ISSN: 0976-9102 (ONLINE)
DOI: 10.21917/ijivp.2019.0288

ADVANCED COLOR COVERT IMAGE SHARING USING ARNOLD CAT MAP AND VISUAL CRYPTOGRAPHY

B.K. Sapna and K.L. Sudha
Department of Electronics and Communication Engineering, Dayananda Sagar College of Engineering, India

Abstract

The demand for effective information security schemes is increasing day by day with the continual growth of the internet. Visual cryptography (VC) is a very important secret sharing scheme. The essential step behind this secret sharing scheme is to convert the color covert image into multiple indecipherable image shares so it cannot reveal the data within the color covert image unless combined along by some mathematical calculation. This paper proposes an advanced color covert image-sharing scheme using Arnold cat map (ACM) and VC. The random matrix-encoding scheme encodes the color covert image into an image matrix. ACM algorithm disrupts the high correlation among the pixels of the image matrix to generate an encrypted image. The generation of shares from this encrypted image is by VC that uses pixel reversal and random matrix generator. The shares one by one does not provide any information concerning the color covert image however put together they offer back the encrypted image. The projected paradigm offers 3 levels of security and through decipherment gives back the covert image without loss of information. Related examples and experimental results reveal the effectiveness of this scheme.

Keywords:

Visual Cryptography, Color Covert Image, ACM, Random Matrix

1. INTRODUCTION

Nowadays much multimedia information is transmitted in a large amount over the internet. Secure and efficient communication of confidential and sensitive information is the initial concern in communication and network storage system. Color image processing gains significant importance as color images are used everywhere in today’s world. It is also important to avoid tampering of the data. The color of the image must also be preserved together with the privacy of the information [1]. Therefore, security becomes more important to prevent the information from being hacked and misused. Thus motivated, the secret-sharing method will be the better technique that not only increases the security but also has an extremely high opportunity of recovering the secret information completely. Visual cryptography is a sensible choice for conserving the privacy of a color covert image [2]. It is an evolving cryptography technology that uses human vision for decryption. The secret holder separates the image into n parts termed as shares and allocates them to n participants. The beauty of this technique is individually each share does not divulge any statistics about the covert image [3]. It also ensures that hackers cannot recognize any hints about the covert image from the shares. Reconstructing the original covert image is also a challenge since it requires all the shares stacked together [4]. Most of the studies, however, concentrate on binary images [5]. Some papers deal with grayscale images [6]. The major drawbacks in these cases are size expansion, contrast, and security.

To address these problems this paper focuses on improving the visual quality of a color image without size expansion. This reduces the burden on processing, storage, and transmission of the shares. The second problem is contrast; it is overcome by the algorithm which optimizes the visual quality of the image. The third problem being security for the shares, it is increased by utilizing VC with encoding and ACM technique. Therefore, an extremely secure encoding technique for the color image without pixel expansion and improved contrast is proposed.

Random matrix encoding of the color covert image into an encrypted image is the initial step to achieve the first level of security. Then ACM method varies the pixel positions and rotates the image k times so that the original image is not visible to the naked eye providing the second level of security. Then, the VC can use its strategy in producing binary shares. This process is flexible in that it can be implemented to images of any size without any pixel expansion providing three levels of security. The decoding stage is of interest to maintain the visual quality of the decrypted image. All the binary shares must be stacked together to form an input to the ACM decryption algorithm. Random matrix decoder restores the original color covert image by keeping its quality intact.

2. RELATED WORKS

Rao et al. [7] discusses a method, which uses AES and VC to increase the security of the image. The VC technique uses each pixel represented by two subpixels that double the size of the share created. A hardware system for deploying the algorithm is specified dealing with area, speed and power-efficient design on an FPGA platform

Shankar et al. [8] deals with VC and Elliptic Curve Cryptography to increase the secrecy and security of the original image. The Color image is first split in RGB color space and multiple shares are created. The test results indicate the PSNR is 58.0025 thereby decreasing the contrast of the image. The correlation coefficients and histogram is analyzed to preserve the discretion of the image.

Karolin et al. [9] presents a technique where the color image is broken down to construct RGB color models and uses the blowfish algorithm for creating the shares. A 64-bit block cipher is used in Blowfish method and for securing the share, the key is in the range 448. This method improves the quality of an image.

