Implementation of Cache-Cache Mechanism and Minimum Spanning Tree for Multiparty Copy Right Protection in Visual Cryptography

Shiny Malar F.R[1], Jeya Kumar M.K[2]

[1]Department of Computer Science and Engineering, Noorul Islam University, Thuckalay, Kanyakumari Dist, India
[2]Department of Computer Application, Noorul Islam University, Thuckalay, Kanyakumari Dist, India
shybertrijo@gmail.com

Abstract: Multiparty Copy Right Protection is one of the most popular applications in Visual Cryptography (VC). In Copy Right protection, watermark does not get superimposed into the protected image, but it is used to generate a secret image and a public digital image using VC techniques. While partitioning the access structure, increase in Average Pixel Expansion (APE), reduce information accuracy and minimum level contrast of the reconstructed secret images are some of the most common issues in VC scheme. The proposed scheme applies Discrete Fourier Filtering (DFT) and texture overlapping, which reduces the APE, increases the information accuracy and improves privacy using cache-cache mechanism and achieves secured communication. Privacy of the owners is preserved using cache-cache mechanism with visual cryptography for distributed digital document. Experimental results show that the proposed scheme significantly verify the copy right of digital image in terms of PSNR, error rate, participant density, accuracy ratio and Universal Quality Index (UQI).
[Shiny Malar F.R, Jeya Kumar M.K. **Implementation of Cache-Cache Mechanism and Minimum Spanning Tree for Multiparty Copy Right Protection in Visual Cryptography.** *Life Sci J* 2013; 10(2): 2037-2047]. (ISSN: 1097-8135). http://www.lifesciencesite.com. 287

Keywords: Copy right Protection, Minimum Spanning Tree, Privacy Preservation, Texture Overlapping, and Visual Cryptography

1. Introduction

Initially (Naor and Shamir, 1994) predicted new security technique named visual cryptography. In visual cryptography, a binary secret image is prearranged into indiscriminate binary patterns, which contains of n shares in a k-out-of-n scheme. The 'n' shares are distributed to 'n' participants in such a way each participant share is not known to other participant.

With the upcoming part of electronic commerce, there is a great deal to solve the crisis related to identifying the factor in open network environment. The encrypting systems of conventional cryptography are generally used to safeguard information security. Privacy-preserving data mining has abundant applications, which are logically standard to privacy-violating requests. Some methods of privacy calculation utilize some amount of transformations involved on data to achieve privacy preservation. Cache obtains a well-explored idea from dispersed systems, explicitly caching, and relates it in the framework of privacy. Cache has two interior ideas, first the location-enhanced contented can be sometimes pre-fetched in great geographic mass onto a device, and second the content can be admitted nearby on a device when it is really needed, without relying on external device.

Secure multiparty copy right protection is one of the applications in VC. The major goal of the 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, data mining has been analyzed as a hazard to privacy since, the extensive propagation of electronic data preserved by corporations. 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.

Texture overlap filtering technique determine optimal patch region for any given offset between the input and output texture for the reduction of average pixel expansion. Privacy of the owners is preserved using cache-cache mechanism with visual cryptography for distributing digital document. The main principle behind the application of cache-cache mechanism is to maintain the information about the users who shares the splitted parts of the image without disclosing the privacy data. While employing filter mechanism, though pixels were considered the image quality was enhanced using texture overlap and Fourier filtering which is remove the noise present in the image using CMY color model.

All information of the users is preserved for distributing digital document using cache-cache mechanism, who shared the secret parts of digital document which has been splitted using visual cryptography for digital document sharing, between the peer users. The application of cache-cache

mechanism does not compromise the user's cache. This cache is in turn preserves the details about the 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.

2. Related Works

Several methods for Visual Cryptography have been introduced recently in the literature. The concept of general access structure method was introduced by (Ateniese, C.Blundo, A.Desantis and D.R.Stinson, 1996).This general access structure method is applied to gray level images. G. Ateniese, C. Blundo, A. Santis, and D. R. Stinson (2001) predicted the extended capabilities for visual cryptography using natural images. A new method of extended visual cryptography for natural images is used to produce meaningful binary share which is predicted by (Nakajima, 2002).

Hou (2003) proposed binary visual cryptography scheme, applied to gray level images & that a gray level image is converted into halftone images. (D. Jin, W. Q. Yan, and M. S. Kankanhalli, 2005) introduced color visual cryptography scheme overcome the image quality in terms of loss of resolution & contrast but this scheme results in severe degradation while performing decryption process.

C. N. Yang, T. S. Chen (2005) predicted the Visual Secret Sharing (VSS) scheme, a perfect secure method to hide secret image by breaking it into shadow images and decrypts it easily by human visual system. (Zhou, Arce, Crescenzo 2006) proposed a novel technique named halftone visual cryptography, to encode a secret binary image into n halftone shares by using void and cluster algorithm, but that have high error bit rate. Soo-Chang Pei has introduced the minimal-error bit-searching technique distribute the embedded watermark image into several error-diffused images with more collision attack (2006).

C.M. Hu and W.G. Tzeng, (2007) proposed a cheating method in Visual Cryptography schemes. In this cheating method, the cheater needs to know the exact distribution of black and white sub pixels of the shares of honest participants. Kharbutli , Yan Solihin (2008) have predicted the counter-based mechanism to identify reassessed lines, bypass the L2 cache, and place them directly in the L1 cache and increases the speed.

