Efficient Visual Cryptographic Algorithm Using AES And Modified (K, N) Share Generation Technique

Sapna B K , K L Sudha

Abstract: Visual cryptography takes an approach to ensure proper protection of transmitted images by allowing the creation of a finite number of share images from a secret image using some mathematical model. The main challenging task in any visual cryptography is to create N shares that are dissimilar from the actual secret image. No information regarding the secret image must be revealed in these shares. In this paper, we propose a new visual cryptographic technique using AES and a modified (k, N) share generation algorithm. The AES is used to encrypt the image to provide high security to the input secret image. Modified (k, N) share generation technique is applied to this encrypted image to generate shares specified by the k and N values. The generated shares by the proposed technique have a granular appearance hiding the information from the observer but with proper decryption procedure and proper key, this algorithm is able to recreate the original secret image whose PSNR is high. The results show that the proposed algorithm is better in various aspects compared to the existing techniques.

Index Terms: Visual Cryptography, AES, Modified (k, N) share generation, Encryption and Decryption etc.,

1. INTRODUCTION

Security and authenticity is a big issue in today's digital media. Normally due to the architecture and working of the internet, it is possible for anyone to misuse the data intentionally or incidentally. These may create very big issues for the individual or organizations if the data is confidential. As an example, in military applications, if the classified information becomes accessible to their enemy countries it may cause exceptionally grave damage to the national interest. Normally in such cases, mathematical algorithms are used to change the format of the data into other formats in such a way that if the observer gets hold of the data it will not be intelligible. These types of security techniques are known as cryptography [1]. Research has shown that AES encryption algorithm [2] is the most secure algorithm. AES is a symmetric key algorithm having a block size of 128 bits. The whole algorithm operates on a 4X4 matrix and consists of several transformation functions that encrypt the secret image. This technique is applied to the color image separately in each color plane in RGB format [3]. The main disadvantage of the Chaos Encryption Algorithm technique [4] is that the entire image is encrypted and the hacker has to work on only one image to decrypt it. This disadvantage is overcome by Visual Cryptography wherein the entire image is dismantled into N shares [5] so that the hacker has to work on all the N shares to decrypt the original image. As these N shares are distributed to various participants it is difficult to crack. Authenticity is used to protect honest participants. It allows the user to determine the correctness of the source. To incorporate authenticity along with VC scheme an authentication id is embedded into the shares which can be retrieved at a later stage to determine the origin of the secret color image [6].

Contributions: The main contribution of this paper is the direct use of color image and the utilization of (k, N) sharing scheme. The scheme is applied to the AES encrypted image to develop the shares.

2 LITERATURE SURVEYS

Dana Yang et al. [7] proposed Visual Cryptography and OCR technique based on an enhanced password protection algorithm. The algorithm uses a text as user-id and subsequently two images using some random function. These random functions are generated by some secret information. At the receiver side, the seed images are recovered by secret information and authenticated by extracting user-ids. This technique offers lower computation, prevents cyber-attack aimed at hash cracking and supports authentication not to expose personal information such as ID to attackers. Shankar and Eswaran [8] presented Visual Cryptography using Elliptic Curve Cryptography techniques. In this case they consider color image which is then divided into RGB color components and then the algorithm is applied to each plane separately. Each plane generates an equal number of shares which is then merged to generate colored shares. To increase security, a user key is used in Elliptic Curve Cryptography. Chien-Chang Chen and Wei-Jie Wu [9] presented a secret image sharing scheme using Boolean based arithmetic operators. In this case, an image is generated using random variables whose size is equal to the input image and XORed with the input image through sharing techniques.This technique produces noise-like image shares. Yawei Ren et al. [10] presented Visual Cryptography using Latin Square technique which prevents anyone from guessing that some information is hiding behind those shares. They consider probabilistic methods to insert the data bits into the main image which increases the efficiency of the algorithm. But due to the uses of probabilistic methods, the processing time is more than most of the other techniques. Xingxing Jia et al. [11] proposed a new scheme which is the merged version of two normal (k, n) sharing scheme which is known as collaborative visual cryptography (CVC) schemes. The construction of the idea matrices in CVC theme between 2 VC schemes is developed into a whole number applied mathematics downside that minimizes the growth beneath the corresponding security and

- *Sapna B K and K L Sudha are currently working in Department of Electronics and Communication Engineering ,Dayananda Sagar College of Engineering, Bengaluru, India,*
- *E-mail:*
  sapnanoorithaya@gmail.com (Sapna B K)
  klsudha1@rediffmail.com (K L Sudha)

distinction constraints. Additionally, the collaboration among additional VC schemes is built. Finally, the experimental results illustrate the development procedure of the CVC theme and demonstrate the effectiveness of CVC theme.

