An Advance Halftone Secure Secret Sharing Scheme with Error Diffusion Technique in Visual Cryptography

I. Diana Judith
Research Scholar
Department of Computer Science and Engineering
PRIST University, Vallam, Thanjavur,
Tamil Nadu, India

G.J. Joyce Mary, PhD
Research Supervisor
Department of Computer Science and Engineering
PRIST University, Vallam, Thanjavur
Tamilnadu, India

ABSTRACT
As there is rapid growth in the digital world, security becomes a major concern for data transmission using image techniques. Visual cryptography (VC) is recent technology in the cryptographic scheme, which is utilized them secret images to be shared securely and also its data is preserved with higher confidentiality. In general, when sender the forwards the secret images which is split into several images and keeps its hidden data in it, so when all the distributed images are aligned and stacked unitedly, they incline to exhibit the secret image data to the receiver. Previous visual cryptography technology, privacy of the share images is not preserved because of the other duplicate shares which can so easily alter or insert some other images, it remains to be the major challenge in the VC. The shared images are obtained by using the basic knowledge of visual (2,2) scheme. To overcome those kind of security issues, we propose the advance halftone secure secret sharing scheme with error diffusion techniques in the visual cryptography.

At first, the visible images is translated into halftones shares by employing halftone error diffusion scheme. Next, the secret image is converted into halftone shares containing efficient visual information. Thus the shared images are disseminated to particular participants and then they are extremely enforced to reveal the secret images. When the shares are generated, it is uses the halftone processing, which first the encryption the images with high quality secret images and then decryption the secret images with same image quality by using diffusion methodology with high quality images. Form the experimental results, it is illustrated that the secret images have very minimum error difference, secret images data is highly impossible to be retrieved by fraudulent shares. Thus the proposed method a provides higher security with quality secret images for the encryption and decryption of the images, which contains fast execution, accuracy and minimum error value.

Keywords
Advance Halftone, Error Diffusion, Secret Sharing Scheme, High Quality and Visual Cryptography.

1. INTRODUCTION
As due to the rapid development of the computer technologies and the internet utilization are incrementally associated with the developing popularity of the data transmission in the network coverage [1]. In various applications, such as military data, important images commercial communications data and others

essential images should be kept secret. There are multiple schemes for the image protection has been introduced to provide the security for the secret images in the visual cryptography. Particularly, visual cryptography permits us to significantly share secret images to the trusted shares in the data transmission. Visual cryptography is very efficient scheme in which, it can share the secret images to the multiple trusted parties [2]. At first, it was proposed by the Adi Shamir and Moni Naor [1] in the year of 1994. In generally visual cryptography, secret images can be identified without the help of the participation by laying over the shares on transparencies together.

Hence, the secret sharing images is termed as one of the cryptographic technology, in which the secret images is classified into a number of share images with or without change of the secret images would be retrieved by predetermining collection of shared images or combining all the share images [3]. Basically in any one of the al secret sharing images protocol, would always contains the participants and dealer. Dealer is an entity who deals with the process of the constructions and disseminates the shares to different dissemination participants. Participants are the important substances who obtain the share images from shares and participate in secret image creation process. A misbehavior entity may meddle the shared images, which can alter the secret images in order to make fraudulent while sharing the images to the participates. This leads to the security concern and secret images integrity is lost, which needs the basic necessity for the improving the secret image sharing scheme.

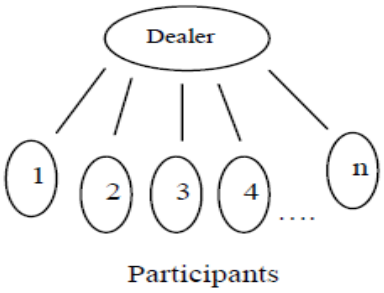


Fig 1: Share Creation and Distribution

The main reason to provide the security for the secret sharing scheme is determined as common consideration to all the shares and participants involved are regarded as honest. In case, if there is any entities remains as fraudulent and attempts to affect the shares, secret image recovery would be damaged [4] . Therefore, it is very necessary to provide security to the secret image sharing. Inside the secret sharing schemes, if any one or more of the participants, where participants is represented as k, in this condition (k<=n) stack their shares the images altogether, the secret images would be retrieved, if ***k-1*** participants tries to rebuild the original images which is considered as secret images, no data relevant to the secret

images can be exposed. They are two different kind of visual cryptography schemes (VCS) are demonstrated below [3]:

A. (n,n) Visual Cryptography Schemes VCS:
In this technique, which separates the secret images into **n** shares, and complete shares are required to detect the secret image. Therefore, $n \geq 2$, where 'n' is defined as a integer. A(2,2) visual cryptography schemes is regarded as specific condition of (n,n) VCS [3] .

