International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Extended Capabilities of Feature-Extraction for Digital Image Sharing by Diverse Image Media

Snehal Pawar[1], Shubhangi Suryawanshi[2]

[1]ME Student Dept of Computer Engineering, G.H. Raisoni Institute of Engineering and Technology, Wagholi, Pune

[2]Assistant Professor at Department of Computer Engineering, G.H. Raisoni Institute of Engineering and Technology, Wagholi, Pune

Abstract: ***In accustomed visual secret sharing algorithm issue like hide secret images in shares that may be printed on transparencies or are encoded and stored in a digital form exist. The shares can be either meaningful images or noise-like pixels, which will definitely arouse suspicion and increase interception threat during transmission of the shares. Therefore, VSS schemes have limitation that it suffers from a transmission risk problem for the secret itself and for the participants who are involved in the VSS scheme. To overcome the problem of transmission risk, we proposed a natural image based VSS scheme (NVSS scheme) which can share secret images via different carrier media to protect the secret and the participants during the transmission phase. We are introducing new technique i.e. k-means clustering for extracting the features of the natural shares and with that there will be an additional permutation and normalization technique on halftone visual cryptography which will replace the random selection of pixel which we were using for generating the noise -like share before the shares moves to pixel swapping. The unaltered natural shares are various and inoffensive, thus to great extent reducing the transmission risk problem. Experimental results indicate that the proposed approach is an excellent solution for solving the transmission risk problem for the VSS schemes.***

Keywords: Feature Extraction, Natural shares, Transmission risk, Visual secret sharing scheme, K-means clustering, Extended visual cryptography scheme

1. Introduction

With swift advancement in Internet and digital imaging technology, there are more and more ways to easily design, post, and distribute images. Here we are focusing on the relationship between digital imaging and privacy conservation, visual cryptography and secret image sharing is an entire initiation to novel security techniques and sharing-control mechanisms used to protect in oppose to unauthorized data access and secure dissemination of sensitive information.

Image data security and image-based authentication methods recommend systematic solutions for controlling how private data and images are made accessible only to specified people. Obligatory, to the design of systems used to manage images that contain fragile data—such as medical evidence, electronic voting framework and financial transactions—the techniques presented are useful to counter conventional encryption proficiency, which do not scale well and are less effective when applied directly to image files.

Secret images can be of different kinds: images, handwritten documents, photographs and others. Sharing and delivering secret images is also called as a visual secret sharing (VSS) scheme. The original inspiration of VC is to securely allocate secret images in non-computer-aided environments; however, machines with computational powers are pervasive (e.g., smart phones). Thus, sharing visual secret images in computer-aided environments has become an major affair today. Accustomed shares, which is made up of many random and meaningless pixels, fulfills the security need for protecting secret contents, but they suffer from two drawbacks: first, there is a high transmission risk as it is holding noise-like shares which will unable attacker's speculation and the shares may be obstructed. Thus, the threat to both the participants and the shares increases, in turn increasing the possibility of transmission incompetent. Second, the meaningless shares are not user friendly. As the amount of shares grows, it becomes more problematic to manage the shares, which never furnish any information for recognizing the shares. The foregoing analysis into the Extended Visual Cryptography Scheme (EVCS) or the user-friendly VSS scheme provided some productive solutions to subsist with the management issue. The shares hold many noise-like display low-quality images or pixels. Such shares are easy to recognize by the unguarded eye, and participants who dispatch the share can simply escort to speculation by others. By acquiring steganography techniques, secret images can be hided in cover images that are halftone gray images and true-color images. However, the stego-images still can be spotted by steganography analysis technique. Therefore the existing VSS schemes still must be scrutinized, for minimizing the transmission risk issues for carriers and shares. A method to minimize the transmission risk is an important problem in VSS schemes.