3. PROPOSED ALGORITHM

The proposed algorithm for visual cryptography is shown in Fig.1. Here first the input color image is encrypted using AES algorithm followed by a private key. This encrypted image is used to generate 'N' shares using the Share Generation scheme with a specified value of 'k' and 'N' from the user. Those shares are sent through a communication channel. At the receiver side, all N-shares are used to generate a recovered image which is the encrypted version of the input image which is then decrypted with the same private key. This decryption generates the recovered image.

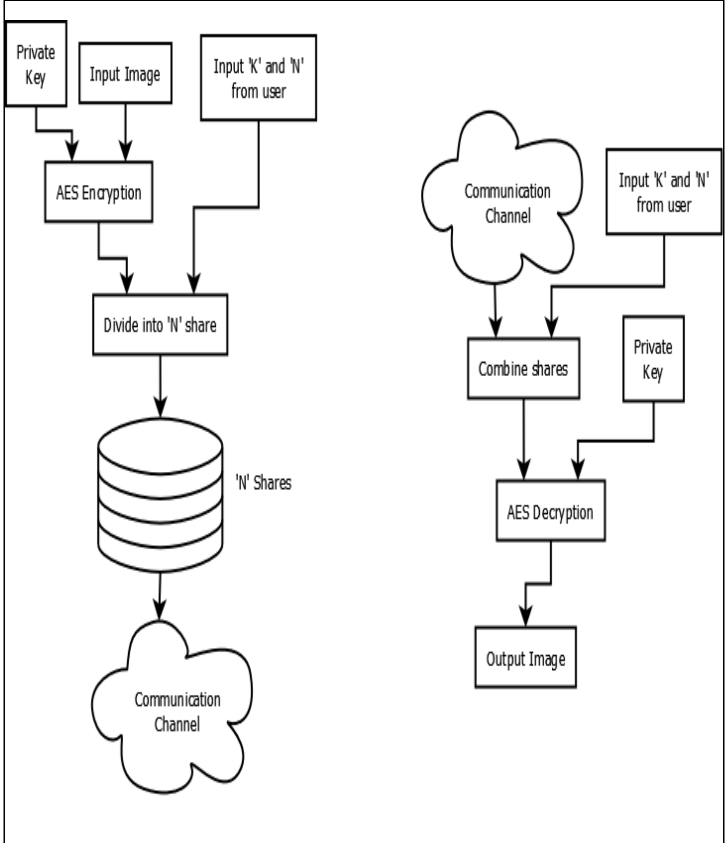

Fig. 1. Proposed Visual Cryptographic Algorithm for Encryption and Decryption

3.1. AES Algorithm

Advanced Encryption Standard (AES) is the most popular and widely used encryption technique due to its speed optimization over most of the other existing encryption techniques such as DES. Moreover, the AES technique shows more immunity than other existing techniques. To implement efficient AES for an image, fast image encryption is used.

3.1.1. Encryption Process:

The block diagram of fast AES encryption for the image is shown in Fig.2 which consists of the XOR gate and normal AES algorithm.