B. (k,n) Visual Cryptography Schemes VCS:
This technique classifies the secret image shares into ***n*** shares, and ***k-out-of-n*** shares are required to detect the secret image, where ***2≤k≤n***, and ***k*** and ***n*** both are represented as an integer. However, there is specific condition for this technique such as (2,3) visual cryptography schemes and etc [3].

Thus Mahmoud and Humbe [3] distinguished the schemes of visual cryptography and given approximately interpretation on the base of few different measures likes share construction, pixel expansion, images quality number of secret images and format of secret image.

2. LITERATURE REVIEW

Moni Naor and Adi Shamir et al [1] had proposed the Visual Cryptography. In their proposed methodology, the secret image is accumulation of white and black pixels, each pixel is treated separately. The major demerits of this method that was decryption section, which was inactive or lost in the contrast. Contrast is very essential inside visual cryptography due to the clearness of the retrieved secret images is depend on visual human system. In this proposed system, the shares creation can be demonstrated by a 2-out-of-2 VCS which known as (2,2)-VCS. The creation process is depend on the following collections of 2×2 matrices.

Srinivasan nagaraj et al [4] had discussed about the elaborated size of the internet and huge communication throughout the networks and also medical requires digital images particularly in the need of security, which turns to be critical role. The proposed encryption technique utilizing elliptic curve cryptography with random matrix operations for obtaining the securing shares images that broadcasts over a public unsafe channel. They utilize the most essential groups of encryption algorithms for the images, such as chaos based selective methods and non chaos-based selective methods

Xuehu Yan et al [5] have introduced three common threshold structure methods from particular condition. The structure threshold visual cryptography schemes are also liberal visual cryptography schemes without the pixel extension. The shares images of the shadow are random noise-like, hence, they have suggested CVCS has no cross disturbance of secret image in the shadow images framework. The liberal visual cryptography scheme suffers from the quality images for the secret images, recovered secret image can be obtained from the CVCS. When the shadow images are accumulated, cannot recover any data from the secret image which could be identified, it represents the security of the CVCS.

Paulius Palevicius et al [6] have demonstrated the consolidation of dynamic visual cryptography method depend on the individual performance of time averaging geometric with Gerchberg–Saxton algorithm in the visual cryptography. They had made analysis on the stochastic grating, that is utilized to combine the secret data into a single secret image. The hidden data can be visually decrypted by a human eye if only the amplitude of harmonic oscillations matches to an exact predetermined value. The visual image cryptography scheme is totally depend on the computer created holography, averaging optimal time and importance's of dynamic visual cryptography were provided.

R. Vijayaraghavan, S. Sathya et al [7] have introduced a bit slice rotation technique with higher security for the digital secret image. Bit Plane Slicing is utilized to classify the digital secret image into eight bit planes. Later on, these bit plane is elevated to rotate in such a manner that advanced encrypted image that makes very complex. The categorization of bit plane is utilized for examining the importance of each and every bit image. It is utilized to determine the pixel of each image. The proposed mechanisms requires rotation of bit planes for obtaining highly secure encryption image. By using this technique, image can be scrambled depend on the secret image with significant technique even it is tapped, the data cannot be retrieved. It is very essentially required for image compression due to its efficiency in the high coding.

Zhicheng Ni et al [8] have illustrated about the novel reversible information hiding algorithm, which can retrieve the exact original image in the visual cryptography without any noise from the secret image after the hidden information have been extracted. The proposed algorithm applies the minimum points or zero points of the image histogram and marginally changes the pixel values of grayscale images to combine information into the image. This can hide more information when compared to the existing RDH algorithms. It is verified analytically and demonstrated experimentally that the peak signal-to-noise ratio (PSNR) of the secret image created by this technique against the original image is assured above than 48 dB. This lower bound of PSNR is highly greater than that of all reversible information hiding. The proposed technique has the computational complexity level is higher and the execution time is faster.