In this study, we spot a VSS scheme, known as natural image–based on VSS scheme (NVSS scheme), to minimize the intercepted threat during the transfer phase. Basically, accustomed VSS schemes uses a unity carrier (e.g., may be transparencies or digital images) for sharing images, which limits the feasibility of VSS schemes. In the recommended scheme, we traverse the possibility of using different media for sharing digital images. The carrier media in the scheme holds printed images, digital images, hand-painted pictures, images taken from a camera and so on. Applying a diversity of media for sharing the secret image expands the level of complication of intercepting the shares.

The suggested NVSS scheme can allocate a digital secret image over n-1 arbitrary natural images (hereafter known as natural shares) and one share. So there is no obligation of redesigning the contents of the natural images, the proposed approach distil or stipulate features from each natural share. These unchanged natural shares are totally edible, thus greatly minimizing the interception probability of these shares. The provoked share that is noise-like can be hidden by using data hiding method to enhance the security level and making it more secure as well as easy to transmit during the transmission phase.

The NVSS scheme uses multiple media as a carrier; hence it has many attainable framework for sharing secret images. For example, we make an assumption that a dealer selects *n* - 1 media as a natural shares for sharing a secret image. To diminish the transmission risk, the dealer can select an image that is not easily reckoned as the content of the media i.e. the user can manipulate any normal image (e.g., hand-painted pictures, landscape, portrait photographs, pictures taken from a camera and flysheets). The digital shares can be accumulated in a participant's digital devices (e.g., digital cameras, tablets, computers, laptops or even a smart phones) to minimize the risk of being suspected. The printed media (e.g., hand-painted pictures or flysheets) can be transmitted via postal or direct mail marketing services or even by e-mail. In such a manner, the transmission channels are also multiple, further maximizing the transmission threat and thus enhancing the security for the images.

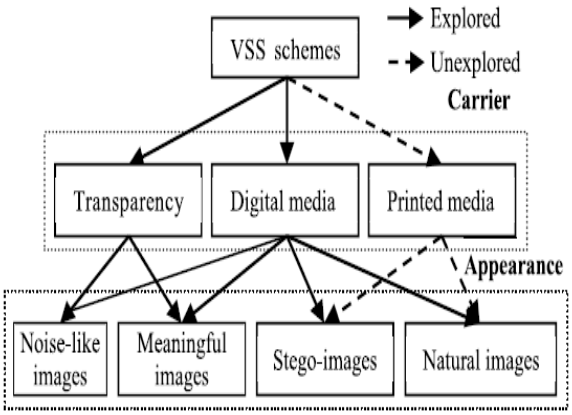

Figure 1: The classification of the existing VSS research from the viewpoints of carriers.

In this proposed scheme, we design effective encryption/decryption algorithms for the (n, n) -NVSS scheme. The propound algorithms are applicable to digital and printed media. The feasible ways to hide the generated share are also examined. The offered NVSS scheme not only has a high degree of user friendliness and manageability, but also it minimizes transmission risk and enhances the security of participants and shares.

The remaining part of this paper is organized as follows. In section 2, we elaborate the Literature Review on capabilities of feature-extraction for digital or printed image sharing by multiple image media . Whereas, section 3 describe the Proposed scheme in which brief description of Hypothesis and Proposed architecture can be observed. In section 4 the Proposed Algorithm is spotted. In section 5, 6 and 7 Acknowledgement and possible Future Work and References is discussed.

2. Literature Review

Visual cryptography concept came into focus to hide the secret text or image behind another image also this concept used by M. Naor and A. Shamir. These can be done by generating the dissimilar shares of the image. Then after applying the process of encryption to encrypt that image and send to the proper destination. On the other hand that received shares can be merged to get the original image. But it deteriorate from the problem of share management, because they generate more than one share to hide the secret image [2].

The problem occurred in the VC scheme that can be defeated by the extended visual cryptography scheme. This VC schemes work on the Share management problem. To get better solution Kai-Hui Lee and Pei-Ling Chiu uses a meaningful cover image concept. This sort of VC scheme uses binary images. For the purpose of managing shares this technique first construct the meaningful share using an optimization technique. And in the next step it will use cover images that can be added in each share directly by using the stamping algorithm. As this VC scheme uses binary image they are not able to sustain the quality of recovered image [3].

