods, CP-VC, EVCS and VC-ED, SPPM achieves 10-20% higher security.

Performance measure of time: Table 3 describes the time taken to read the visual information after reconstruction of image when more number of participants involved. The outcome of the time using SPPM is compared with existing three methods, CP-VC, EVCS and VC-ED.

Figure 5 describes the time taken to read the visual information after reconstruction of image when more number of participants involved in a communication. The time consumption is measured in terms of seconds. When participant density increases, the time taken to read the text in SPPM is comparatively less. When compared to three other methods, CP-VC, EVCS and VC-ED, the time taken to read the text is low since the visual quality of the image is good using cache-cache mechanism which maintains the location of the image

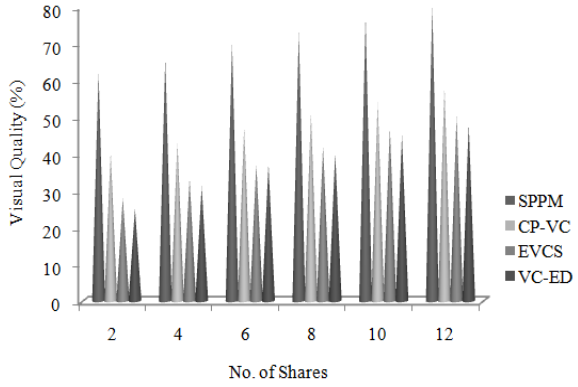


Fig. 3: Visual quality

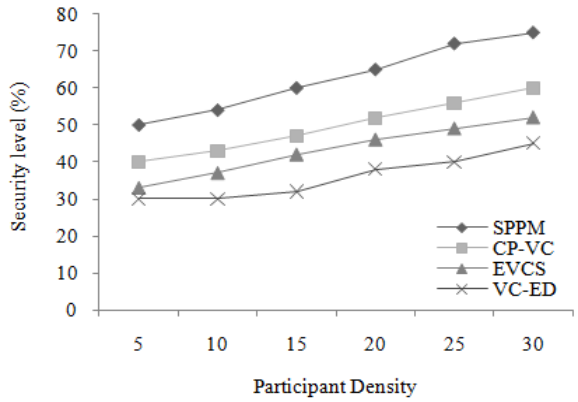


Fig. 4: Measure of security level

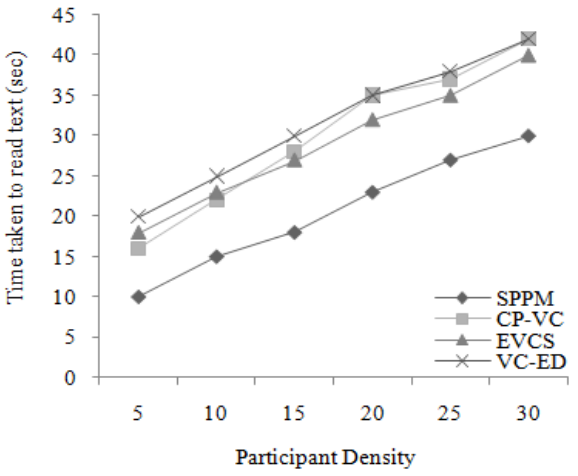


Fig. 5: Measure of execution time

and by applying error transmission technique, the time to read the text is less with a variance of 50-60%.

Performance measure of error rate: Table 4 shows the performance evaluation of error rate. A detailed comparison analysis is made with three other methods, CP-VC, EVCS and VC-ED.

Table 4: Participant density vs. security level

No. of shares	Error rate (%)			
	SPPM	CP-VC	EVCS	VC-ED
2	20	25	28	32
4	24	30	35	40
6	28	40	42	45
8	30	40	45	50
10	35	42	50	52
12	38	45	52	55

Table 5: Participant density vs. privacy overhead

Participant density	Privacy overhead (%)			
	SPPM	CP-VC	EVCS	VC-ED
5	3.0	4.3	7.0	10.0
10	4.5	6.5	7.5	12.0
15	4.8	9.2	10.0	12.5
20	5.2	12.2	12.0	14.0
25	5.8	13.5	12.5	15.0
30	6.0	14.0	13.0	15.5