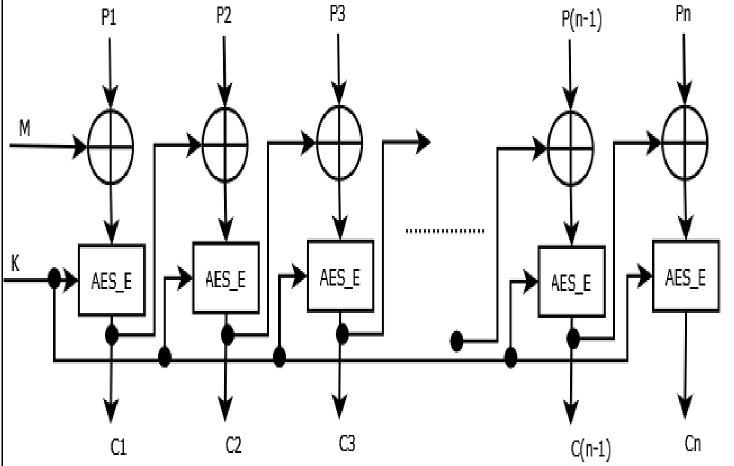

Fig. 2. Fast AES Encryption for Image

The algorithm for fast AES encryption for an image is given as

Algorithm-1: Fast AES Encryption of Image

1. 'M' is generated by Tent map [4] which is public and depends upon the key used. The initial value of the Tent map is generated by pseudo-random number generator which is denoted by x_i in Eq. (1)

   $$f(x) = \begin{cases} 2x, \text{when } 0 < x < 0.5; \\ 2(1-x), \text{when } 0.5 < x < 1; \end{cases}$$

   (1)

   Then convert x_i into an integer using Eq. (2)

   $$x = floor(10^4 x_i)\ mod256$$

   (2)

   Where floor(x) returns the largest integer which is smaller than x.

2. The plane image P is encrypted block-wise using Eq. (3)

   $$C_1 = AES\_E(K, M\ XOR\ P_1)$$

   (3)

   Where AES_E represents the AES encryption algorithm with the inputs of the secret key C_1 is the first block of ciphered image C.

3. To encrypt ith block, Eq. (4) is used as

   $$C_i = AES\_E(K, C_{i-1}\ XOR\ P_i)$$

   (4)

   Where, i= 2,.....,n

3.1.2. Decryption Process:

In this case, the encrypted image is used to recover the original image. The block diagram of the decryption process is shown in Fig.3.

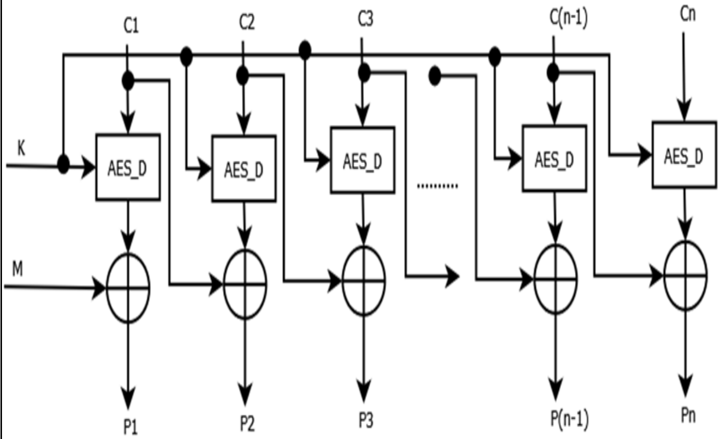

***Fig. 3**. Fast AES Decryption for Image*

The algorithm for fast AES decryption for image [2] is given as

Algorithm-2: Fast AES Decryption of Image

1. The encrypted image C is used with the key for the decryption process.
2. The first block of the cipher image C_1 is decrypted using Eq. (5) as
   $P_1 = AES\_D(K, C_1)\ XOR\ M$
   (5)
   Where AES_D represents the AES decryption algorithm
3. The remaining blocks are deciphered using Eq. (6) as
   $P_i = AES_d(K, C_i) XOR\ C_{i-1}$
   (6)
   Where, i= 2,3,...,n
4. Combine {P_i=1,2, ... ,n}into an image of size MxN, which is the recovered image.

3.2. Share Creation using Modified (k, N) Secret Sharing Scheme

Share creation is done by a modified (k,N) secret sharing scheme and the number of generated shares is controlled by the user-defined input number. The pixel values of the secret color image are in RGB format, therefore each pixel must be converted into 24-bit binary number where each plane consists of 8-bit binary numbers. In the proposed Modified (k, N) secret sharing scheme, the input image is divided into 'N' number of shares with the help of random matrix in such a way that at least k-number of shares is required to extract the hidden information in proper way.