Shivani et al. [10] uses a color code table to decompose the color image to CMY color space. Floyd Steinberg diffusion technique is used to generate color half-toned images that expand every pixel leading to pixel expansion. A gray-scale image is transformed into binary using halftone technique. This paper exploits the color disintegration and half-tone to bring out cryptograms for color image

Narendra et al. [11] proposes a visual secret sharing scheme where two shares are created without pixel expansion. Verification of the originality of the image is done using watermarking. By the retrieval of the watermark, the authenticity of the original image is possible. The reconstructed image has a PSNR of 50.06dB.

Dahat et al. [12] presents a CMY color model with ((n-1), n) secret sharing using VC. The VC technique used is basic Shamir secret sharing. The work proves that CMY color space is better than the RGB color space.

Shiny et al. [13] extend VC by introducing a tag pattern in the shares generated by using probabilistic VC. This provides interested parties with augmented information to identify particular shares among numerous shares. The-inserted tags ensure the security of the shares.

Jabi et al. [14] discusses tiny encryption encoding for creating the shares. Shares are then hidden in a cover image using steganography. Subtractive model (C,M,Y) is utilized for a color image.

3. PRELIMINARIES

3.1 RANDOM MATRIX ENCODER

The conventional methods normally convert the color image into a gray image before encryption. The disadvantages are

1. The RGB components of the color image must be saved after conversion as they are required for reconstruction of the original image
2. Saving and processing these components require extra memory space
3. Transmitting the three components takes more time i.e Extra time for data transmission
4. Security must be provided for all the components

A random matrix encoder technique overcomes these disadvantages.

In probability theory and mathematical physics, a random matrix is a matrix in which some or all elements are random variables. An image is considered as a matrix $J[n]$ of M rows and N columns. A color image can be considered as three matrices of RGB components. The color image size will be $3\times M\times N$. To represent this color image as a single matrix all the color components are represented as a one-dimensional array. The array is reshaped into a single matrix by entering the numbers out in rows over a specified number of columns. If the matrix is incomplete, then the remaining spaces are padded with zeros. This matrix is multiplied with a random matrix of the same size to get the first stage encrypted image. The utilization of the random matrix minimizes the likelihood of hacking.

3.2 ARNOLD CAT MAP ENCRYPTION

The second stage of encryption is done by the ACM method. The ACM is a two-dimensional invertible chaotic map that is employed to vary the image's pixel positions without losing the information [15]-[17]. ACM algorithm encrypts the image by rotating the image k times so that the information in the image is no longer visible to a naked eye. Consider an image of size $N\times N$, the coordinates are $S = \{(a,b)|a,b=0,1,2,...,N\text{-}1\}$ the 2D ACM can be mathematically defined as Eq. (1)

$$\begin{bmatrix} a' \\ b' \end{bmatrix} = A\begin{bmatrix} a \\ b \end{bmatrix}(\bmod N)$$

$$= \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix}(\bmod N) \qquad (1)$$

The determinant (A) = $1\cdot(a',b')$ is the new position of the original pixel position (a,b).

$\begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}$ is the 2D scrambling matrix, where p and q are positive integers. The result of applying ACM for k iterations will give a random image which consists of all the pixel values of the original image but in different positions. The values of p, q and the number of iterations k act as secret key to increase the security of the original image. The main benefit of using this algorithm is that the correlation between the neighboring pixels is completely disturbed. After the transformation, the image gets a noisy appearance. Due to the cyclic nature of the transform number of iterations hinge on the size of the input image. The time taken to reconstruct the original image increases as the size of the given image increases. The inverse transform to recover the image is mathematically given by Eq.(2),

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} pq+1 & -p \\ -q & 1 \end{bmatrix}\begin{bmatrix} a' \\ b' \end{bmatrix}(\bmod N) \qquad (2)$$

3.3 VISUAL CRYPTOGRAPHY

VC is often used for image encryption. The general structure of color VC system consists of the color image $I[n]$ as its input and output have n number of shares $S_1[n],\ldots,S_n[n]$ as shown in Fig.1.