Asha S.N et al [9] has discussed about the visual cryptography is a technique where the secret image is classified into three or more shares, it is termed as shares and the secret image is exposed by covering the shares without any complex computation regarded. They have defined how to execute the extended visual cryptography scheme by embedded more secret image as an input image. The secret image visual quality parameters like MSEm, MAXERROR and PSNR are determined in this section. The creations of covering shares images are demonstrated by using half toning method with the dithering matrix.

InKoo Kang et al [10] have proposed a color visual cryptography encryption techniques that develops substantial color shares through visual data pixel (VDP) synchronization and error diffusion halftoning. visual data pixel synchronization holds the positions of images pixels containing visual data of original images of the shares with representing error diffusion and color channels, which produces shares images effectively to human eyes. Thus the proposed method is compared with existing techniques, which demonstrates the superior performance of the proposed method. It proposes a color visual cryptography encryption techniques which guides to substantial shares and is free of the existing mentioned drawbacks. Error diffusion is a easy but significant algorithm for image halftone creation. Each pixel has filtered the quantization error and fed back to future inputs.

3. PROPOSED METHOD

In this paper, we propose the secure visual quality of secret images by advanced halftone scheme with diffusion techniques. At first, the visible images is translated into halftones shares by employing halftone error diffusion

scheme. Next, the secret image is converted into halftone shares containing efficient visual information. Thus the shared images are disseminated to particular participants and then they are extremely enforced to reveal the secret images. When the shares are generated, it is uses the halftone processing, which first the encryption the images with high quality secret images and then decryption the secret images with same image quality by using diffusion methodology.

The proposed methodology is consists of following process:

1. Share Creation Process
2. Data Hiding Process
3. Advanced Halftoning Process
   - 3.1 Advanced Halftoning Encryption Process
   - 3.2 Advanced Halftoning Decryption Process
   - 3.3 Error diffusion
4. Retrieving Process
5. Confirmation Process

The proposed scheme for any separate image element, each element is made up of 256 various shades of the corresponding channel. In this method, Visual cryptography can encrypt not only binary images such as white or black pixel, but also any color image pixel. For processing the original continuous tone in the digital image technique in order to transform binary image comprising of 1's and O's, such conversion from a continuous tone of the digital image in order to obtain the bitmap representation, it is known as the Halftoning.

In general, there are two kinds of Halftoning which is explained below:

1. **AM Halftoning (Amplitude Modulated)**: In the Amplitude Modulated scheme, spatial frequency is always kept fixed and then the halftone dots changes with respect to their size. This scheme clearly states that the size of the halftone dot turns to be larger as the tone becomes darker. The amplitude modulated scheme generally consequences larger in homogeneously halftoned images if the color tones of the separate channel of the image changes very slowly.
2. **FM Halftoning (Frequency Modulated)**: In the Frequency Modulated scheme, it is considered that dot size is determined, when the number of micro dots or (frequency) changes. The frequency modulated scheme, on the other side, it is termed as superior while handling the heavily textured original images .

Thus the Advanced Halftoning process includes the encryption and decryption process with error diffusion in order to minimum the noise in the images and to produce the high quality images for both encryption and decryption, in which high quality image is utilized for sharing the secret images in the visual cryptography. Thus hidden data mechanism is incorporated in the secret images for sharing between the specific user in the shares. Next, for the retrieving images we have proposed the image recovery algorithm, in which the specific participants would only retrieve the images for the obtaining the security. Finally, in the confirmation process, it verifies the whether the secret images is shared to the specific participants in the order to receive the secret image data.

An n × n binary confirmation digital image and n × n binary secret digital image are given as the input parameter to the share creation process and two share images such as share1 and share 2 are received. Share creation process is processed out by using bit-level using Eqn. (1) and Eqn. (2).

The below equations is obtained from the share creation algorithms, which is explained in the following next section. The obtained shares do not disclose any data regarding as the both secret as well as confirmation image. In the data hiding process, created shares are individually hidden inside two selected user n × n cover images and then stego-share images are obtained.