3.2.1. Encryption Process:

The encryption algorithm is used to divide a digital color image into N number of shares where minimum k numbers of shares are sufficient to reconstruct the image. If k numbers of shares are taken then the remaining shares are (N−k). In an image, if certain position of a pixel is 1, then in (N−k)+1 number of shares the pixel value in that position will be 1. In the remaining shares the pixel value will be 0. A random number generator is used to identify those (N−k)+1 number of shares. An image is taken as input. The number of shares the image would be divided (N) and number of shares to reconstruct the image (k) is also taken as input from user. The encryption, i.e. division of the image into N number of shares such that k numbers of shares are sufficient to reconstruct the image; is done by the following algorithm.

Algorithm-3: Share Generations

```
I.    Calculate the height (h) and width (w) of the input image.
II.   Consider the number of shares (N) and minimum number of shares (k) as user-defined input in such a way that 'k' always must be lesser or equal to 'N'.
III.  Create a three-dimensional array 'img_share' to store the pixel of N-shares.
IV.   (k, N) secret sharing algorithm is then
      $RECONS = (n - k) + 1$
      $for(i = 0; i < \{(w * h) - 1\}; i++)$
      {
        $PIX = convert\ pixel\ values\ into\ 24\ bit\ string$
        $for(j = 0; j < 24; j++)$
        {
          $if\{PIX(i) = 1\}$
          {
            $temp$
            $= array\ of\ random\ number\ generated\ by\ MATLAB$
            $for(l = 0; l < (RECONS - 1); l++)$
            {
              $rand\_int = Generate\ a\ random\ number$
              $if(rand\_int \neq temp[RECONS])$
              $temp[i] = rand\_int$
            }
          }
          $for(k = 0; k < RECONS; k++)$
          {
            $img\_share[temp[k]][i][j] = 1$
          }
        }
      }
```

3.2.2. Decryption Process:

In this process, k numbers of shares are taken as input from user. Each share must be of equal height and width as the source image. Then bitwise OR operation is performed among pixels of the k shares, and final pixel values are stored in an array. The decryption algorithm is as follows.

Algorithm-4 : Reconstruction

1. Input number of shares to be taken (k), height (h) and width (w) of each share.
2. Create a two dimensional array share[k][w*h] to store the pixel values of each share. Create a one dimensional array final[w*h] to store the final pixel values of the image to be produced by performing OR operation.
3. for i=0 to k-1
   {
   input the name of the i^{th} image share to be taken.
   for j=0 to (w*h-1)

```
      {
      Scan each pixel value of the i^th image share and
      store the value in share[i][j].
      }
      }
4.    for i=0 to (k-1)
      {
      for j=0 to (w*h - 1)
      {
      final[j]=final[j] | share[i][j];
      }
      }
5.    Generate image from final[w*h].
```

4 SIMULATION RESULTS

To implement the proposed algorithm, MATLAB 2013a is used and the program is written using standard MATLAB programming method. In this case, image processing toolbox present in the MATLAB tool is used.

4.1. Graphical User Interfaces

To make a simple user interface to the designed algorithm, Graphical User Interfaces (GUI) [12, 13] is built for the design at the top level. The top-level GUI is used to choose the encryption or decryption option. Then the user needs to specify the input image locations in the GUI along with k and N value and desired key. At decryption stage, the user has to give the location of share images and k and N value with desired key. The snapshots of those GUI are given below