Chin-Chen Chang (2009) introduced extended 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 the scheme. Experimental results verified that each shadow generated by the scheme is a noise-like image and eight times smaller than secret image.

InKoo Kang et al. (2011) proposed concept of visual information pixel synchronization and error diffusion to obtain color visual cryptography that achieves high quality images. Ka Lung Law and Minh N Do (2011) studies the optimality to be arrived using filter bank set up where images are acquired from multi channel method, which included robust reconstruction in the presence of noise. Florian Luisier et al. (2011) proposed a technique to optimize thresholding algorithms for removing the noise which was completely corrupted by poission-gaussian.

Garima Chopra and A. K. Pal (2011) presented an improved image compression algorithm, using slope intercept representation and comparison was made to evaluate the wavelet based model which also results in improvement of the decibels level. (Guangming Shi et al., 2011) obtained high resolution images by adapting compressive measurement and optimization reconstruction which results in improvement of transmission and memory space. (Yun-Fu Liu et al., 2011) presented method to obtain high quality inverse halftone images. The algorithm applied was the least mean square algorithm in order, to establish relationships between current processing position and its corresponding neighboring positions. The result obtained shows better visual quality and improvement in psnr ratio with better memory consumption. (Egil Bae et al., 2011) presented a minimization algorithm on the basis of graph cuts in order to minimize the energy.

In this work, DFT and texture overlapping is applied for digital images using max flow min cut algorithm to improve the image quality, while the generated output is preserved using cache-cache mechanism which achieves higher level of privacy. Finally, the data is distributed to achieve group dynamics using binary span tree. The forthcoming section discusses in detail about the process involved in Multi Party Copy Right Protection scheme for digital images using DFT, texture overlapping, applying cache-cache mechanism.

3. Multi Party Copy Right Protection Scheme for Digital Images

Watermarking technology is used to superimpose digital document and secret images into digitized image. Visual cryptography is applied to the digitized image and is split into two or more shares. (Figure1).The shares include how many participants are involved in the communication networks. The

main objective of Cache-cache mechanism is to (i) maintain information about users who share splitted parts of image, (ii) maintain information about user who have the splitted parts of the images, which are partitioned by VC. One of the sharing images is delivered to owner as public share.

The process of achieving efficient and secure, distributed file and data sharing is to use the Binary Spanning Tree (BST). BSTs are also used to enhance the progress of secure distributed file sharing in VC. Whenever some users need to declare their rights, the process to be followed is (i) to presently submit the shares to owners and (ii) then interpret the secret (watermark) image which is evident from the original digital documents.