Then, the ensued shares are significant. These shares are transmitted to the different participants. It is represented in the block diagram representation of the proposed system in figure.2 . The proposed framework is consists of the five major process, which is described in the above section such are Share creation, data hiding, advanced halftoning with error diffusion, retrieving process and confirmation process.

Block Diagram Representation Of The Proposed System

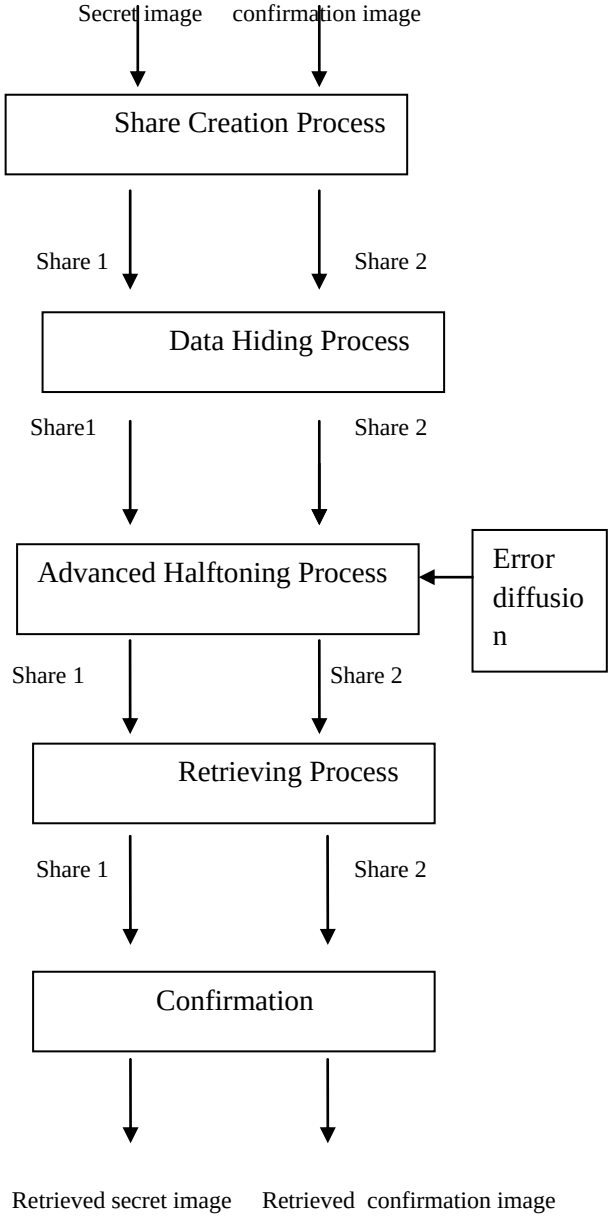


Fig 2:The Proposed Scheme

A. Share creation process

Share creation process is made up of 4 important steps, which is stated above in this section. At first, dealer starts the process of share creation by using the equations (1) and (2). The ensued shares are then given to next process. The secret image is represented as O and confirmation image is represented as C are input to this process. Then the two shares images are created by applying Eqn. (1) and (2)

$$S^{J}_{c_{xy}} = [((O_{xy} \times 2 + C_{xy} + 1) \bmod 2] \quad \text{-----} \quad (1)$$

$$S^{J}_{c_{xy}} = [((O_{xy} \times 2 + C_{xy} + 1) \bmod 2] \quad \text{------} \quad (2)$$

However, it is noticed that, received shares are informatory, which means that some data would be expose about the secret and confirmation image. Therefore in order to scramble the pixel data further, we are using the discrete wavelet transformation method and finally, it provides share S^{I} and $C^{'}_{xy} = [((S^{I}_{xy} \times 2 + S^{J}_{xy} + 3) \bmod 2]$ are obtained.