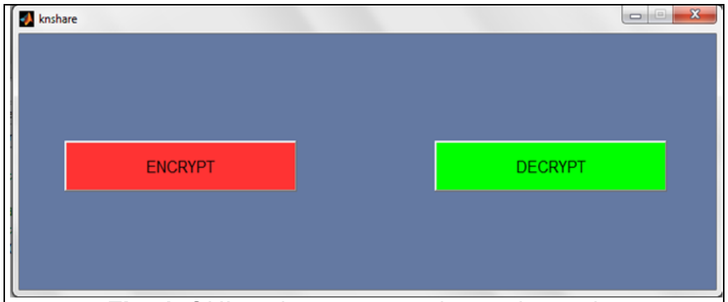

Fig. 4. *GUI to choose encryption or decryption*

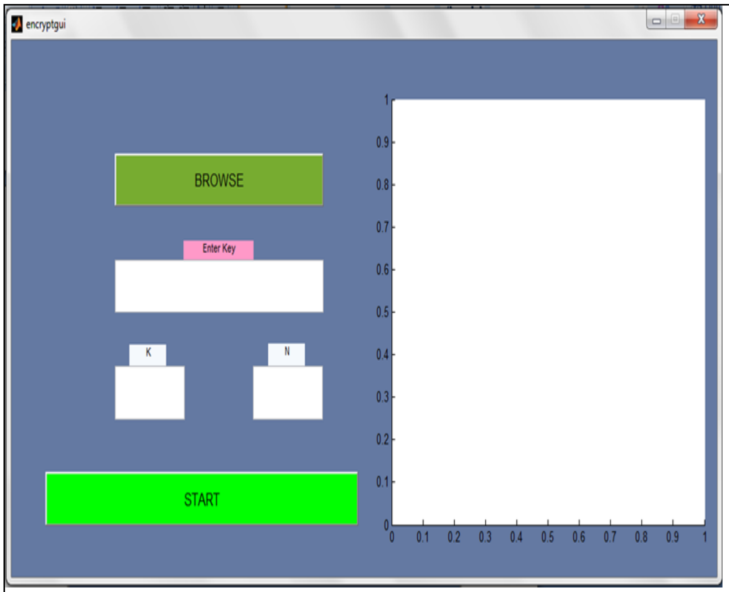

Fig. 5. *GUI for encryption*

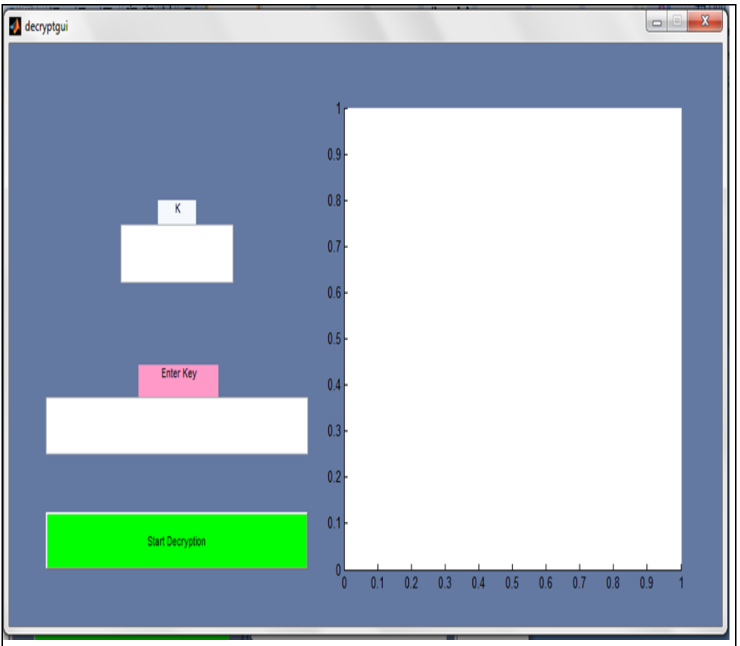

Fig. 6. *GUI for decryption*

4.2. AES Encryption and Decryption

Fast AES encryption for image [2] is used for encryption and decryption process with a secret key. This encryption is done in color image through encrypting it's separate color components. The encrypted and decrypted image is shown in Fig.7 respectively.

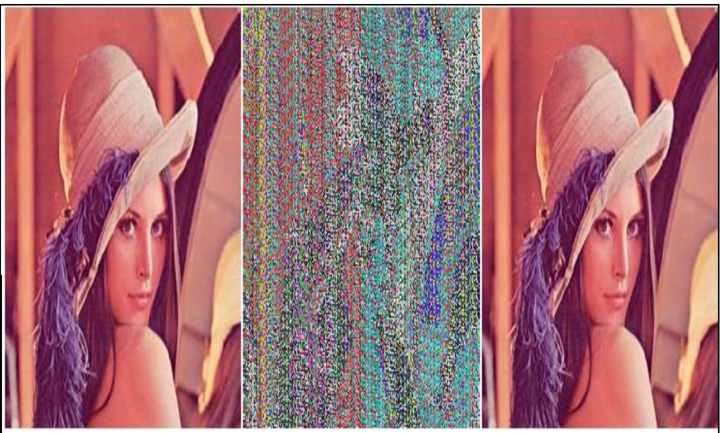

Fig. 7. *AES encryption and decryption of image ((a) Input Image, (b) Encryption and (c) Decryption)*

4.3. Share generation

Modified (k, N) share generation scheme is used to generate shares by specifying k and N values. This share generation produces noise-like shares. The shares of k=4 and N=4 is shown in Fig.8 respectively.