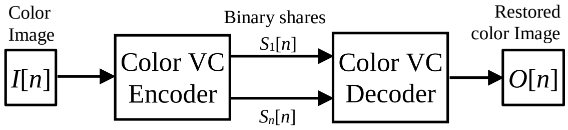


Fig.1. General Structure of Color VC system

These shares are binary images in indecipherable forms. These fragments of the image are sent on separate channels. As the entire image is not sent in one channel the secret image is secure. When the channels, shares are independent of each other security is optimum. Distributing trust is the sole purpose of VC. VC decoder recovers the color image by stacking the shares. The restored image $O[n]$ is obtained from Eq.(3),

$$O[n] = \prod_{i=1}^{n} S_i[n] \qquad (3)$$

4. PROPOSED FRAMEWORK

The proposed framework is illustrated in Fig.2. The transmission stage ends when shares are created. These shares are transmitted in different channels to ensure the security of the covert image. Considering shares as the input to the receiving system, the reverse process recovers the color covert image.

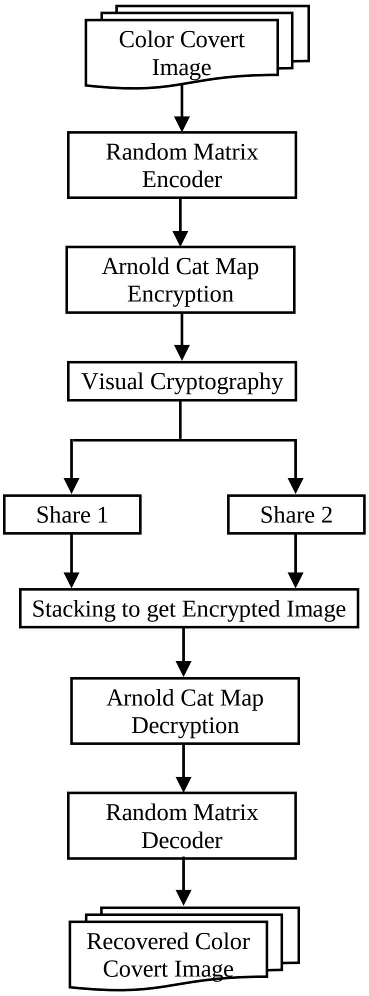

Color Covert Image
Random Matrix Encoder
Arnold Cat Map Encryption
Visual Cryptography
Share 1
Share 2
Stacking to get Encrypted Image
Arnold Cat Map Decryption
Random Matrix Decoder
Recovered Color Covert Image

Fig 2. Flowchart of the proposed framework

4.1 SHARE CREATION

The entire transmission process is further subdivided into subsections to understand the complete flow of the work. Pixel-by-pixel basis encryption is done. Pre-processing, encryption and share creation are the three stages in the transmission stage. The entire process is shown in Fig.3.

4.1.1 Pre-processing:

The random matrix encoder and the ACM method are used to generate an encrypted image. The Pre-processing stage involves encoding of the image to make sure the color image is ready for encryption. The input image *J*[*n*] is a color covert image fed to random matrix encoder that converts the three- dimensional color image into a one-dimensional array. Using random matrix multiplication, a two-dimensional image matrix is obtained.

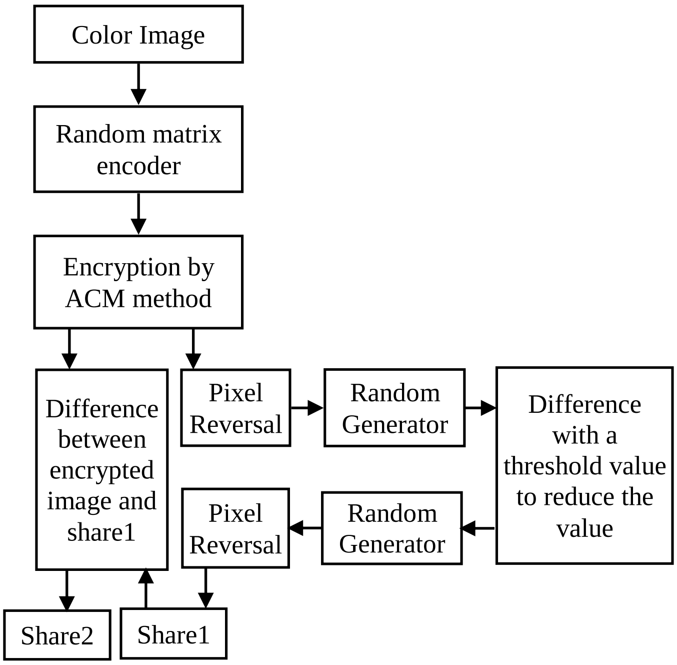


Fig.3. Process of share creation

The random matrix-encoding algorithm is as follows:

Input: RGB color image known as covert image

Output: 2D image

Step 1: 3D RGB is transformed into a 1D array

Step 2: One-dimensional array is expanded to the nearest square number by padding with zero

Step 3: The array is reshaped into two-dimensional matrix *S*

Step 4: A random matrix *T* is generated

Step 5: *T* and *S* are multiplied to get an encrypted version *E* of the covert image

The steps are illustrated as an example. The 3D input color image is

$$A_i(;,;,1)=\begin{matrix}25 & 125 & 103\\ 36 & 67 & 110\\ 100 & 215 & 89\end{matrix}$$

$$A_i(;,;,2)=\begin{matrix}120 & 15 & 43\\ 136 & 102 & 10\\ 50 & 25 & 209\end{matrix}$$

$$A_i(;,;,3)=\begin{matrix}50 & 35 & 93\\ 67 & 12 & 130\\ 250 & 73 & 19\end{matrix}$$

Converting three dimensional into a one-dimensional array

```
                  Columns 1 through 16
25 36 100 125 67 215 103 110 89 120 136 50 15 102 25 43
                  Columns 17 through 27
        10 209 50 67 250 35 12 73 93 130 19
```

Reshaping into Two-Dimensional matrix

$$S = \begin{matrix} 25 & 103 & 15 & 50 & 93 & 0\\ 36 & 110 & 102 & 67 & 130 & 0\\ 100 & 89 & 25 & 250 & 19 & 0\\ 125 & 120 & 43 & 35 & 0 & 0\\ 67 & 136 & 10 & 12 & 0 & 0\\ 215 & 50 & 209 & 73 & 0 & 0 \end{matrix}$$

Generating a random matrix. This random matrix changes every time the process starts. This ensures complete security as the random matrix cannot be predicted by the hacker

$$T = \begin{matrix} 2 & 2 & 2 & 1 & 2 & 2\\ 1 & 2 & 2 & 1 & 1 & 1\\ 2 & 1 & 1 & 1 & 2 & 1\\ 1 & 1 & 2 & 1 & 2 & 1\\ 1 & 1 & 2 & 2 & 2 & 2\\ 1 & 2 & 1 & 1 & 2 & 1 \end{matrix}$$

Multiplying S and T to generate a Two-dimensional image matrix E.

$$E = \begin{matrix} 50 & 206 & 30 & 50 & 186 & 0\\ 36 & 220 & 204 & 67 & 130 & 0\\ 200 & 89 & 25 & 250 & 38 & 0\\ 125 & 120 & 86 & 35 & 0 & 0\\ 67 & 136 & 20 & 24 & 0 & 0\\ 215 & 100 & 209 & 73 & 0 & 0 \end{matrix}$$

4.1.2 ACM Encryption:

In this second stage encryption of image E is performed using ACM. For every element of the input image E, encrypted image F is obtained from Eq.(4)

$$F = E(\text{mod}(R\text{-}1,row)+1,\ (\text{mod}(C\text{-}1,col)+1)) \qquad (4)$$

To find R and C

$$\begin{bmatrix}1 & p\\ q & pq+1\end{bmatrix}\begin{bmatrix}a\\ b\end{bmatrix}$$

$$\begin{bmatrix}1 & 1\\ 1 & 2\end{bmatrix}\begin{bmatrix}a\\ b\end{bmatrix}$$

For a=1 and b=1

$$\begin{bmatrix}2\\ 3\end{bmatrix}$$

Then R=2, C=3.

Every pixel of the image undergoes this process to get the encrypted image F.