The purpose of this scheme is to generate noise-like random pixels on shares to hide secret images which can be done in the conventional visual secret sharing. But it suffers a management problem, for the reason of which dealers cannot visually identify each share. This management problem is resolved by the extended visual cryptography scheme (EVCS), which adds a meaningful cover image in every share. However, the foregoing approaches involving the EVCS for general access structures deteriorate from a pixel expansion problem [4].

A construction of EVCS which is noticed by embedding random shares into meaningful covering shares, and we name it the embedded extended visual cryptography scheme (embedded EVCS). A construction of EVCS which was realized by embedding the random shares into the meaningful covering shares. A method to revamp the visual quality of the share images. Embedded EVCS has many specific advantages against different well-known schemes, such can deal with grey-scale input images, has smaller pixel expansion, always unconditionally reliable, and thus does not require complementary share images, one participant only requires to carry one share and can be applied for general access structure [5].

Extended VCS is that where hyper graph colorings are cast-off in constructing meaningful binary shares. Since hyper graph colorings are constructed by random distributed pixels, the resultant binary share holds strong white noise leading to inadequate results. An encryption method to built color

EVCS with VIP (Visual information pixel) synchronization and error diffusion for visual quality refinement. [6].

Gray level visual cryptography is designed to provide the better quality image in the VC scheme. Here they applying adaptive order dither technique as well as existing visual cryptography scheme for binary image to construct the shares. This technique reduces the size of decrypted images. The quality of decrypted image will be enhanced as compared to the EVCS scheme. But this mechanism suffers from the pixel expansion problem [7].

Pixel expansion problem can be further considered in the Halftone VC scheme. This technique uses Halftone error diffusion method to convert secret image and the visible image in to the halftone image. Halftone shares are generated, because the secret information is embedded into the halftone shares and it will give the output as recovered good quality of image. This technique can circumvent the transmission risk problem [8].

Mechanism which is used for halftone technique is error diffusion method, which take one gray scale image and convert it into binary image by applying halftone technique?. In this binary share images, place secret image pixel in to each share image by applying void and cluster algorithm. The reconstructed image is procured by superimposing two share images. As it is an very good method but still there is a tradeoff between pixel expansion and contrast loss of original image. In this method the size of pixel is same as original image pixel size. That seems relieved secret image size and original image size is same so it diminish the problem of pixel expansion. In this technique random grid R is defined as a two dimensional array of pixels. Each pixel is either transparent (white) or opaque (black) by a coin flip procedure The numbers of transparent pixels and opaque pixels are probabilistically same and the average opacity of a random grid is 50% [9-11].

Color image with natural shadow visual cryptography scheme uses the natural image to hide the secret information and one noise-like share image. For the encryption process it needs to alter the natural image. So that this type of VC scheme suffers from texture problem i.e. original texture of the image will be adrift [12].

In order to guarantee the secret image that transmits through the network will not be stolen, the secret images must be encrypted, the concept of this process is called secret image encryption. The random grid algorithm is used to encrypt the secret image. The scheme can adjust distortion to infinitesimal it also improves the problem of decoding. The secret image consists of a collection of pixels, where each of pixel is associated with a grey level ranging from white to black and each pixel is handled individually. Any set of qualified participants stack their transparencies they can correctly recover the image shared by the dealer. The security of the scheme, since it implies that, even by inspecting all their shares, some set of forbidden participants cannot gain any information on the value of the grey level of the distributed pixel. [13-15].

Tsung- Lieh Lin et al have together designed a framework for visual secret sharing scheme (VSS) with numerous secrets without the pixel expansion. In this framework, the visual secret sharing methods has been assign in a different way, which is used through the two binary secret images on two rectangular share images that promotes non expansion of pixels leads to high image quality. The main advantage of this method is several secrets were used. As the result of this, the framework has very good quality in recovering the secret image [16].