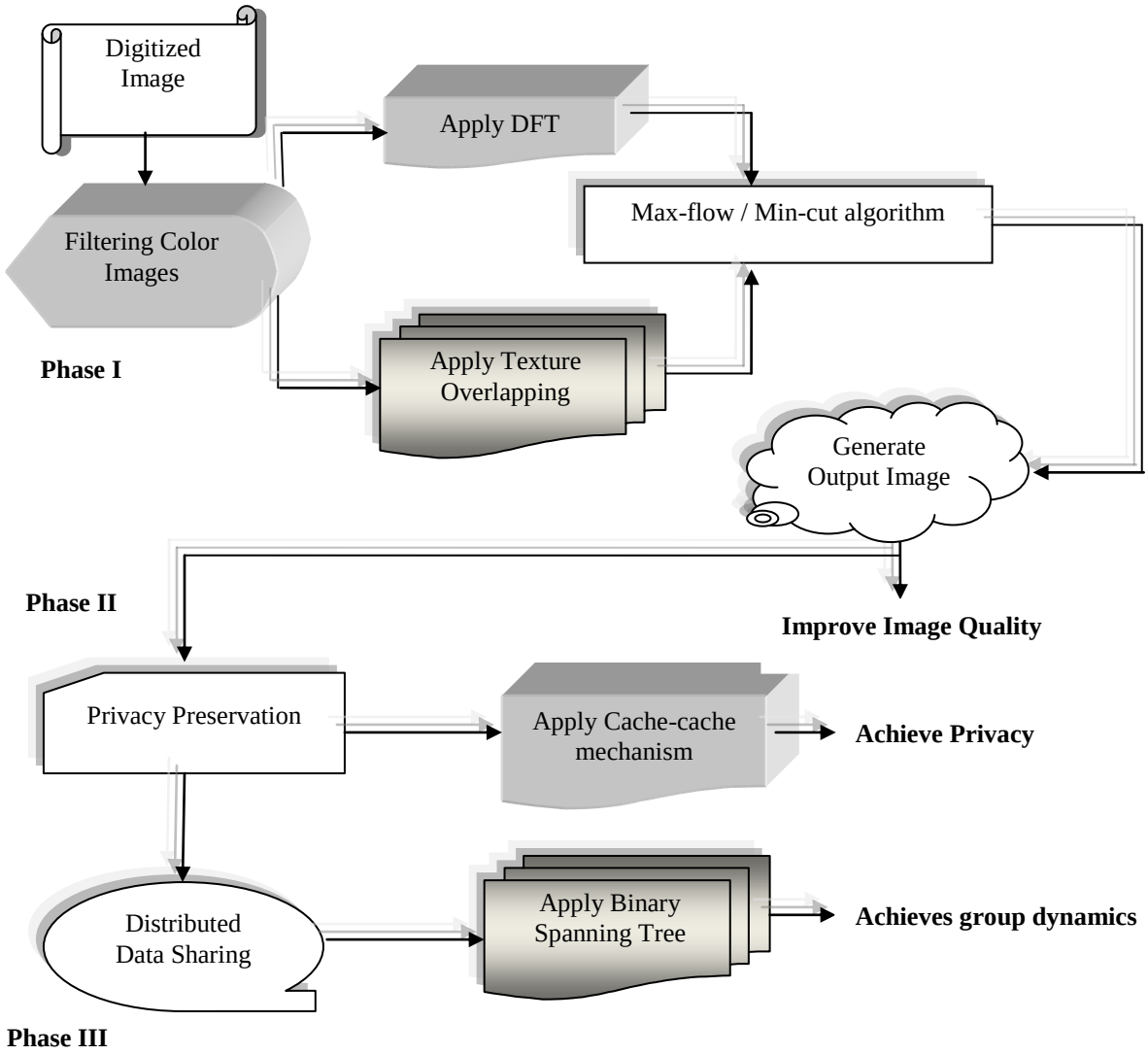


Figure 1. Architecture diagram of Multiparty Copy Right Protection for digital images.

The architecture diagram of Multi Party Copy Right Protection scheme for digital images is illustrated in Figure 1. The Multi Party Copy Right Protection scheme is divided into three phases. The first phase concentrates on filtering of color images using visual crypting. The second phase involves with the preservation of the owners using cache-cache mechanism. Finally, sharing the data in

distributed manner is performed using visual cryptography in the third phase.

3.1 Color image visual cryptic filtering

To start with, let us discuss about the first phase which involves with filtering of color images. Color image visual cryptic filtering method is presented for deblurring effect on the non-uniform distribution of visual cryptic share pixels using Discrete Fourier Filtering (DFT) and Texture Overlapping.

3.1.1 Discrete Fourier Filtering

The first filtering method used in Multi Party Copy Right Protection scheme for digital images is DFT, one of the most significant tools in digital image processing. It converts a limited list of uniformly spaced model of a function into the coefficients of a finite grouping of intricate sinusoids ordered by their frequencies. For a square image of size $N \times N$, the two-dimensional DFT is shown in the equation 1.

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

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. The inverse Fourier transform is exposed in the equation 2.

$$f(i,j) = {}^{1}/_{N^2}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} F(x,y)e^{y2\pi\left(\frac{xi}{N}+\frac{yj}{N}\right)} \quad (2)$$

Here, $\frac{1}{N^2}$ normalization term is the inverse transformation. Sometimes, this normalization is carried out for the forward transformation instead of the inverse transformation.

By using these two equations, the spatial domain image is transformed into transitional image using N one-dimensional Fourier Transforms.

$$F(x,y) = 1/N\sum_{j=0}^{N-1} K(x,j)\, e^{-\frac{y2\pi pj}{N}} \quad (3)$$

Where,

$$K(x,j) = 1/N\sum_{i=0}^{N-1} f(i,j)e^{-y2\pi xi/N}$$

This intermediate image is then transformed into the final image, again using N one-dimensional Fourier Transforms. Expressing the two-dimensional Fourier Transform in terms of a series of $2N$ one-dimensional transform reduces the number of needed computations.

3.1.2 Texture Overlapping

The second filtering method used in Multi Party Copy Right Protection scheme for digital images is Texture overlapping filters, decide which parts of the input image to be patched into the output texture. Now, the two overlapped visual cryptic shares images are copied to the output, by Max Flow Min Cut algorithm and then stitched together along optimal seams to generate a new output.

3.1.3 Max Flow Min Cut Algorithm

The main aim of this algorithm is, the maximum value of all flow values is equivalent to the minimum capacity of all cut is minimal.

Lemma 1. Given a network, for any flow X and cut Y on the network, Val X< cap C.

Proof. Let C= (P, P). As P is comprised of sources and intermediates, clearly

$$Val\ X = X_{out}(Z) - X_{in}(Z) = X_{out}(P) - X_{in}(P) \quad (4)$$

As the intermediates contribute to the flow value let us consider an arc with both endpoints in P: its flow is counted in both $X_{out}(P)$ and $X_{in}(P)$, and thus makes no net impact on the flow value. Therefore the only arcs flows which positively impact Val X is those originating in P and terminating in P which is precisely the flows over the cut C. include that

$$val\ X \leq \sum_{a\in c} X(a) \leq \sum_{a\in k} c(a) \quad (5)$$

Once the process of filtering of color images using DFT and Texture Overlapping process is completed the next section concentrates on to apply privacy using Cache-cache mechanism.

3.2 Privacy of the owners using cache-cache mechanism

Caching is an efficient approach to accomplish high scalability and increase performance. It is used to reduce the average memory access time. The details of users are preserved for distributed digital document using cache-cache mechanism, between the peer users. The application of cache-cache mechanism does not compromise the data, as the user's cache and this in turn preserves the details about the users. Once the privacy of the owners is preserved the next section finally concentrates on distributed data sharing using visual cryptography.

