ISSN 2303-4521
Periodicals of Engineering and Natural Sciences *Original Research*
Vol. 10, No. 2, April 2022, pp.358-375

Text image secret sharing with hiding based on color feature

Nuha J. Ibrahim[1], Yossra H. Ali [1], Alyaa Al-barrak [2] and Tarik Ahmed Rashid [3]
[1] Computer Science Department, University of Technology, Baghdad, Iraq
[2] Computer Science Department, college of science, University of Baghdad, Baghdad, Iraq
[3] Computer Science and Engineering Department, University of Kurdistan Hewler, Erbil, Iraq

ABSTRACT

The Secret Sharing is a scheme for sharing data into *n* pieces using (*k*, *n*) threshold method. Secret Sharing becomes an efficient method to ensure secure data transmission. Some visual cryptography techniques don't guarantee security transmission because the secret information can be retrieved if the hackers obtain the number of shares. This study present a secret sharing method with hiding based on YCbCr color space. The proposed method is based on hiding the secret text file or image into a number of the cover image. The proposed method passes through three main steps: the first is to convert the secret text file or image and all cover images from RGB to YC_bC_r, the second step is to convert each color band to binary vector, then divide this band in the secret image into four-part, each part is appended with a binary vector of each cover image in variable locations, the third step is converting the color space from YC_bC_r to RGB color space and the generated shares, hidden with covers, are ready for transmission over the network. Even if the hackers get a piece of data or even all, they cannot retrieve the whole picture because they do not know where to hide the information. The results of the proposed scheme guarantee sending and receiving data of any length. The proposed method provides more security and reliability when compared with others. It hides an image of size (234x192) pixels with four covers. The MSE result is 3.12 and PSNR is 43.74. The proposed method shows good results, where the correlation between secret and retrieved images is strong ranging from (0.96 to 0.99). In the proposed method the reconstructed image quality is good, where original and reconstructed images Entropy are 7.224, 7.374 respectively.

Keywords: Secret sharing, YC_bC_r color space, Visual cryptography

Corresponding Author:

Nuha J. Ibrahim
Computer Science Department
University of Technology
Baghdad, Iraq
Nuha.j.ibrahim@uotechnology.edu.iq

1. Introduction

Visual cryptography is a secret sharing scheme that allows encryption of a secret image among a number of participants, the decryption of the secret image requires neither knowledge of cryptography nor complex computation, it can encrypt a large amount of secret information, i.e., an entire image where the content can be versatile. VCS can be applied in secret sharing, information hiding, identification/authentication, copyright protection, etc. [1]. Access to very important resources via several authorized people is showing the necessity of secret sharing. Many techniques were improved to serve increasing levels of secret sharing security focusing on information privacy becoming one of the most significant computing sciences leading to growth in demand for data and media technologies [2, 3]. At present, effective management and protection of the content of digital multimedia, in addition to the prevention and deletion of computer crimes and increasingly dangerous information from illegal diversion, have become a point of contact in the field of information security [4-7]. The encryption techniques are used to ensure that the message is not damaged through the use of secret keys by different methods; thus, the eavesdropper cannot understand the confidential information. However, at the same time, the results of encryption can attract the attention of hackers, in addition, cryptographic algorithms are complex encryption and decryption operations require large space and time, then the secret sharing scheme is

used to enhance security and prevents authority fraud by avoiding the loss, modification, or destruction of important hidden information [8, 9]. Secret sharing divides the secret information into parts among participants group, where each part of the secret is taken by each participant, this part is called a share. These shares are combined together for recovering the secret. The secret cannot be retrieved with the loss of any of these secret parts. Visual cryptography is the new method in a cryptographic system, which is used for solving the secret sharing problem. The idea of visual cryptography is to hide secret information within images by encoding images into shares and decoding them later [10, 11]. Visual cryptography can encrypt the original image for providing more security by allowing the encryption of information where a decryption process can be done by the human visual system. The visual cryptographic system performance depends on different measures, for example, the type of secret image (color image, binary image), security, computational complexity, and accuracy [12, 13]. This paper proposes a schame based on hiding a secret text or image into a number of cover images by converting images from RGB to YC_bC_r color space and then to binary vector followed by hiding the information in the cover image with variable locations. In the extraction and restoration phase, the original image can be retrieved from variable locations of Y, C_b, and C_r color bands then these shares are combined together for reconstructing the hidden secret image.