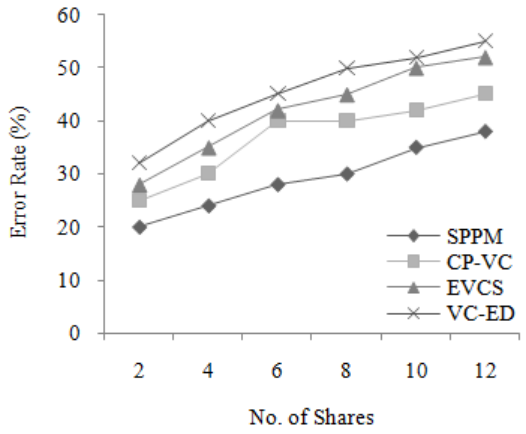


Fig. 6: Measure of error rate

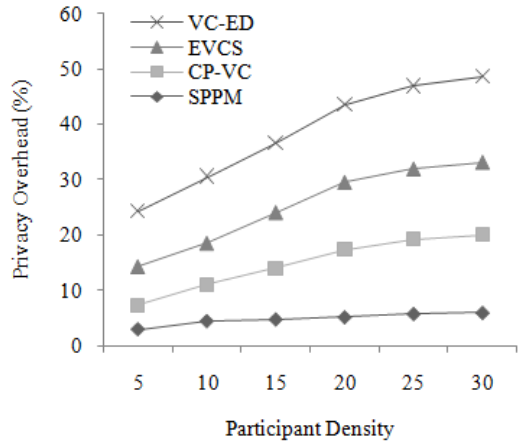


Fig. 7: Measure of privacy overhead

Figure 6 illustrates the error rate for digital document. The results of our experiments in figure indicate that the error rate of SPPM is comparatively less by applying fourier filtering and texture overlapping methods which removes the noise present in the digital document when compared to three other methods, CP-VC, EVCS and VC-ED which uses watermarking and error diffusion techniques. The error rate is reduced to 10% when compared to CP-VC, 15% when compared to EVCS and 30-35% when compared to VC-ED.

Performance measure of privacy overhead: Table 5 describes the privacy overhead occurred when more number of participants involved. The outcome of the SPPM for distributed digital document is compared with CP-VC, EVCS and VC-ED for varied levels of participant densities.

Figure 7 describes the process of privacy overhead when more number of participants involved in secure communication. The privacy overhead is measured in terms of %. From the figure it is evident that, the privacy overhead is comparatively low in SPPM when compared to three other methods, CP-VC, EVCS and VC-ED because SPPM uses cache inside a cache to preserve the details about the users who shared the secret parts of digital document. The variance in privacy overhead is 40-50, 50 and 55-60% low when compared to CP-VC, PPS-CCM and VC-ED, respectively.

CONCLUSION

SPPM develops an efficient color image visual cryptic filtering scheme to improve the image quality on restored original image from visual cryptic shares using DFT and Texture overlapping. It is obvious that there is tradeoff between image quality and privacy. To enhance privacy for the shares obtained by the individuals, cache-cache mechanism is used to preserve the privacy and distributed to different levels of users using binary spanning tree with file block id relating to the participant id.

Finally, an error transmission technique used to encrypt and separates a secret image into n number of shares. The shares are passed through diverse transmission channels from sender to receiver so that the possibility of obtaining adequate shares by the intruder gets reduced. Experimental results have shown that SPPM for distributed digital document using DFT and texture overlapping with cache-cache mechanism using error transmission technique are efficient in terms of visual quality of image obtained, security, privacy overhead and error rate when compared to the three other methods CP-VC, PPS-CCM, VC-ED, respectively. The performance of visual quality is improved to 20-25% when compared to CP-VC with error rate reduced to 10, 15 and 30-35% when compared to CP-VC, EVCS and VC-ED respectively. Finally, privacy and security is enhanced 40-60% and 10-20%, respectively using cache-cache and error transmission techniques.

REFERENCES

Che-Wei, L. and T. Wen-Hsiang, 2012. A secret-sharing-based method for authentication of grayscale document images via the use of the PNG image with a data repair capability. IEEE T. Image Process., 21(1): 207-218.

Chin-Chen, C., L. Chia-Chen, T.H.N. Le and B.L. Hoai, 2009. Self-verifying visual secret sharing using error diffusion and interpolation techniques. IEEE T. Inf. Foren. Sec., 4(4): 790-801.

Chopra, G. and A.K. Pal, 2011. An improved image compression algorithm using binary space partition scheme and geometric wavelets. IEEE T. Image Process., 20(1): 270-275.

Egil, B., S. Juan and T. Xue-Cheng, 2011. Graph cuts for curvature based image denoising. IEEE T. Image Process., 20(5): 307-318.

Gunging, S., G. Dachau, S. Xiaoxia, X. Xuemei, C. Xuyang *et al*., 2011. High-resolution imaging via moving random exposure and its simulation. IEEE T. Image Process, 20(1): 276-282.

He, W., X. Liu, H. Nguyen, K. Nahrstedt and T. Abdelzaher *et al*., 2007. PDA: Privacy-preserving data aggregation in wireless sensor networks. Proceeding of the 26th IEEE International Conference on Computer Communications, pp: 2045-2053.

InKoo, K., G.R. Arce and H.K. Lee, 2011. Color extended visual cryptography using error diffusion. IEEE T. Image Process., 20(1): 132-145.

Jin, D., W.Q. Yan and M.S. Kankanhalli, 2005. Progressive color visual cryptography. J. Electron. Imaging, 14(3): 19-33.

Ka, L.L. and M.N. Do, 2011. Multidimensional filter bank signal reconstruction from multichannel acquisition. IEEE T. Image Process., 20(5): 1-10.

Luisier, F., T. Blu and M. Unser, 2011. Image denoising in mixed poisson-gaussian noise. IEEE T. Image Process., 20(3): 696-708.

Naor, M. and A. Shamir, 1995. Visual cryptography. In: De Santis, A. (Ed.), Advances in Cryptogoly Eurocrypt' 94. Lect. Notes Comput. Sc., Springer-Verlag, Berlin, 950: 1-12.

Yang, C.N. and T.S. Chen, 2005. Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion. Pattern Recogn. Lett., 26(10): 193-206.

Yun-Fu, L., G. Jing-Ming and L. Jiann-Der, 2011. Inverse half toning based on the Bayesian theorem. IEEE T. Image Process., 20(4): 308-406.

Zhou, Z., G.R. Arce and G.D. Crescendo, 2006. Halftone visual cryptography. IEEE T. Image Process., 18(8): 2441-2453.