***Fig. 8**. Four shares of the Encrypted image after share generation*

4.4. Reconstruction of Image

The correct shares with the corresponding private key are used to reconstruct the image. If the correct numbers of shares are not used then the reconstruction will not yield the original image with high PSNR which is shown in Fig. 9 by considering different numbers of shares.

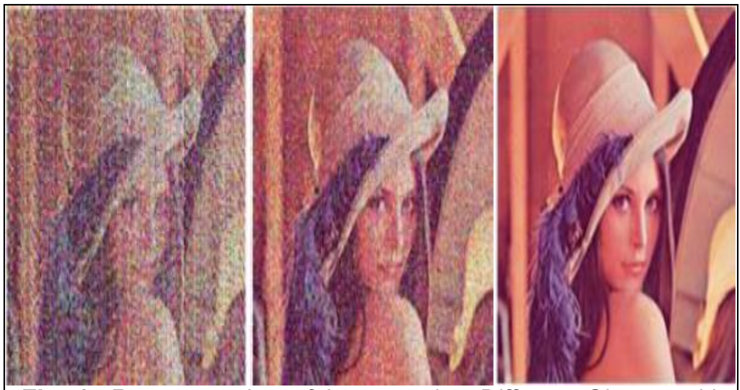

***Fig. 9**. Reconstruction of Image using Different Shares with correct key ((a) 2-Shares,(b) 3-Shares and (c) 4-Shares)*

The important factor in the reconstruction process is the use of the correct key. If the key is not correct then the reconstruction process generates a blurred image which is shown in Fig. 10.

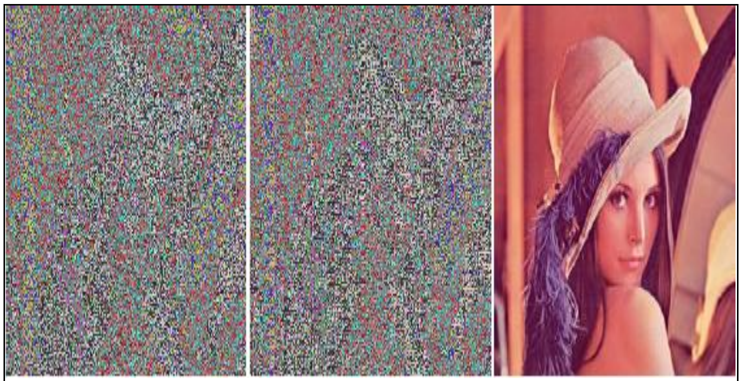

***Fig. 10.** Reconstruction of Image using Shares with incorrect key((a) Incorrect Key, (b) One part of key is Correct and (c) Correct Key)*

5 PERFORMANCE ANALYSIS

The performance of the proposed algorithm is analyzed in this section.

5.1. Performance Parameters

The Peak Signal to Noise Ratio (PSNR) [14] is used to analyze the performance of the proposed algorithm. The equation of PSNR is given in Eq. (13)

$$\mathrm{PSNR} = 10\log_{10}\frac{(\mathrm{MAX_I})^2}{\frac{1}{\mathrm{MN}}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[\mathrm{I(i,j)}-\mathrm{K(i,j)}]^2}$$

(13)

Where $\mathrm{MAX_I}$ is the maximum possible input value.
I(i,j) and K(i,j) are image matrix.
M and N are the image dimensions.

5.2. PSNR Calculations

To check the performance, it is necessary to calculate PSNR values using standard images. For this purpose, k=4 and N=4 are considered. The PSNR values of Encrypted, Decrypted and Shares are calculated in Table.1 it can be seen that the encrypted images and shares having very low PSNR values which shows that the difference between input image and share images is very large. Moreover the PSNR of the decrypted image proves that the difference between input and decrypted image is very less.