B. Data hiding process

To hide the data inside the secret images in the secret images of the visual cryptography . Two noise-like random shares are utilized to hide the data in the user-selected camouflage images by proposing steganography method. Bit-Plane Complexity Steganography (BPCS) method is utilized for this hiding the data process. In this proposed work, cover image is classified into bit-plane images and then blocks are identified depend on white and black border length. The bit plane block of secret images is substituted with random binary code. Bit-Plane Complexity Steganography consists of two processes, such as data embedding and data extraction. In this Bit-Plane Complexity Steganography initial it requires to embed, complex block or regions in each bit-plane of cover image are substituted with random binary share blocks i.e. The final stego share images are significant and realistic images of higher quality due to the error diffusion which is described in the below section. The block diagram representation of the data hiding process with embedding Bit-Plane Complexity Steganography, it is given in the fig.3. Hence, the secret image can be present either in the share1 or share2. When the complex regions are substituted, bit plane images are merged together in order to produce stego share images. Then the participants would receive these stego shares from the dealer. Interactive participants would perform reverse actions to retrieve the shares images of S^{I} and S^{J} when they receive stego share images. This procedure is known as Bit-Plane Complexity Steganography Extraction and the process are illustrated in fig and finally random binary shares are retrivered. The stego share image is present either in stego-share1 or stego-share2.

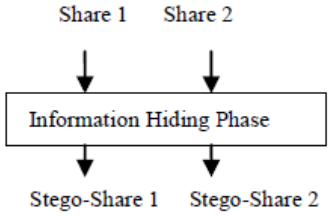


Fig 3:Data Hiding Process

C. Advanced Halftoning process with error diffusion

In the proposed method, it utilize the advanced halftoning process with error diffusion technique for the secret images of the Share 1 and share2. It uses the 5x5 non casual error filter, which disseminate error uniformly to all the neighboring pixels. In General, the quantization error of each pixel is used to filter and then it is given as the fed back loop to the future input samples in order to minimum the noise error. It is demonstrated w in the figure 4, which represents about the a binary error diffusion diagram.

Where f(m, n) demonstrates about (m, n) th pixel of the input secret or grayscale image, d(m,n) is the total amount of the of the input pixel value and the diffused past errors, and g(m,n) represents the output value of the quantized pixel. Error diffusion made up of two important elements. The first elements is the indicates about the thresholding regions where the output is demonstrated by (3)

$$g(m,n) = \begin{cases} 1, & d(m,n) \geq t(m,n) \\ 0 & otherwise) \end{cases} \quad \text{-------} \quad (3)$$

The threshold t(m,n) would be defined as the position-dependent. The second elements is termed as error filter h(k,l) whose input value is determined as the difference between the d(m,n) and g(m,n). Hence, calculate d(m,n) as eqn (4)

$$d(m,n) = f(m,n) - \sum_{k,l} h(k,l) e(m-k, n-l) \quad (4)$$

Here, the quantization error of one pass is gathered and applied on the next pass as a quantization error of the neighboring pixels. The error filter is usually demonstrated as FIR with the coefficient at (0,0)=0. The error filter magnitude response must be low pass, because this might leads to low frequency spectrum of the advanced halftoning corresponding so that the feedback of the error report is included to the input image in this process to maintain the sharp edges. Thus the proposed scheme with error diffusion minimizes the error difference in the images which is disseminated for the entire process in the visual cryptography.

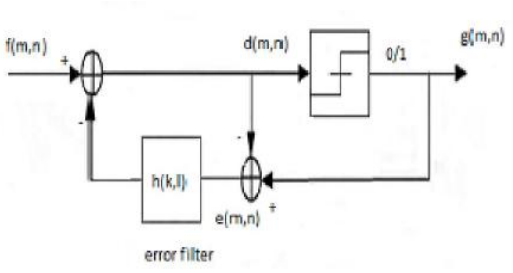


Fig 4: Error diffusion

1. **Adavnced halftoning process** Advanced halftone consider the input gray scale image or any color image and secret image.
2. **Adavnced encryption process**Creation the significant shares utilizing both input halftone image and halftone secret image by employing fundamental visual(2,2) scheme.
3. **Advanced decryption process**

Rebuild the secret image by lying halftone shares all together.

ADAVNCED HALFTONING PROCESS

In this process advanced halftone image I is received by implementing error diffusion halftone scheme on a grey scale

image G or any color image, The scheme would utilize secret image one pixel at a time and one row at a time. The current pixel value is equated to threshold value (127.5). If the current pixel value is more than above mentioned value then white pixel is produced as the resulting image. In case pixel is much less than the than above mentioned, a black pixel is produced. If it remains the same threshold value then it is used for the color image. The produced pixel is either full white or full black or even the color image. The halftone image received by above threshold process is assumed to participant 1, and its complementary image as I', received by reversing all black/while pixels of I to white/balck pixels , or even the color image and is to participant 2 or share2 .