4.1.3 Share Generation by VC:

Shares are generated by using the Pseudo randomized VC technique that involves the following steps [18],[19]

Input: Encrypted image F

Output: Share1, Share2

Step 1: Pixel F_{ij} is the pixel value of F at i,j positions are taken as input.

Step 2: Pixel reversal on image F is performed i.e. $F_{ij}' = 255\text{-}F_{ij}$.

Step 3: G is obtained by reducing F_{ij}' randomly by using a pseudorandom number.

Step 4: By taking the difference between every element of G and a threshold value share 1 is generated.

Step 5: Difference between share 1 and encrypted image provides share 2.

4.2 DECRYPTION PROCESS

The two shares are taken as input to the decryption process as in Fig.4. The first step is to get back the encrypted image by taking the difference between the two shares. Decryption is done by using the ACM method to get back the Image E. Random matrix decoder receives E as its input and uses the random matrix T to recover the two-dimensional matrix S. The zeros existing in this matrix are detached and the remaining pixel values are arranged as a one-dimensional array. The color covert image is recovered from this array without any losses.

The decrypted image is calculated by Eq.(5),

$$S = F(\text{mod}(R\text{-}1,\ row)+1,\ (\text{mod}(C\text{-}1,\ col)+1)) \qquad (5)$$

For a' = 1 and b'= 1 of F

$$\begin{bmatrix}a\\ b\end{bmatrix} = \begin{bmatrix}pq+1 & -p\\ -q & 1\end{bmatrix}\begin{bmatrix}a'\\ b'\end{bmatrix}(\text{mod}\,N)$$

$$= \begin{bmatrix}2 & -1\\ -1 & 1\end{bmatrix}\begin{bmatrix}a'\\ b'\end{bmatrix}$$

$$\begin{bmatrix}1\\ 0\end{bmatrix}$$

Then R=1, C=0.

Every pixel of the image undergoes this process to get the decrypted image S. The original color image is recovered by using the Random matrix decoder. The steps involved in the decoding phase are

Input: Decrypted image D

Output: Color covert Image

Step 1: D is multiplied with the inverse of random matrix T to get back S.

Step 2: S is transformed into a 1D array

Step 3: Expanded elements are eliminated by removing the zeros

Step 4: The array is reshaped into a 3D matrix to get back the color covert image.

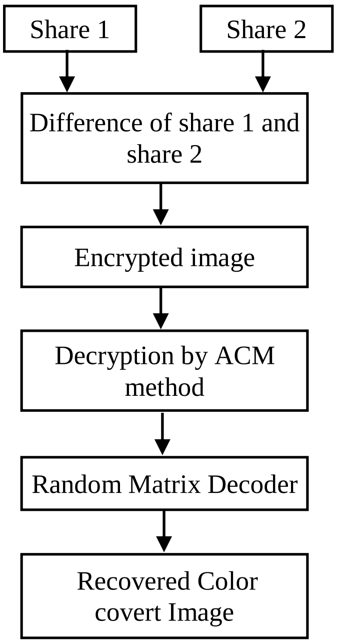
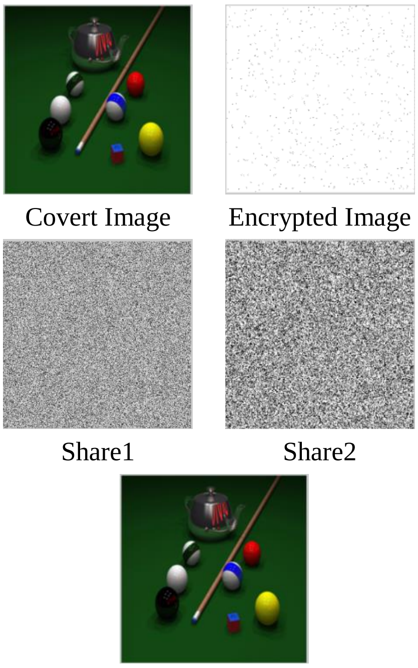


Fig.4. Process of secret image recovery

5. EXPERIMENTAL ANALYSIS

The proposed method is evaluated using color images. The color covert image of size 218×218 is considered. The experimental results in Fig.5 display the covert image, the encrypted image using random matrix encoder and ACM, the shares generated by VC technique and the recovered covert image