A multi-level visual secret-sharing scheme with no size enlargement of pixels was put forth by Yung-Fu Chen et al. here the visual secret sharing scheme prefers a block of secret image in accordance to the similar sized block in all of the share images with no pixel size expanding. In this manifesto, histogram width equalization (HWE) and histogram depth equalization (HDE) were the two techniques that were used for creating the corresponding share images. That outcomes in the increase in the quality of the reconstructed secret image when compared with other techniques [17].

An efficient k-means clustering algorithm taken into scenario as the emergence of the extracted feature may remain some texture of the original image. It will out-turn in decreasing the randomness of the generated share and finally diminish security of the scheme. To fortify clarity

and security of the proposed scheme, we emerge a feature extraction method to contribute natural shares into clusters which will improve the quality of recovered image. The drawback that is instead of generating noise-like share with random selection we will propose permutation and normalization techniques so as to procure high degree of security.[18]

3. Proposed Scheme

3.1 Hypothesis

The proposed (n, n)-NVSS scheme arrogate arbitrary n-1 natural shares and one precipitated share as media to share one digital original color secret image that has 24-bit/pixel color depth.

The purpose of this study is to minimize the transmission risk of shares by using multiple and innocuous media. We make the following hypothesis:

1) When the amount of delivered shares grows, the transmission risk also get increase.
2) The transmission threat of shares with a meaningful cover image is less than compared with noise-like shares.
3) The transmission risk drops as the quality of the meaningful shares increases.
4) The natural images without artificially revamped or modified contents have the lowest transmission risk, lower than that of meaningful shares and noise-like.
5) The present quality of distortion-free original-color images is superior to that of halftone images.

In the NVSS scheme, the natural shares can be gray or color photographs of family activities, scenery or even flysheets, bookmarks, web images, hand-painted pictures or photographs. The natural shares is either in digital or printed form. The encryption technique only distil features from the natural shares; it does not refine the natural shares. The innocuous natural shares can be distributed by participants who are intricate in the NVSS scheme, by the holders of the photographs, or via public Internet. Since the natural shares are not modified, it is likely that they will not induce speculation during transmission. Even if the natural shares are obstructed, it will not be possible to uphold that there is any unseen data in the images before reaching the decryption threshold. In such a framework, the transmission of the innocuous natural shares is more assured than the transmission of shares in another physique, such as noise-like or meaningful shares. Another share, which is created by the secret image and features that are distilled from n-1 natural shares, can be concealed behind other media and then distributed by a well-disciplined person or via a high-security transmission channel.

When the amount of shares *n* increases, based on Hypothesis 1, the transmission risk of the conventional VSS schemes increases promptly. On the contrary, regardless of the increasing in amount of shares, the proposed NVSS scheme inevitably requires only one generated share. Because the natural images have immensely high security, even though the number of innocuous natural shares is also proportional to *n*, the transmission risk of the proposed scheme will increase immensely somewhat as *n* increases.

In the subsisting VSS schemes, the sort of shares incorporate noise-like shares, shares with halftone cover images and shares with binary cover images; the latter has the ultimate display quality among the above-mentioned kinds of shares. Furthermore, the display quality of the proposed original-color natural shares is surpassing to that of shares with halftone cover images. Based on Hypothesis 2 and 3, the transmission threat of the true-color natural shares is the lowest between the existing approaches. Based on Hypothesis 4 and 5, the proposed (*n, n*)-NVSS scheme delivers *n*-1 unaltered natural shares that possess a very low transmission threat, this property greatly minimize the transmission cost of distributing *n*-1 natural shares of the scheme. Compared with traditional (*n, n*)-VSS schemes, which must carefully distribute *n* noise-like shares, the proposed (*n, n*)-NVSS scheme must furnish a single generated share in a high-security manner. When the transmission cost is restricted, the proposed scheme using unaltered natural shares can greatly minimize transmission threat.