3.3 Distributed data sharing using visual cryptography

The process of an efficient and secure, distributed file and data sharing to each and every co-owner by using binary spanning tree are represented in Figure 2. Privacy of the file sharing is performed with file block id related to the participant id, using binary tree. Group dynamic is handled effectively

with distributed key exchange model based on the principal operation of minimum spanning tree variants.

To avoid the adversary attack, a unique id is assigned to both the user and shared image data, which is used for construct binary spanning tree for sharing the images in reliable manner. The distributed key model provides a key to each and every participant and allows the sharing of each file with a secure key to preserve privacy of current participants.

Spanning tree is a set of |V| - 1 edge that connects all the vertices of a communication. Minimum spanning tree is the set of edges E_{span} such that,

$$C = \sum (Cij \mid \forall eij \in Espan) \qquad (6)$$

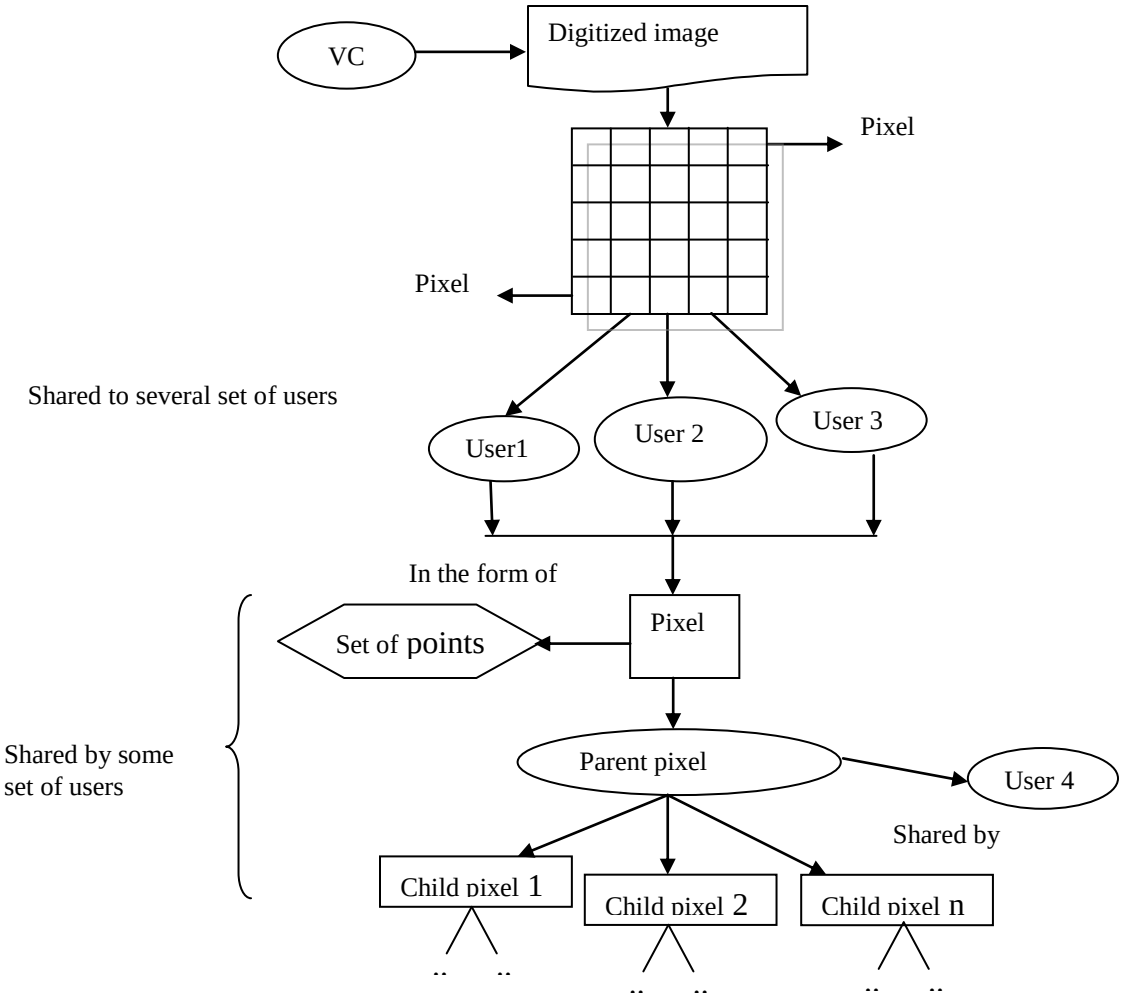


Figure 2. Distributed data sharing – Binary Span Tree

Algorithm:

Input: S the point set with file id relating to participant id

Let e be an edge in the MST constructed from S

Let W_e be the weight of e

Let σ be the standard deviation of the edge weights

Let n_c be the number of clusters

Let n be the root number of binary tree

Output: k number of clusters with binary tree

Process

Step 1: For each user U and shared file

Step 2: Obtain user id Uid and file id fid

Step 3: End For

Step 4: Build MST from S

Step 5: Determine the average weight of W of all the edges

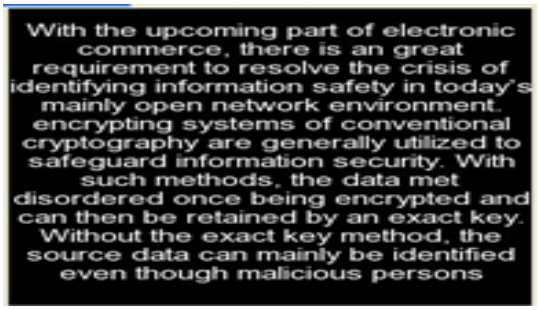
Step 6: Determine standard deviation σ of the edges
Step 7: $S_T = \varnothing$; $n_c = 1$; n = 0;
Step 8: Repeat
Step 9: For each e ∈ MST
Step 10: If ($W_e > \hat{W} + \sigma$) or (Current longest edge e)
Step 11: Remove e from MST which result T', a new disjoint sub tree
Step 12: $S_T = S_T \cup \{T''\}$ // T' is new disjoint sub tree
Step 13: $n_c = n_c+1$; n = n + 1;
Step 14: Tree (T', n) // Construction of Minimum Spanning Clustering Tree
Step 15: Until $n_c = k$
Step 16: Return k Minimum spanning clustering tree

4. Experimental Results

The experimental simulation is conducted using image processing software package (MATLAB). The digital document and color secret image is given as input (Figure 3). 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 pixel's location.

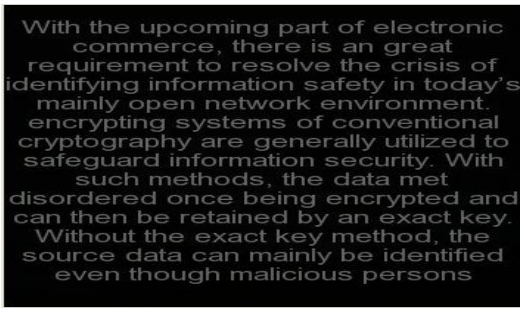
Input digital image and secret images are superimposed into digitized image (Figure 4(a)), then apply the DFT for giving clarity of that images (Figure 4(b)). VC is applied to DFT images and split the number of shares (Figure 5) into secret image and distribute to all participants involved in communication.

(a)

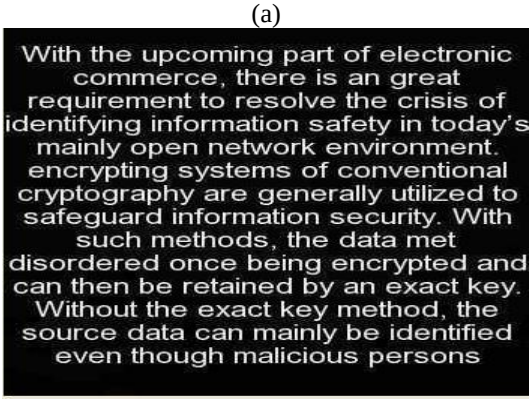


(b)

Figure 3.Experimental results of (a)Digital image and (b) secret image of (2, 2) scheme in size 256 X 256

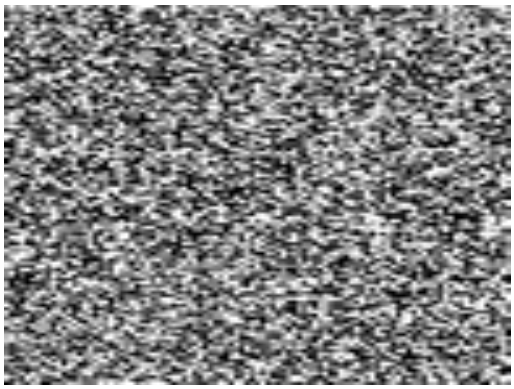


(a)

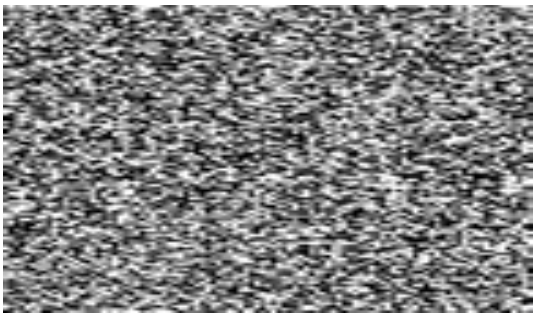


(b)

Figure 4.Experimental results of (a) Digitized image and (b) DFT image of (2, 2) scheme in size 256 X 256



Share 1



Share 2

Figure 5.Experimental results of the DFT image is encoded into two shares of (2, 2) scheme

The performance of privacy preservation scheme in visual cryptography is measured in terms of,

i. Peak Signal-to-Noise Ratio (PSNR)
ii. Error Rate
iii. Participant Density
iv. Accuracy
v. Universal Quality Index (UQI)

4.1 Peak Signal-to-Noise Ratio (PSNR)

The essential parameter includes Peak Signal-To-Noise Ratio (PSNR). PSNR is the ratio between the maximum possible power of the signal and the power of corrupted noise that is articulated in decibels.

4.2 Error Rate

$$Mean\ Square\ Error = Error\ /Size\ of\ the\ image \quad (7)$$

The Mean Square Error is the average square of the error in a particular image. The calculation of MSE & PSNR is given in the equation 8 and equation 9.

$$MSE = 1\Big/MN[\sum_{i=1}^{M}\sum_{j=1}^{N}(Iij - I'ij)^2 \quad (8)$$

$$PSNR = 20 * \log_{10}(255/sqrt(MSE)) \quad (9)$$

Where, 255 is the maximum possible value of the image. In general the Peak signal -to-noise ratio for two shares are increased and the perceived error for that two shares are decreased. These works are some examples that prove the improvements and high performance of the color images in visual cryptography and also reduce the perceived errors.