TABLE 1

PSNR CALCULATIONS

Image	Key	PSNR (dB)					
		Encrypted Image	Decrypted Image	Share 1	Share 2	Share 3	Share 4
Lena	Visual Cryptography	8.6079	72.2302	6.3023	6.3074	6.3053	6.3051
Mandrill		9.0925	72.3202	6.6567	6.6540	6.6591	6.6603
Peppers		8.1554	71.3020	7.0224	7.0347	7.0429	7.0442
Jelly Bins		8.5648	72.3202	4.5625	4.5587	4.5631	4.5625
Airplane		7.79755	72.3202	3.8449	3.8425	3.8429	3.8540
Girl		7.4469	72.3202	11.2361	11.2589	11.2205	11.2392

To generate shares, a random matrix of the same dimension of an input image is considered which are generated by the random operator available in MATLAB tool. At different times of simulation, different types of random matrix are generated which makes different types of shares with different PSNR values. The PSNR values of different k are plotted in Fig. 11 which shows the variations.

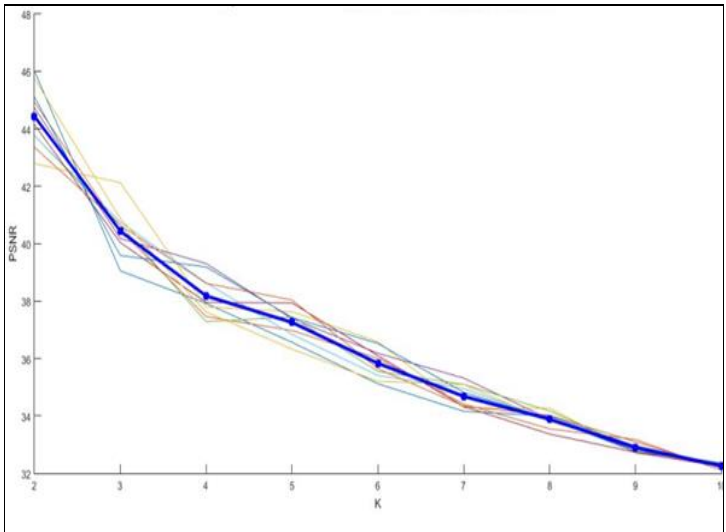

Fig. 11*. PSNR versus K for single image showing variations in PSNR for 10 iterations*

6 COMPARISON WITH EXISTING TECHNIQUES

In this section, the proposed algorithm is compared with different existing techniques in various aspects to prove the superiority of the proposed algorithm.

6.1. Performance Parameters

The PSNR values of the shares of the proposed algorithm are compared with the technique presented by Shankar and Eswaran [15]. For this comparison purpose, the proposed algorithm is simulated using k=2 and N=2. The PSNR values of both shares are more than the corresponding shares of different standard images in the proposed technique. This shows that the randomization of data inside each share more than exists.

TABLE 2

PSNR VALUE COMPARISON OF SHARES OF DIFFERENT IMAGES

Images	PSNR (dB)			
	Shankar and Eswaran [15]		Proposed	
	Share 1	Share2	Share 1	Share 2
Lena	8.77	8.77	7.4063	7.4102
Mandrill	8.80	8.81	7.8492	7.8560

6.2. PSNR Values of Reconstructed Images

The PSNR of the reconstructed image after decryption shows the suitability of the algorithm. The proposed algorithm is compared with different existing techniques using different standard images which are given in Table 3. it can be seen that the PSNR values of the proposed algorithm are much higher than existing in all standard images which prove that the proposed algorithm is more efficient in generating good quality recovered images

TABLE 3

PSNR VALUE COMPARISON OF RECONSTRUCTED IMAGES

Image	Shankar and Eswaran [8]	Javvaji Ratnam et al. [6]	Narendra et al. [16]	Proposed
Lena	58.0025	64.328	49.8556	72.2302
Pepper	56.684	----	----	71.3020
Mandrill	58.1438	----	49.8628	72.3202
Bird	----	----	49.3150	72.2232

6.3. Overall Comparisons

In this section, the proposed algorithm is compared with various aspects of existing algorithms such as recovery type, pixel extension, color depth, recovery strategy, sharing type and extra security. The recovery type indicates whether the recovered secret images are visually recognizable or losslessly recovered. Pixel expansion indicates if the pixels in secret images are expanded in shared images. Color depth shows the color number that each pixel represents. The recovery strategy compares the recovered secret images acquired from different mathematical computations. A Lossless secret image can only be acquired from mathematical calculations such as XOR.