3.2. Proposed Architecture

As Fig.2 shows, the encryption technique of the proposed (n, n)-NVSS scheme, $n \geq 2$, includes two main part: feature extraction and encryption. In feature extraction part, 24 binary feature images are extracted from every single natural share. The natural shares (N_1,..., N_{n-1})_ include n_p printed images (symbolized as P) and n_d digital images (symbolized as D), $n_p \geq 0$, $n_d \geq 0$, $n_p + n_d \geq 1$ and $n = n_p + n_d + 1$. The feature images (F_1,...., F_{n-1}) that were distilled from the similar natural image eventually are combined to make one feature image with 24-bit/pixel color depth.

In the encryption part, the *n*-1 feature images (F_1,…, F_{n-1}) with 24-bit/pixel color depth and the secret image accomplish the XOR operation to precipitate one noise-like share S with 24-bit/pixel color depth. The resultant share S is called the generated share. The *n* -1 innocuous natural shares and the created share are *n* shares in the (*n, n*)-NVSS scheme. When all *n* shares are collected, the decryption end distil *n*-1 feature images from all natural shares and then perform the XOR operation with share S, to acquire the recovered image, as shown in Fig.2. Each module of Fig.2 is described in the upcoming sections.

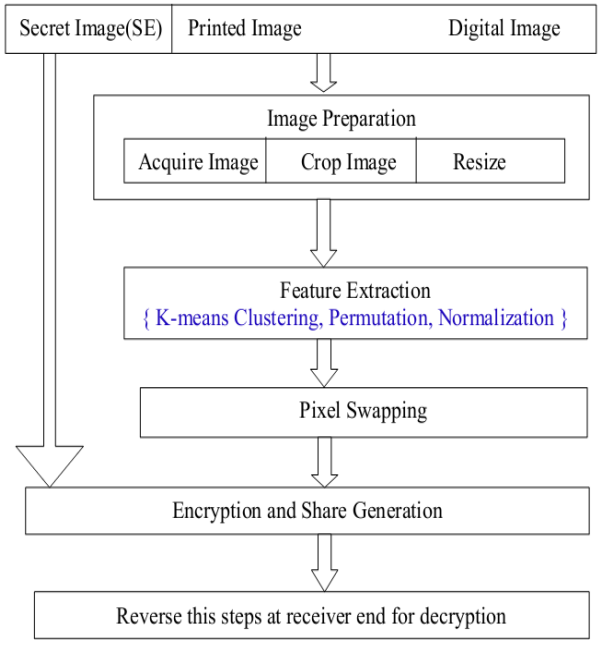

Figure 2: The encryption/decryption process of the (*n, n*)-NVSS scheme

4. Proposed Algorithm

4.1 The Feature Extraction Module

In this section the illustration of the feature extraction module that distil feature images from the natural shares. The module which is the crucial module of the feature extraction process is relevant to printed and digital images concurrently. Then, the composition of image and the pixel-swapping modules are instigate for processing printed images.

There are some subsisting techniques that are used to distil features from images, such as the wavelet transform. Although, the emergence of the extracted feature may remain some texture of the true image. It will out-turn in decreasing the randomness of the generated share and finally diminish security of the scheme. To fortify security of the proposed scheme, we emerge a feature extraction method to contribute noise like feature images from natural images such that the generated share is also a noise-like image.

Assume that the area of the natural shares and secret image are w × h pixels and that each natural share is distributed into a number of k clusters We explicate the notations as follows:

Algorithm 1 - Feature Extraction Algorithm

Parameters:
Algorithm FE()
Input: N,K, K-1, P_{noise}
Output: Feature matrix
1. Divide N into K-1 arbitrary clusters
2. For each cluster repeat step 3-8
3. For all $x_1 \le x \le x_k$, $y_1 \le y \le y_k$, determine pixel value $H^{x,y}$ by Eq. (1)
4. Calculate M i.e. M-Mean or Centroid
5. For all $x_1 \le x \le x_k$, $y_1 \le y \le y_k$, determine pixel value $f^{x,y}$ by Eq. (2)
6. Calculate Q_s by Eq. (3)
7. Calculate Q_c by Eq. (4)
8. Instead of selecting random values for black pixel, white pixels and for generating noise-like share we are introducing new technique i.e. With the help Half-tone visual cryptography [8] we are enhancing it with permutation and normalization technique in order to reduce the transmission threat, boost security and for transparent recovered image
9. Output as Feature Matrix.