4.3 Contrast

The performance metric, contrast refers to the ability to distinguish between differences in intensity in digital image. The metric, contrast is used for digital images to quantify the quality of acquired images.

4.4 Accuracy

Accuracy measures the percentage of accuracy obtained by applying the DFT and texture overlapping using the max flow min cut algorithm.

4.5 Universal Quality Index (UQI)

Universal Quality index attempts to measure the quality of the image after the removal of the noise present in the image using DFT which are easy to calculate and involve low computational complexity.

5. Result and Discussion

In Multi Party Copy Right Protection (MPCRP), the image quality is improved and achieves privacy and group dynamics, using cache-cache mechanism and binary spanning tree, with the max flow min cut algorithm for digital image. Comparison is made with the existing Color Extended Visual Cryptography (CEVC) scheme using the image processing software package MATLAB. The table given below and graph describes the performance evaluation of the Multi Party Copy Right Protection for digital images.

Table 1 Image Size Vs PSNR

Image Size (Pixels)	PSNR (dB)	
	MPCRP	CEVC
20	120.25	100.25
40	125	110.15
60	132.5	125.25
80	140	130
100	145.25	135.25
120	148.5	140

The above (Table 1) describes the peak signal-to-noise ratio based on the size of images. The efficiency of rate of psnr using the multi party copy right protection scheme for digital image is compared with the color extended visual cryptography using error diffusion mechanism.

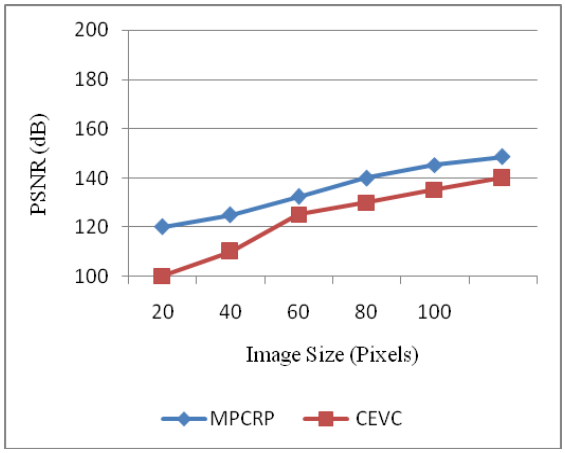


Figure 6 Image Size Vs PSNR

The (Figure 6) describes the process of peak signal-to-noise rate based on size of images present

in the digital image. When the size of the image increases, the PSNR value is also increases in the multi party copy right protection scheme for digital images using max flow min cut algorithm. The PSNR rate is measured in terms of decibel (dB). From the (Figure 6) it is evident that comparatively, MPCRP attains higher PSNR rate when compared to the existing methods, which proves the reconstruction of higher quality images. The application of DFT and Texture overlapping using max flow min cut algorithm further enhances and improves the image quality. The compression ratio is measured in terms of megabyte (mb). Compared to the existing scheme using error diffusion methods, MPCRP scheme achieves an improvement of over 25-30%.

Table 2 Image Size Vs Error Rate

Image Size (Pixels)	Error Rate (%)	
	MPCRP	CEVC
20	35	45
40	38	48
60	40	52
80	45	55
100	50	58
120	55	62

The above (Table 2) describes the Mean Signal Error Rate based on the size of images. The measure of error rate using MPCRP for digital images is compared with the existing method using error diffusion mechanism.

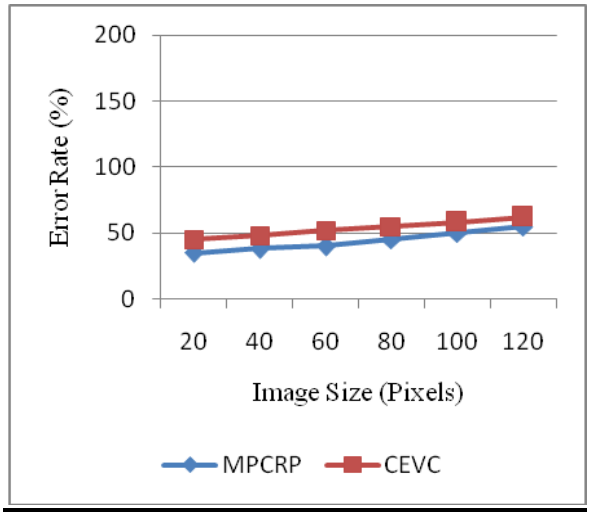


Figure 7 Image Size Vs Error Rate

The (Figure 7) illustrates the error rate of the image size in the range of 20-120 pixels. Y axis represents the error rate, measured in terms of (%). It is also observed, if the size of the images is increased there is also an increase in the error rate for both the methods. The error rate is reduced to certain extent in MPCRP due to introduction of privacy preservation using Cache-cache mechanism. The error rate variance is reduced to 15-20% in MPCRP when compared to existing one.