Covert Image Encrypted Image

Share1 Share2

Recovered Image

Fig.5. Experimental results

5.1 VISUAL QUALITY OF THE IMAGE

The contrast of the image can be analysed by testing the visual quality of the image. The measure of the visual quality is given by the PSNR value that is usually calculated in the logarithmic scale. A good visual quality image has higher value of PSNR. PSNR is computed as in Eq.(6),

$$\text{PSNR} = 20\log_{10}\left(\frac{255}{\sqrt{MSE}}\right) \tag{6}$$

and the MSE is given by Eq.(7).

$$MSE = \frac{1}{rc}\sum_{i=1}^{r}\sum_{j=1}^{c}\left(I_{mg}\left(i,j\right)-D_{mg}\left(i,j\right)\right) \tag{7}$$

The Table.1 shows the PSNR values of the original and recovered image, share 1 and share 2, encrypted image and share 1, encrypted image and share 2.

Table.1. PSNR values of different images

Images	PSNR
Original and recovered image	-
Share 1 and share 2	4.82
Encrypted image and share 1	6.91
Encrypted image and share 2	6.92

The PSNR value infinity between original and recovered image implies that the image is recovered without any losses. Therefore, the visual quality of the image is not compromised. The low PSNR values of the shares and the encrypted image infer that the original image is completely obscured and the hacker cannot get any information. This takes care of the security issue.

5.2 COMPARATIVE ANALYSIS

The comparison of the proposed scheme with color image sharing scheme based on share creation, security, basis of share generation and PSNR is shown in Table.2. The PSNR value depicts that the proposed scheme is able to recover the color covert image without any losses

Table.2. PSNR values of different images

Features	Narendra et al. [11]	Proposed
Type of Image	Color	Color
Color space	RGB	Direct
Size of the input image	256×256	218×218
Shares Generated	Blocks	Pixels
Share Creation	Dividing, sticking, camouflaging	Random matrix, ACM, pixel reversal, Random generator
PSNR	62dB	infinity
Security	One level	Three levels

5.3 SECURITY ANALYSIS: ANALYSIS OF CORRELATION COEFFICIENT

In an original image, the adjacent pixels are highly correlated vertically, horizontally and diagonally. A good encryption system reduces the degree of correlation as much as possible. The correlation coefficient of the nearby pixels is given by Eq.(8),

$$C = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$D = \frac{1}{N}\sum_{i=1}^{N} y_i$$

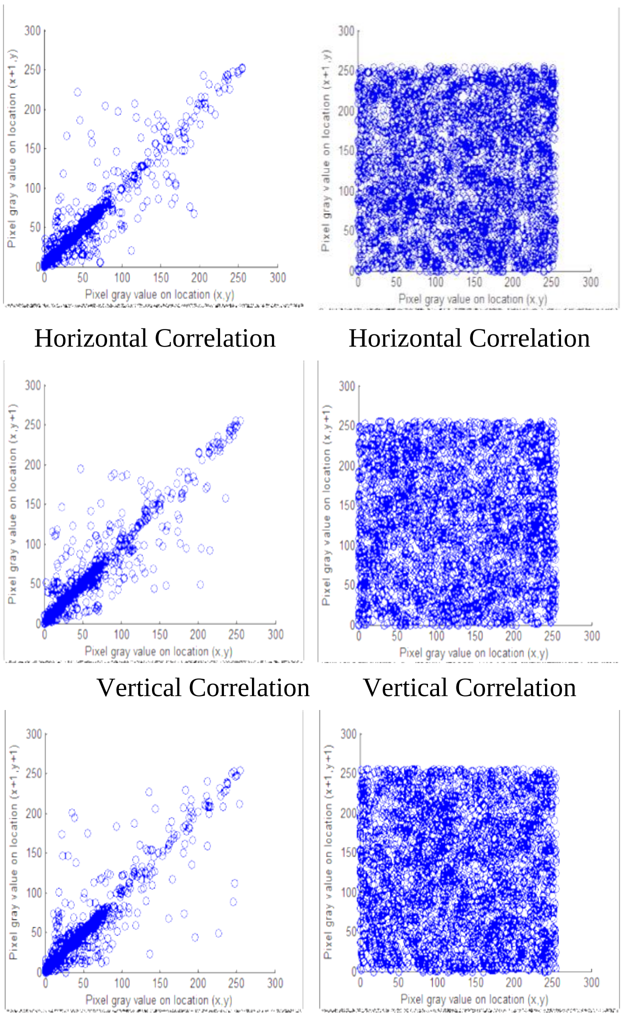
$$H = \frac{\sum_{i=1}^{N}(x_i - C)(y_i - D)}{\sqrt{\left(\sum_{i=1}^{N}(x_i - C)^2\right)\left(\sum_{i=1}^{N}(y_i - D)^2\right)}} \tag{8}$$