ADAVNCED ENCRYPTION PROCESS

In this process the significant shares are produced using basic visual (2,2) methodology. The data of secret image is encrypted into halftone image I and inverse of halftone image I' .To encrypt a secret pixel is termed as p into a Q1xQ2 halftone cell matrix in which it contains two shares for the each pixel, if only two pixels is required then it is called as secret data pixels, in each halftone cell required to be changed. The two secret data pixels must be at the same locations in two secret images shares. Therefore, as far as their positions are independent of the secret data creation. It meets the security criteria to improve the visual cryptography. The easiest scheme to chose the positions of the secret data pixels in halftone images is random selection process.

ADAVNCED DECRYPTION PROCESS

In this process, the secret data that is embedded would be rebuild from the shares. Shares received in encryption process are stacked on each other. Once after all the shares are layered, the significant data vanishes and the secret is retrieved in the following section.

D. Retrieving Process

The image retrieving process the original image includes the random shares and recalling all the huffed shares together, further from these separate shuffled images shares, so that orginila data can be received with data hidden without compromising its quality. This image would be utilized for making the effective transmission; the bit level planning and difference expansion techniques applied here to obtain the higher data security.

E. Verification Process

After revealing process, final step is confirmation process of the proposed scheme. The proposed scheme confirmation process permits the determined participants to extract the data from the embedded confirmation image and rebuild the secret image from two random shares, S^I and S^J .

This process is consists out in bit-level using Eqn. (1) and (2)

$$O'_{xy} = [((S^I_{xy} \times 2 + S^J_{xy} + 3) \bmod 4)/2] \text{------} \quad (5)$$

$$C'_{xy} = [((S^I_{xy} \times 2 + S^J_{xy} + 3) \bmod 2] \text{----------} \quad (6)$$

The high quality of the rebuild secret image is same as that of the original secret image and has no noise ort distortion due to the error diffusion. However, the process assistants legitimate participants to confirm the rebuild secret image O' depend on the extracted confirmation image C' .

The extracted confirmation image can be checked by applying mean square error (MSE) and Structural Similarity Index value test. When the Structural Similarity Index value is equal to 1 or mean square error value is equal to 0, the extracted confirmation secret image is same as the hidden data secret image and there has been no malicious by the participant. Or else, the receiver can enquire the dealer to disseminate the complete share once again.

Thus the shared images are disseminated to particular participants and then they are extremely enforced to reveal the secret images. When the shares are generated, it is uses the halftone processing, which first the encryption the images with high quality secret images and then decryption the secret images with same image quality by using diffusion methodology.

4. PERFORMANCE ANALYSIS

The proposed scheme is executed in Matlab 2010 b. The implementation results obtained are described in this section. To prove the effectiveness of the proposed system, it should obtain the general criteria such as security, accuracy, error diffusion, peak signal-to-noise ratio (PSNR) and execution time, this performance analysis demonstrates a set of experimental results. The proposed scheme for the data hiding method is capable to embed about 5–80 kb into a 1024*1024 color image, when ensuring the PSNR of the secret image against the original image to be above 10dB. However, this proposed scheme is very easy, and the stimulation time is much lesser. Thus, its complete performance is efficient than existing methods, it is demonstrated in the experimental results. and 512 x 512 are represented as grayscale images in the proposed system: "Girl" and "Monkey" are the color images utilized for the cover images . In the experimental results tests, they " Black Peppers" represent as the secret image, while "GoldHill," represents as the confirmation image which are utilized to check the rebuild secret images. However, color images are used as cover images are "Girl" and "Monkey"

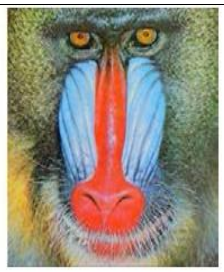
In this table 1, we demonstrate the our proposed effectiveness in the tables 2, we have utilized the set of

samples images in the Fig X. The set comprises of 512 x 512 binary set of images: " Black Peppers," "GoldHill,"

Table 1: Test Sample

 Secret images- Black Peppers. Png	 Confirmation image- Godhill.png

Cover image 1-Girl.png

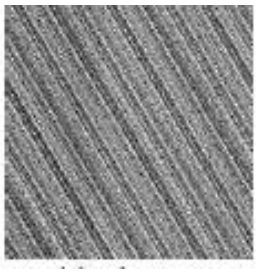


Cover image 2-Monkey.png

Fig 5 : Test samples images

The secret images " black peppers" and confirmation image "Goldhill" are given as a input images to share creation process and the obtained two shares images are represented in Fig. 6(a) & 6(b). Share1images is known as hidden data "girl" cover image on Bit-Plane Complexity Steganography embedding section and it results to stego share 1 was obtained as represented in Fig.6 (c).