Table 3 Image Size Vs Contrast

Image Size (Pixels)	Contrast (%)	
	MPCRP	CEVC
20	45	25
40	65	45
60	80	60
80	120	90
100	140	120
120	220	150

The above (Table 3) describes the contrast based on the size of images. The measure of contrast value using MPCRP for digital images is compared with the existing method using error diffusion mechanism.

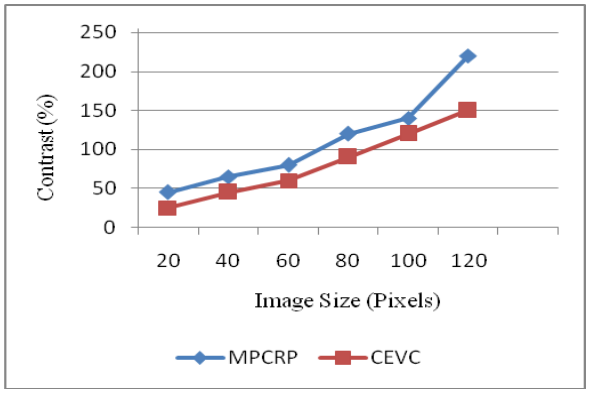


Figure 8 Image Size Vs Contrast

The (Figure 8) illustrates the metric contrast and comparison analysis is made with the existing method using error diffusion. Contrast is measured in terms of %. The metric, contrast is very difficult to define as it purely depends upon the human observer and varies to a larger extent. Images having higher contrast level and display a greater degree of enhancements when compared to the lower contrast level. The result is a general overall increase in digital image contrast, since the majority of brightness value in each digital image tends to occupy the mid range of intensity levels. An increase in image size results in higher contrast level when compared to the existing model using error diffusion and the variance achieved is 85-90%.

Table 4 Image Size Vs Accuracy

Image Size (Pixels)	Accuracy (%)	
	MPCRP	CEVC
20	65	50
40	68	55
60	72	60
80	78	68
100	85	75
120	88	80

The (Table 4) describes accuracy based on the size of images. The measure of accuracy value using MPCRP for digital images is compared with the existing method using error diffusion mechanism.

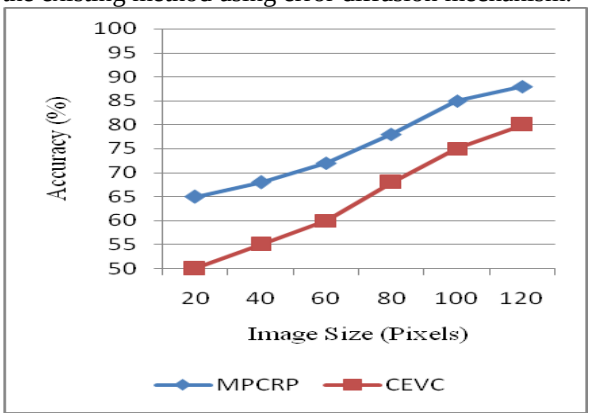


Figure 9 Image Size Vs Accuracy

The (Figure 9) illustrates the accuracy obtained for different size of image measured in terms of pixels in the range of 20 to 120. The accuracy is measured in terms of %. The measure of accuracy value using the MPCRP for digital images is compared with the existing method using error diffusion mechanism. Accuracy factor increases with the increase in the image size. When compared to the existing work CEVC, the accuracy for MPCRP is comparatively higher and the variance is increased to 60-65%. The increase in accuracy is due to the fact that the introduction of discrete fourier filtering and texture overlapping reduces the APE and results in the increase of accuracy level in digital images.

Table 5 Image Size Vs. Universal Quality Index

Image Size (Pixels)	Universal Quality Index (%)	
	MPCRP	CEVC
20	45	32
40	52	40
60	58	48
80	65	52
100	68	55
120	72	60

The above (Table 5) describes the Universal Quality Index based on the size of images. The measure of UQI using MPCRP for digital images is compared with the existing method using error diffusion mechanism.

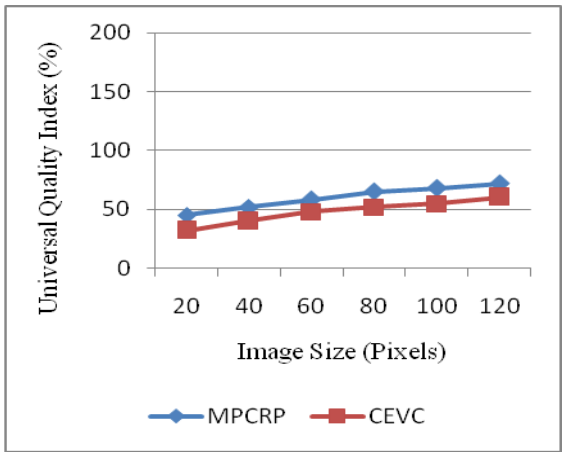


Figure 10 Image Size Vs Universal Quality Index

The (Figure 10) illustrates the universal quality index which is a measure of quality images obtained once the filtering technique, DFT is applied to the digital images. X axis represents the image size measured in terms of pixels in the range of 20-120 pixels, whereas the y axis denotes the universal quality index measured in terms of %. Increase in image size causes an increase in UQI value. When compared to the color extended visual cryptography using error diffusion mechanism, the quality of image is improved in MPCRP with the application of both DFT and texture overlapping method.