where,

N is the number of nearby pixels selected in the image,

X_i and Y_i is the values of nearby pixels vertically, horizontally and diagonally.

The analysis of the correlation of pixels in an original and encrypted images in all directions is shown in Fig.6.



Horizontal Correlation Horizontal Correlation

Vertical Correlation Vertical Correlation

Diagonal Correlation Diagonal Correlation

Fig.6. Correlation of image "Pool" and its encrypted image

The neighboring pixels in the covert image shows high correlation whereas neighboring pixels in the encrypted image shows weak correlation. The Table.3 shows the correlation coefficient of several images along three directions. It is seen that the correlation values of the encrypted images are close to 0 or less than 0 indicating a weak correlation between pixels. Similarly, it can be observed that the correlation of the original images is fairly strong. The results indicate the encryption technique is strong providing high security for the original color image.

Table.3. Correlation coefficient values of various test images

Correlation coefficient Analysis			
Image	**Orientation**		
	Horizontal	**Vertical**	**Diagonal**
Original pool	0.9507	0.9499	0.9677
Encrypted pool	**-0.0148**	**-0.0133**	**0.0135**
Original monarch	0.8925	0.8854	0.8902
Encrypted monarch	**0.0207**	**0.0097**	**0.0080**
Original bee	0.9772	0.9808	0.9785
Encrypted bee	**0.0227**	**0.0122**	**-0.0124**
Original tulips	0.9270	0.9368	0.9313
Encrypted tulips	**0.0135**	**0.0217**	**-0.0079**
Original rosebud	0.9707	0.9749	0.9765
Encrypted rosebud	**0.0150**	**-0.0045**	**-0.0237**
Original flower	0.9926	0.9904	0.9908
Encrypted flower	**-0.0113**	**0.0202**	**0.0076**

5.4 PERFORMANCE ANALYSIS

The average computation time (in sec) of each stage in the proposed algorithm is given in Table.4.

Table.4. Computation time

Stages	**Time elapsed in sec**
Random matrix encoder	0.342
ACM	1.78
VC	1.24
Total for share generation	3.36
decryption	2.55

The proposed method takes less time to be executed, which implies that it is appropriate for real-time, and is practical in many applications. It can also be observed that decryption time is less than encryption which decreases the computational complexity in the receiving section this time can be further reduced with code optimization and porting to a compiled language

6. CONCLUSIONS

Targeting at improving the visual quality of the recovered color image by VC we propose a novel framework to push the PSNR value to infinity. This framework is flexible and can be applied to any VC algorithm without sacrificing security. A novel method of converting the color image and recovering it back completely without converting into RGB or CMY color space is proposed. This brings about ease of management of color images.

A completely secure algorithm is designed by using Random matrix encoder, ACM and VC providing three levels of security. The experimental results show that the algorithm is not vulnerable to statistical attacks.

REFERENCES

[1] Xinyi Zhou, Wei Gong, Wen Long Fu and Lian Jing Jin, "An Improved Method for LSB Based Color Image Steganography Combined with Cryptography", *Proceedings of IEEE 15th International Conference on Computer and Information Sciences*, pp. 26-29, 2016

[2] Meera Kamath, Arpita Parab, Aarti Salyankar and Surekha Dholay, "Extended Visual Cryptography for color Images using Coding Tables", *Proceedings of IEEE International Conference on Communication, Information and Computing Technology*, pp. 1-6, 2012.

[3] Bin Yan, Yong Xiang and Guang Hua, "Improving the Visual Quality of Size-Invariant Visual Cryptography for Grayscale Images: An Analysis-by-Synthesis (AbS) Approach", *IEEE Transactions On Image Processing*, Vol. 28, No. 2, pp. 896-911, 2019.