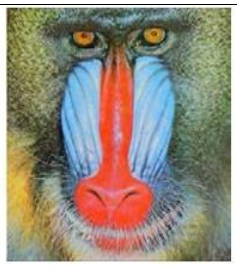
Table 2 : Experimental Results



a) Share 1

b) Share 2

c) Stego share1



d) Stego share2

e) retrieved confirmation image

MSE=0

SSIM index=1

f) retrieved secret image

PSNR= ∞

Fig 6: Experimental Results

In same manner, share2 images also contains the hidden data inside "monkey" image which results to stego share2 images as demonstrated in Fig.6 (d). These images are effective shares which is transmitted to participants. Afterwards, original shares are evoked from these shares on Bit-Plane Complexity Steganography based extraction process. During the retrieving and verification process, first, we retrieved the confirmation image and then obtained image would be same as the original confirmation image as given in Fig.6 (e). At last, secret image is retrieved without any loss of PSNR value which is resulted as '∞' as shown in Fig.6 (f).

The quality of the secret image retrieved was significant than error diffusion when the advanced halftoning is utilized, which was exactly described in the given below table 3. Here, the experimental results would prove that after advanced halftoning is applied, there is very minimum error loss has occurred in the proposed system in each channel in the visual cryptography. Thus the proposed method has the minimum error and provides efficient scheme in hiding data without compromising the quality.

Table 3: Error Table

Methods utilized	**Error produced**
Error diffusion	4.89×10^{10}
Advanced Halftoning	2.27×10^{10}

Accuracy

In our proposed method, the peak signal-to-noise ratio (PSNR) is applied to determine the quality of the rebuild secret image with original secret images. The peak signal-to-noise ratio evaluates the image quality by first estimating the mean squared error (MSE) and then classifying the maximum data range and its type by using mean squared error as demonstrated in the fig. Generally, peak signal-to-noise ratio value must come under the range from 30dB to 40dB , if the method obtains the value in between these ranges then it is termed as better visual quality. When peak signal-to-noise ratio value equals to ∞ that represents that scheme has obtained the maximum visual quality. To evaluate the proposed method accuracy, retrieved secret image is compared with original image, it is described in the table.

As per the descriptions of proposed methodology, the computational complexity depends on the two factors such as: the sum operation and discrete wavelet transformation in share creation process. Obviously, sum operation in terms complexity which is very much lesser and has small impact on the computational complexity of proposed system scheme. In our technique, the execution time for share secret images such as " girl" and "monkey" is represented in Table 4.

Table 4: Execution Time

Image Name	Share Creation /Generation	Share Retrieved/Reconstructed
Girl	0.095	0.011
Monkey	0.097	0.014

Thus the execution time carried to generate the share images is almost 0.095 seconds and shares rebuild or reconstruction is 0.011 seconds respectively. Hence, the experimental results of the proposed scheme has taken very lesser time for shares creation and retrieved which proves to be very fast and also maintains the image quality. The experimental results is

compared with the existing system in order to prove its effectiveness, it is demonstrated in the fig.7 and 8.