The above algorithm-1 can be used for feature extraction of natural shares of either printed or digital image. An efficient k-means clustering technique used here for extracting the features of natural image into clusters which reduce the transmission threat as we have seen in hypothesis-1 i.e. When the amount of delivered shares grows, the transmission risk also get increase. Here k-means will help us to group the similar features into clusters which will diminish the confusion as the number of share increases and at the end will help us to acquire transparent recovered image and previously the noise-like share is procured from random selection of pixel which have high degree of security and transmission threat for that we proposed permutation technique and for calculating the black and white pixel value the technique in Half-tone cryptography being defined on that we are introducing the normalization process which will remove the random selection of pixel values for generating one noise-like share.

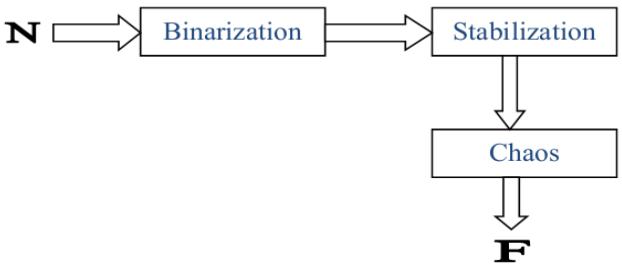

Figure 3: The block diagram of the feature extraction.

As shown in Fig.3, the feature extraction module is composed of three processes—binarization, stabilization, and chaos .In First part, a binary feature matrix is extracted from natural image N through the binarization process. Then, the stabilization balances the manifestation frequency of values 1 and 0 in the matrix. And Finally, the chaos process disperse the clustered feature values in the matrix.

4.2 The Image Preparation and Pixel Swapping Processes

The image preparation and pixel swapping processes are used for preprocessing printed images and for post-processing the feature matrices that are distilled from the printed images. The printed images were stipulated for sharing secret images, yet the contents of the printed images must be obtained via computational devices and then be changed into digital data.

Figure 4: An example of the image preparation process: (a) a hand-painted picture (3264 × 2448 pixels) was seized by the digital camera on the iPhone 4S, (b) the resultant picture (512 × 512 pixels).

To diminish the difference in the content of the acquired images between the encryption and decryption processes, the sort of the acquisition devices and the parameter settings (e.g., resolution, image size) of the devices should be the similar in both processes. The next stride is to crop the additional images. Ultimately, the images are resized so they have the same dimensions as the natural shares. An specimen of the image preparation process is demonstrated in Fig.4. The hand-painted picture is sketch on A4 paper. First, the picture is seized using a popular smart phone, Apple iPhone 4S, as shown in Fig. 4(a). The picture then is processed using the Paint application in Microsoft Windows 7 platform. Eventually, the picture is cropped and resized as a rectangular image as shown in Fig. 4(b). The resultant picture is used in the experiments in the succeeding section.

The acquired digital images in the encryption and decryption phases are not the similar. These deformation result in noise that become noticeable in the recovered images. When a huge volume of noise clusters all together, the image is badly deranged, which may makes it intolerable for the naked eye to recognize it. The pixel-swapping process is used to subsist with this problem. Once the feature extraction process completes then, a pixel-swapping module is applied to randomize the true spatial correlation of pixels in a printed image. In other term, the pixel-swapping module assist tolerance of the image distortion caused by the image preparation process.