[4] Ratnesh N. Chaturvedi, Sudeep D. Thepade and Swati N. Ahirrao, "Quality Enhancement of Visual Cryptography for Secret Sharing of Binary, Gray and Color Images", *Proceedings of IEEE International Conference on Computing Communication Control and Automation*, pp. 14-20, 2018.

[5] Feng Liu, Teng Guo, Chuan Kun Wu and Lina Qian, "Improving the Visual Quality of Size Invariant Visual Cryptography Scheme", *Journal of Visual Communication and Image Representation*, Vol. 23, No. 2, pp. 331-342, 2011.

[6] Chih-Ming Hu and Wen-Guey Tzeng, "Cheating Prevention in Visual Cryptography", *IEEE Transactions on Image Processing*, Vol. 16, No. 1, pp. 36-45, 2007

[7] Sudhir Rao, R. Anushree and Y. Kavitha, "A Novel and Highly Secure Encryption Methodology using a Combination of AES and Visual Cryptography", *Proceedings of International Conference on Advances in Computing, Communications, and Informatics*, pp. 112-118, 2016.

[8] K. Shankar and P. Eswaran, "RGB Based Multiple Share Creation in Visual Cryptography with Aid of Elliptic Curve Cryptography", *China Communications*, Vol. 14, No. 2, pp. 118-130, 2017.

[9] M. Karolin and T. Meyyappan, "Secret Multiple Share Creation with Color Images using Visual Cryptography", *Proceedings of International Conference on Communication and Signal Processing*, pp. 1-7, 2019.

[10] Shivani Pahuja and Singara Singh Kasana, "Halftone Visual Cryptography for Color Images", *Proceedings of International Conference on Computer, Communications and Electronics*, pp. 233-239, 2017.

[11] Modigari Narendra, Dhanya Ben, C.P. Jetlin and L. Jani Anbarasi, "An Efficient Retrieval of Watermarked Multiple Color Images using Secret Sharing", *Proceedings of International Conference on Signal Processing, Communications and Networking*, pp. 16-22, 2017.

[12] Ankush V. Dahat and Pallavi V. Chavan, "Secret Sharing Based Visual Cryptography Scheme using CMY Color Space", *Procedia Computer Science*, Vol. 78, pp. 563-570, 2016.

[13] R.M. Shiny, P. Jayalakshmi, A. Rajakrishnammal, T. Sivaprabha, "An Efficient Tagged Visual Cryptography for Color Images", *Proceedings of International Conference on Computational Intelligence and Computing Research*, pp. 261-267, 2016.

[14] Rubeena Jabi, Punyaban Patel and Deepty Dubey, "An Efficient Secure Data Transmission Based on Visual Cryptography", *Proceedings of International Conference on Research Advances in Integrated Navigation Systems*, pp. 1-7, 2016.

[15] Eko Hariyanto and Robbi Rahim, "Arnold's Cat Map Algorithm in Digital Image Encryption", *International Journal of Science and Research*, Vol. 5, No. 10, pp. 1363-1365, 2016.

[16] Priyanka Gupta, Sonia Singh and Isha Mangal, "Image Encryption based on Arnold Cat Map and S-Box", *International Journal of Advanced Research in Computer Science and software Engineering*, Vol. 4, No. 8, pp. 807-812, 2014.

[17] Manjit Kaur and Vijay Kumar, "Colour Image Encryption Technique using Differential Evolution in non-Subsampled Contourlet Transform Domain", *IET Image Processing*, Vol. 12, No. 7, pp. 1273-1283, 2018.

[18] Chien-Chang Chen and Wei-Jie Wu, "A Secure Boolean-based Multi- Secret Image Sharing Scheme", *Journal of Systems and Software*, Vol. 92, pp. 107-114, 2014.

[19] R. Babu, M. Sridhar and B. Raveendra Babu, "Information Hiding in Gray Scale Images using Pseudo-Randomized Visual Cryptography Algorithm for Visual Information Security", *Proceedings of International Conference on Information Systems and Computer Networks*, pp. 445-453, 2013.