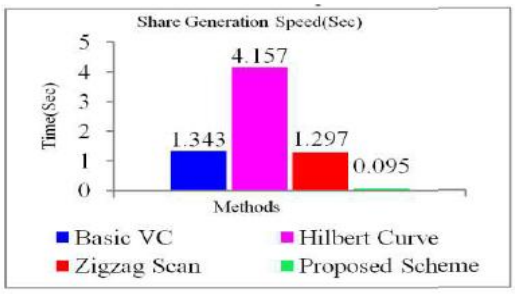


Fig 7 : Comparative results of Share Generation

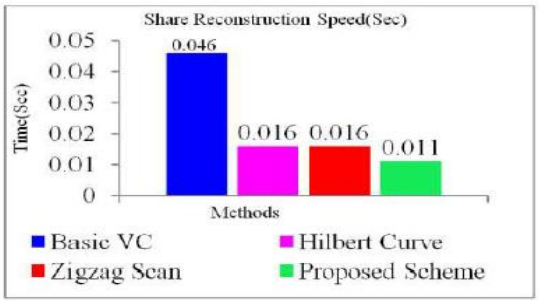


Fig 8 : Comparative results of Share Reconstruction

5. CONCLUSION

In this paper, we propose advanced halftone scheme with error diffusion technique in order to make the secure sharing of the secret images to the participants. It used to share the hidden data in the secret image for that shares are generated with the help of advanced halftone processing, which first the encryption the images with high quality secret images and then decryption the secret images with same image quality by using diffusion methodology. Furthermore, it also retrieve the secret images and makes the verification using the confirmation images with quality images. From the experimental results, it proves that the error diffusion in the advanced halftoning process has minimized the image distortion, it provides the high security in terms of producing peak signal-to-noise ratio value has ∞ that represents that scheme has obtained the maximum visual quality. Hence, the proposed scheme has taken very lesser time for shares creation and retrieved which proves to be very fast and also maintains the image quality. In future work, we will apply medical images in the proposed scheme for the health care applications.

6. REFERENCES

[1] M. Naor and A.Shamir. (1995). Visual Cryptography ",Advances in cryptography EUROCRYFT94, LNCS, vol-950, pp.1-12, 1995.

[2] J. Fridrich, M. Goljan, and D. Rui. (2002). Lossless Data Embedding - New Paradigm in Digital Watermarking. In Special Issue on Emerging Applications of Multimedia Data Hiding: February; Vol. 2; pp. 185-196.

[3] Mahmoud E. Hodeish,V. T. Humbe. (2014). "State-of-the-Art Visual Cryptography Schemes," International Journal of Electronics Communication and Computer Engineering, vol. 5, pp. 412-420.

[4] Srinivasan nagara, Raju and Koteswara rao. (2015). Image encryption using ECC and Matrix. In proceedings of Intelligent computing, Communication 7 Convergence 2015;48:276-281

[5] G.R Zhi Zhou Arce., G. Di Crescenzo. (2006). "Halftone Visual Cryptography," IEEE Transactions on Image Processing. , Vol. 15, pp. 2441-2453.

[6] R. Lukac, K.N. Plataniotis. (2005). Bit-level based secret sharing for image encryption. The Journal of Pattern Recognition Society.

[7] R. Vijayaraghavan, S. Sathya, N. R. Raajan. (2014). Security for an Image using Bit-slice Rotation Method–image Encryption. Indian Journal of Science and Technology:April 2014;Vol 7(4S); p 1–7.

[8] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, Wei Su. (2006). Reversible Data Hiding. IEEE transactions on circuits and systems for video technology: March; vol. 16, no. 3.

[9] Asha S.N, Dr. Shreedhara. (2012). Performance Evaluation Of Extended Visual Cryptography Schemes With Embedded Extended Visual Cryptographic Scheme. International Journal of Scientific & Engineering Research: April; Volume 3, Issue 4.

[10] InKoo Kang, Gonzalo R. Arce, Heung-Kyu Lee. (2009).Color extended visual cryptography using error diffusion. IEEE.

7. AUTHOR PROFILE

I.Diana Judith received M.E degree in Computer Science and Engineering from the Department of Computer Science and Engineering in Periyar Maniammai University, Thanjavur, Tamilnadu, India. She is a Research Scholar in the Department of Computer Science and Engineering, Center for Research and Development, PRIST University, Vallam, Thanjavur, Tamilnadu, India. She is working as Assistant Professor in the Department of Computer Science, Stella Maris College, Chennai. Her current research interest includes Visual Cryptography, image encryption and decryption.

Dr.G.J.Joyce Mary completed her Ph.D in the area of Parallel Computing in 2012. Now she is working as a Research supervisor and Associate Professor in the Department of Computer Science and Engineering, PRIST University, Thanjavur, Tamilnadu, India. Her area of interest includes Parallel Computing, Digital Image Processing and Webservice.