4.3 Encryption/ Decryption Algorithms

The propound (n, n)-NVSS scheme can encipher a true-color secret image by one noise like share and n -1 innocuous natural shares. For single image, we designate a bit with the same weighted value in the similar color as a bit plane; then a original color secret image has 24 bit-planes. Hence, the noise-like share and the feature images also are enlarged to 24 bit-planes. Each bit-plane of a feature image subsists of a binary feature matrix that equates to the similar bit-plane as the secret image.

Before encryption (resp. decrypt) of each bit-plane of the secret image, the proposed algorithm first extricate n-1 feature matrices from n-1 natural shares. Then the bit-plane of the secret image (resp. noise-like share) and n-1 feature matrices execute the XOR operation (to procure the bit-plane of the share image (resp. recovered image). Therefore, to encrypt (resp. decrypt) a true-color secret image, the encryption (resp. decryption) procedure must be accomplished iteratively on the 24 bit-planes.

Algorithm 2 (n, n)-NVSS Encryption/Decryption Algorithm

Algorithm NVSS()
Input: S, $N_1, \ldots, N_{n_p+n_d}$, n_p, n_d, b, P_{noise}, ρ, t
Output: $\overline{S}$

1. Initialize the random number generator G by the seed ρ
2. $n \leftarrow n_p + n_d + 1$
3. $\forall 1 \le \alpha < n, \forall \varphi \in \{R, G, B\}, \mathrm{FI}_{\alpha,\varphi} \leftarrow 0$
4. $\forall 1 \le \alpha < n, \forall \varphi \in \{R, G, B\}, \forall 0 \le i \le 7$, **repeat** Steps 5 and 6
5. **Call** procedure FE(N_α, b, P_{noise}, $\boldsymbol{F}$)
6. $\forall (x, y), x \in [1, w], y \in [1, h], p^{x,y}_{\alpha,\varphi} \leftarrow p^{x,y}_{\alpha,\varphi} + f^{x,y} \times 2^i$
7. **If** $n_p = 0$ **then goto** Step 12
8. $\forall 1 \le \alpha \le n_p$, **repeat** Steps 9—11 t times
9. Randomly selects $(x_1, y_1), x_1 \in [1, w], y_1 \in [1, h]$
10. Randomly selects $(x_2, y_2), x_2 \in [1, w], y_2 \in [1, h]$
11. $\forall \varphi \in \{R, G, B\}$, exchange values of $p^{x_1,y_1}_{\alpha,\varphi}$ and $p^{x_2,y_2}_{\alpha,\varphi}$
12. $\forall \varphi \in \{R, G, B\}, \overline{S}_\varphi \leftarrow S_\varphi \oplus \mathrm{FI}_{1,\varphi} \oplus \cdots \oplus \mathrm{FI}_{n-1,\varphi}$
13. **Output** $\overline{S}$

The above algorithm -2 can be used for the encryption and decryption phases by setting diverse limitations as:
1) Encryption: Input images invoke n-1 natural shares and one secret image. The resultant image is a noise-like share.
2) Decryption: Input images invoke n -1 natural shares and one noise-like share. The resultant image will be recovered image.

5. Future Work

Once the Decryption process has been done, Recovered Image will be created. By using comparing the pixel values of Secret image and Recovered image we can originate that there is no Pixel Expansion or Pixel corruption in the Recovered image. But here we see no change between Secret image and Recovered image. An optimized technique can be used for feature extraction of natural image and share generation as still it's so prolonged and complicated process

6. Acknowledgment

I express my gratitude towards Prof. Shubhangi Suryawanshi, of Department of Computer Engineering, G. H. Raisoni Institute Of Engineering and Technology, Wagholi, Pune for her valuable advice and motivation. No words are adequate to convey my recognition to Dr. A. R. Dani for their unwavering encouragement. Hereby, the authors appreciate the anonymous reviewers for their valuable comments.