2. Related work

In this section, available literature-published information related to the proposed method, Secret Sharing is introduced. Shamir [14] and Blakley [15] in 1979 proposed the first secret sharing method by using *(k, n)* secret sharing scheme, by dividing the image to a number of shares, the human visual system implements the decoding process without any difficult computation. The scheme uses the polynomial of order *(k −1)* as: $f(x) = a_0 + a_1x_1 + a_2x_2 + \cdots \ldots a_{k-1}x_{k-1} \quad (mod\ q)$ (1)

Where, a_0 the secret, q the prime number. The shares as a pair of (x_m, y_n) values.

$$y_n = \begin{cases} f(x_m) & 1 \quad \leq m \leq p \\ 0 & x_1 < x_2 \ldots < x_p \leq q-1 \end{cases} \quad (2)$$

A polynomial function $f(x)$ is smashed after each contributing own values (x_i, y_i)) where each contributing doesn't know the secret value a_0. The SSS Shamir's is the best secret sharing technique because it does not display the information about the secret. D.Wang, L.Zhang, N.Ma, X.Li [16] in 2007 proposed a probabilistic *(2, n)* and deterministic *(n, n)* method for grayscale images by using Boolean operations and have no pixel expansion. Chang and Kieu [17] in 2008 proposed a technique for embedding a secret image and bitstream into two shadow images. Then after extracting the stream of the secret bit, the secret image is restored pixel by pixel completely. J. Ida Christy and V. Seenivasagam [18] in 2012 proposed the Extended Visual Cryptography technique depending on Back Propagation by taking one secret image with two cover images of the same size as input to the system and producing two shares as system output. Vandana G. Pujari, et. al. [19] in 2014 proposed an OGWO using the Elliptic Curve method by separating the color image into three color bands and generating shares using pixel measures and partitioning shares to blocks. Ankush V. Dahat, et.al. [20] in 2016 used CMY color space for visual cryptography that was implemented with *((n-1), n)*, then compare the results with RGB color space that was free from security, pixel expansion, and accuracy issues. MohitRajput ,MarotiDeshmukh [21] in 2016 proposed the *(n, n + 1)*- MSIS method based on additive operation for images. Javvaji V.K. IN 2017 proposed (k,n) secret sharing method using XOR operations for enhancing the security of image by using the circular shifting method [22]. Her Chang Chaoa and TzuoYauFanb in 2017 proposed a secret sharing scheme with multi-level encoding using a random grid, where the original image and shares size are the same without expansion [23]. Wanmeng Ding et al. in 2018 proposed the (k,n) threshold secret sharing method using the matrix method [24]. Xuehu Yanaet al. in 2018 proposed the Chinese remainder method for secret sharing images in three decoding choices: capability of visual preview, grayscale recovery, and lossless recovery. In an encoding process, the random grid and the Chinese remainder are used for encoding the binary and grayscale images. In a decoding process, the grayscale recovery, visual previewing capability are applied [25]. Yu-Chi Chen et al. in 2018 presented an address shared one key scheme, where using multi-secret sharing as encryption, only the provider and receiver share the secret key without any knowledge from the data hider [26]. M. Karolin , T. Meyyappan [27] in 2019 used the blowfish algorithm to create the RGB images and share1, share2. The shares are encrypted and decrypted with the same original image. John Blesswin et al. in 2019 proposed an Enhanced Secret Sharing method that shares the gray-scale image with the receiver by using two

covers. Then the receiver reconstructs the secret image [28]. Nikhil C. Mhala in 2019 proposed the modified Visual Secret Sharing method to enhance the contrast of reconstructed medical images by using high-resolution idea [29].