6. Conclusion

In MPCRP, the quality of digital image is improved using two techniques namely, DFT and texture overlapping with the help of max flow min cut algorithm. The Improvisation of quality is achieved using DFT which initially apply filtering method of digital color image using visual cryptic filtering for deblurring effect on the non-uniform distribution of visual cryptic share pixels.

The advantages of the proposed schemes for digital images using DFT and cache-cache mechanism are,

- It improves the image quality by removing the noise using DFT technique.
- It efficiently achieved privacy between the owners by following cache-cache mechanism.
- Greatly reduced the time taken for removing the noise present in the images and thereby achieving group dynamics.

Experimental results have shown that the MPCRP for digital images using DFT technique and

texture overlapping are efficient in terms of peak signal-to-noise ratio, mean square error rate, universal quality index, participant density and finally contrast when compared to the existing color extended visual cryptography using error diffusion methods.

Corresponding Author:
F.R.Shiny Malar,
Department of Computer Science and Engineering,
Noorul Islam University, Thuckalay,
Kanyakumari District -629180, Tamilnadu, India.
E-mail: shybertrijo@gmail.com .

References

[1] M.Naor and A. Shamir, *Visual Cryptography*, in "Advanced in Cryptology – EUROCRYPT' 94", A. De. Santis, Ed., Vol. 950 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, PP. 1-12,1995.

[2] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Visual cryptography for general access structures," *Inf. Comput.*, vol. 129, no. 2, pp. 86–106, 1996.

[3] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, Extended Schemes for Visual Cryptography, submitted to Discrete Mathematics, 1996.

[4] L. A. MacPherson, "Gray level visual cryptography for general access structure," M. Eng. thesis, Univ. Waterloo, Ontario, Canada, 2000.

[5] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Extended Schemes for Visual Cryptography". *Theoretical Computer Science*, No. 250, pp. 143-161, 2001.

[6] M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images," *J. WSCG*, vol. 10, no. 2, 2002.

[7] C. C. Lin and W. H. Tsai, "Visual cryptography for gray-level images by dithering techniques," Pattern Recognit. Lett., vol. 24, pp. 349–358, 2003.

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

[9] 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.

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

[11] Soo-Chang Pei et al.,' High-capacity data hiding in halftone images using minimal-error bit searching and least-mean square filter', IEEE Transactions on Image Processing, 2006.

[12] 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.

[13] W. He, X. Liu, H. Nguyen, K. Nahrstedt and T. Abdelzaher, "PDA: Privacy-preserving Data Aggregation in Wireless Sensor Networks," In 26th IEEE International Conference on Computer Communications (Infocom), 2007.

[14] 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.

[15] S. A. M. Gilani, A. N. Skodras," Adaptive Image Watermarking Using Multiple Transforms",International Review on Computers and Softwares, Vol. 2. n. 6, pp. 653 – 660, Nov 2007.

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

[17] T. Feng, C. Wang, W. Wang and L. Ruan, "Confidentiality Protection for Distributed Sensor Data Aggregation," In 27th IEEE International Conference on Computer Communications (Infocom), 2008.

[18] W. Zhang, C. Wang and T. Feng, "GP2S: Generic Privacy-Preservation Solutions for Approximation Aggregation of Sensor Data," In 6th Annual IEEE International Conference of Pervasive Computing and Communications 2008.

[19] Shi, Runhua et al., "A (t, n) Secret Sharing Scheme for Image Encryption", Congress on Image and Signal Processing, 2008.

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

[21] Hai Vu_, Thuc Nguyen et al., 'PEQ: A Privacy-preserving Scheme for Exact Query Evaluation in Distributed Sensor Data Networks', 28th IEEE International Symposium on Reliable Distributed Systems, 2009.

[22] 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, JANUARY 2011.

[23] Ka Lung Law and Minh N. Do," Multidimensional Filter Bank Signal Reconstruction From Multichannel Acquisition",

IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 20, NO. 2, FEBRUARY 2011.

[24] Florian Luisier, Thierry Blu, and Michael Unser," Image Denoising in Mixed Poisson–Gaussian Noise", IEEE TRANSACTIONS ON.

[25] Guangming Shi, Dahua Gao, Xiaoxia Song, Xuemei Xie, Xuyang Chen, and Danhua Liu," High-Resolution Imaging Via Moving Random Exposure and Its Simulation", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 20, NO. 1, JANUARY 2011.

[26] Yun-Fu Liu, Jing-Ming Guo, and Jiann-Der Lee, "Inverse Halftoning Based on the Bayesian Theorem", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 20, NO. 4, APRIL 2011.

[27] Egil Bae, Juan Shi, and Xue-Cheng Tai," Graph Cuts for Curvature Based Image Denoising", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 20, NO. 5, MAY 2011.

[28] Yingxi Xu, Chunling Gao, Zeyu Sun, Chuanfeng Li," Improved Image Matching and Encryption Algorithm Based on Polar Transform and Fourier Transform", International Review on Computers and Softwares, Vol. 7 N. 2(Part B), pp. 701-705, March 2012.

[29] Che-Wei Lee Et al., „A Secret-Sharing-Based Method for Authentication of Grayscale Document Images via the Use of the PNG Image With a Data Repair Capability", IEEE Transactions on Image Processing, 2012.

6/7/2013