References

[1] Pei-Ling Chiu and Kai-Hui Lee, ―Digital Image Sharing by Diverse Image Media" , IEEE Trans on Information Forensics and Security, vol. 9, no. 1, pp. 88–98, January. 2014.
[2] M. Naor and A. Shamir, ―Visual cryptography," in Advances in Cryptology,vol. 950, pp. 1–12, New York, NY, USA: Springer-Verlag, 1995
[3] C. N. Yang and T. S. Chen, ―Extended visual secret sharing schemes: Improving the shadow image quality" ,Int. J. Pattern Recognit. Artif. Intell , vol.21, no. 5, pp. 879–898, Aug. 2007.
[4] K. H. Lee and P. L. Chiu, ―An extended visual cryptography algorithm for general access structures", IEEE Trans on Information Forensics and Security, vol. 7,no. 1, pp. 219–229, Feb. 2012.
[5] F. Liu and C. Wu, ―Embedded extended visual cryptography schemes" ,IEEE Trans on Information Forensics and Security, vol. 6, no. 2, pp. 307–322, Jun. 2011.
[6] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, ―Extended capabilities for visual cryptography", Theoretical Comput. Sci., vol. 250,nos. 1–2, pp. 143–161, Jan. 2001.
[7] I. Kang, G. R. Arce, and H. K. Lee, ―Color extended visual cryptography using error diffusion", IEEE Trans on Image Process, vol. 20, no. 1,pp. 132–145, Jan. 2011.
[8] Z. Zhou, G. R. Arce, and G. D. Crescenzo, ―Halftone visual Cryptography", IEEE Trans on Image Process. vol. 15, no. 8, pp.2441– 2453, Aug. 2006.
[9] Z. Wang, G. R. Arce, and G. D. Crescenzo, ―Halftone visual cryptography via error diffusion", IEEE Trans on Information. Forensics and Security, vol. 4,no 3, pp. 383–396, Sep. 2009.
[10] R. Z.Wang, Y. C. Lan, Y. K. Lee, S. Y. Huang, S. J. Shyu, and T. L. Chia,―Incrementing visual cryptography using random grids"Opt. Commun., vol. 283, no. 21, pp. 4242– 4249, Nov.2010.
[11] P. L. Chiu and K. H. Lee, ―Asimulated annealing algorithm for general threshold visual cryptography schemes", IEEE Trans on Information Forensics and Security, vol. 6, no. 3, pp. 992– 1001, Sep. 2011.
[12] K. H. Lee and P. L. Chiu, ―Image size invariant visual cryptography for general access structures subject to display quality constraints", IEEE Trans on Image Processing, vol. 22, no. 10, pp. 3830–3841, Oct. 2013.
[13] T. H. Chen and K. H. Tsao, ―User-friendly random-gridbased visual secret sharing", IEEE Trans. Circuits Syst andVideo Technol., vol. 21,no.11, Nov. 2011.

[14] T. H. N. Le, C. C. Lin, C. C. Chang, and H. B. Le, ―A high quality and small shadow size visual secret sharing scheme based on hybrid strategy for grayscale images", Digit. Signal Process., vol. 21, no. 6, pp. 734–745, Dec. 2011.
[15] D. S. Tsai, G. Horng, T. H. Chen, and Y. T. Huang, ―A novel secret image sharing scheme for true-color images with size constraint", Inf. Sci., vol. 179, no. 19, pp. 3247–3254, Sep. 2009.
[16] T sung-Lieh Lin et al, ――A novel visual secret sharing (VSS) scheme for multiple secrets without pixel expansion", Expert Systems with Applications, vol. 37, pp. 7858–7869, 2010.
[17] Yung-Fu Chen , Yung-Kuan Chan , Ching-Chun Huang , Meng Hsiun Tsai c, Yen-P ing Chu ――A multiple-level visual secret - sharing scheme without image size expansion", Informat ion Sciences, vol. 177 , pp. 4696–4710, 2007.
[18] Tapas Kanungo, David M. Mount, Nathan S. Netanyahu, Christine D.Piatko, Ruth Silverman, and Angela Y. Wu, ―An Efficient K- Means Clustering Algorithm: Analysis and Implementation",IEEE Trans. Machine Intelligence, Vol. 24, No.7,July. 2002.