3. The contribution of the work

This paper proposes a method based on hiding a secret text file or image into a number of the cover image. The hiding process is implemented in three steps: the first step is to convert the secret text file or image and all cover images from RGB to YC_bC_r, the second step is to convert each color band to binary vector then divide this band in the secret image into four-part, each part is appended with a binary vector of each cover image in variable locations where C_b color band hide in ascending order, C_r color band hide in descending order and Y color band hide after (C_b, C_r) locations depending on covers then each color band from binary to decimal for all images. The third step is converting the color space from YC_bC_r to RGB color space and the generated shares, hidden with covers, are ready for transmission over the network.
The results guarantee sending and receiving data of any length. The proposed method provides more security and reliability where even if the hackers get a piece of data or even all, they cannot retrieve the whole picture because they do not know where the information is hidden.

4. YC_bC_rColor space

The images are represented in (Red, Green, Blue) color space. where these images must be converted to another color space, for the reason of the sensitivity to color and brightness in the human visual system. The YC_bC_r are widely used in image and video techniques that are defined by the transformation from RGB color space [30]. The digital video standard develops YC_bC_r as a part of ITU-R. YC_bC_r scaled and YUV color space version.
The 8-bit with a range of 16– 235, defines Y, and the Nominal range of 16–240, defines the C_b and C_r [31]. The values of *RGB* color space can be transformed into YC_bC_rcolor space. In YC_bC_r the term Y component represents the brightness and C_b , C_r components represent the chrominance.
The individual eye is more sensitive to brightness and less sensitive to variations of colors and saturation. This means that the color and resolution of C_b and C_r can be reduced to the visual impact of the viewer. The color components RGB of the original image is transformed into less correlated color space YC_bC_r to reduce the spectral redundancy [32]. (See equations (3), (4), and (5)):

$$\begin{bmatrix} y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix} + \frac{1}{256} \begin{bmatrix} 65.738 & 129.057 & 25.064 \\ -37.945 & -74.494 & 112.439 \\ 112.439 & -94.154 & 18.285 \end{bmatrix} . \begin{bmatrix} Rn \\ \mathrm{Gn} \\ Bn \end{bmatrix} \quad (3)$$

$$(4)$$

$$(5)$$

The values of YC_bC_r color space can be back-transformed *RGB* color space by (See equations (6), (7), and (8)):

$$\begin{bmatrix} Rn \\ Gn \\ Bn \end{bmatrix} = \frac{1}{256} \begin{bmatrix} 298.082 & 0 & 408.583 \\ 298.082 & -100.291 & 208.120 \\ 298.082 & -516.411 & 0 \end{bmatrix} . \begin{bmatrix} \mathrm{Y} - 16 \\ \mathrm{Cb} - 128 \\ \mathrm{Cr} - 128 \end{bmatrix} \quad (6)$$

$$(7)$$

$$(8)$$

5. Proposed algorithm

The proposed algorithm is based on hiding the secret text file or image into a number of the cover image. This is done by converting the color space of the secret text file or image and the covers from the RGB to the YC_bC_r color space and converting each color band to a binary vector for all images then dividing this secret image information into 4 parts and hiding each part in cover image in variable locations where C_b color band hide in ascending order, and C_r color band hide in descending order, and Y color band hide after (C_b, C_r) locations depending on covers as shown in algorithm (1). Figure (1) describes the shares generation, hiding, and construction process.