TABLE 4

OVERALL COMPARISONS

	Recovery Type	Pixel Expansion	Color Depth	Recovery Strategy	Sharing Type	Extra Security
Narendra et al. [16]	Lossy	No	Gray	Stacking	----	No
Chen and Wu [17]	Lossless	No	Gray	XOR	Rectangle	----
Lin et al. [18]	Lossy	No	Binary	Stacking	Circle	----
Proposed	Lossless	No	Binary	OR	Circle	Yes

7 CONCLUSION

The AES with a modified (k, N) sharing algorithm is proposed in this paper to perform optimum visual cryptography of any colored image using a secret key. Here the input image is first encrypted using AES algorithm to provide extra security which is then used to generate a finite number of shares using a modified (k, N) sharing algorithm. This whole process ensures that the generated shares look like noise, but with the use of proper decryption technique along with correct shares and key to produce the resultant image which is very much nearer to the input image. This is proved in the paper and also the comparison result shows that the proposed technique is better than the existing in producing good quality shares and decrypted images.

REFERENCES

[1] https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

[2] Yong Zhang, Xueqian Li and Wengang Hou, “A Fast Image Encryption Scheme Based on AES”, 2nd IEEE International Conference on Image, Vision and Computing, pp. 624-628, 2017, China.

[3] https://en.wikipedia.org/wiki/RGB_color_model

[4] Ali M. Meligy, Hossam Diab and Marwa S. El-Danaf, “Chaos Encryption Algorithm using Key Generation from Biometric Images”, International Journal of Computer Applications, Vol. 149, No. 11, pp. 14-20, September 2016.

[5] Daoshun Wang, Lei Zhang, Ning Maand Xiaobo Li, “Two secret sharing schemes based on Boolean operations”, Pattern Recognition, Elsevier, Vol. 40, pp. 2776-2785, 2007.

[6] Rafel C. Gonzalez and Richard E. Woods, “Digital Image Processing”, Pearson Education, 3rd Edition, 2008

[7] Dana Yang, Inshil Doh and Kijoon Chae, “Enhanced Password Processing Scheme

[8] Based on Visual Cryptography and OCR”,IEEE International Conference on Information and Networking, pp. 254-258, Vietnam, 2017.

[9] K. Shankar and P. Eswaran, “RGB Based Multiple Share Creation in Visual Cryptography with Aid of Elliptic Curve Cryptography”, IEEE China Communications, Vol. 14, Issue. 2, pp. 118-130, 2017.

[10] Chien-Chang Chen and Wei-Jie Wu, “A secure Boolean-based multi-secret image sharing scheme”, Journal of Systems and Software, Elsevier, Vol. 92, pp. 107-114, 2014.

[11] Xingxing Jia, Daoshun Wang, Daxin Nieand Chaoyang Zhang, “Collaborative Visual Cryptography Schemes”, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 28, Issue. 5, pp. 1056-1070, 2018.

[12] https://in.mathworks.com/discovery/matlab-gui.html.

[13] http://www.datatool.com/downloads/MatlabStyle2%20book.pdf .

[14] https://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio.

[15] Shankar K, Eswaran P “Sharing a Secret Image with Encapsulated Shares in Visual Cryptography” 4th International Conference on Eco-friendly Computing and Communication Systems, Procedia Computer Science 70 (2015) 462.

[16] Modigari Narendra, Dhanya Ben, C.P. Jetlin , Dr. L. Jani Anbarasi “An Efficient Retrieval of Watermarked Multiple Color Images using Secret Sharing”, 4th IEEE International Conference on Signal Processing, Communications and Networking, March 16 – 18, 2017, Chennai, India.

[17] Chen, T.H., Wu, C.S., Efficient multi-secret image sharing based on Boolean operations. Signal Processing 91, 90–97, 2011.

[18] Lin, S.J., Chen, S.K., Lin, J.C., Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion, Journal of Visual Communication and Image Representation 21, 900–916, 2010.