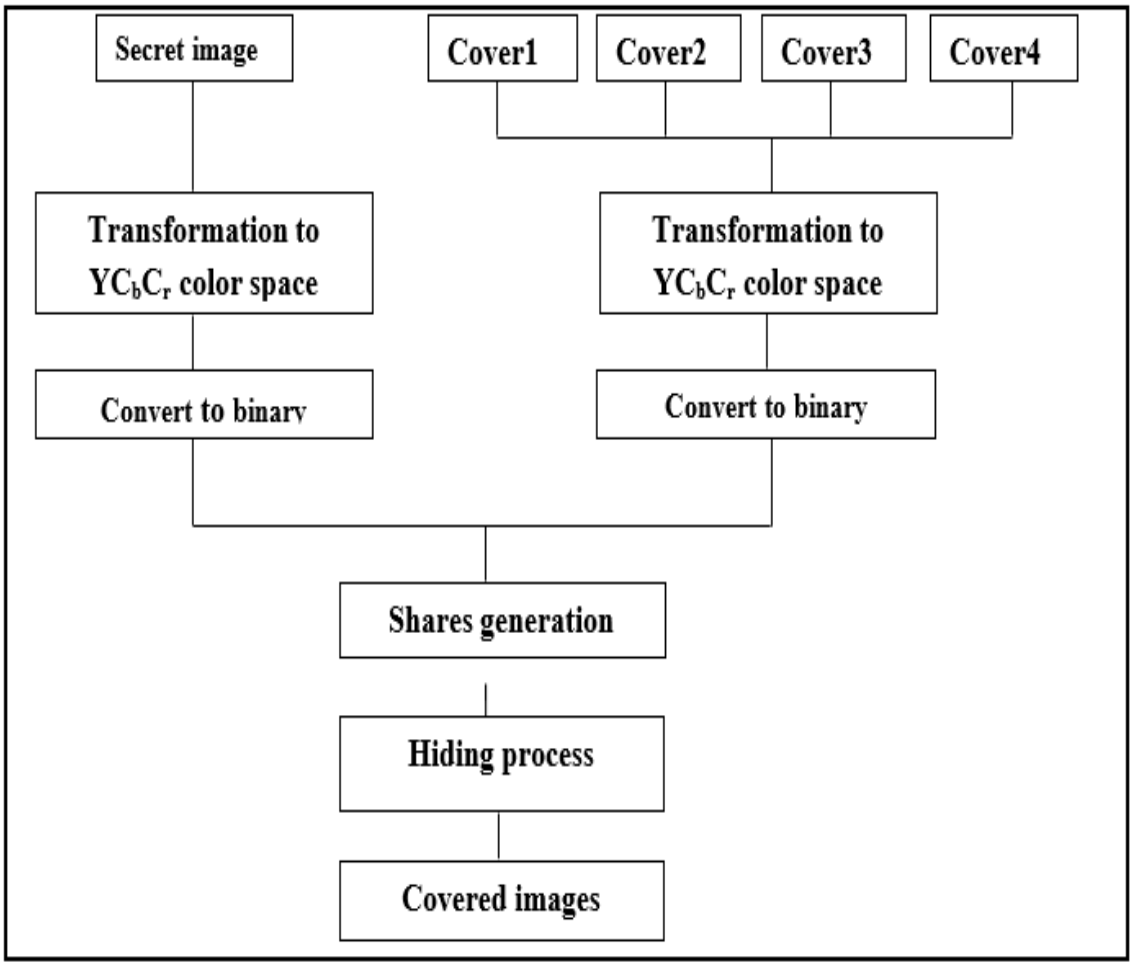

Figure 1. Shares generation

Algorithm 1: Hiding and Construction
Input: Original secret text file or image, Cover Images
Output: Covered images

Start
Step1: Get a secret text file or image and four covers
Step2: Do Until not EOF(image file, text file).
Step3: Separate the color component to three channels (R,G,B).
Step4: Convert RGB color space to YCbCr color space using equations (3), (4) and (5)
Step5: Convert YCbCr color band to binary vector for all images.
ybin = IntToBin(y)
cbbin = IntToBin(Cb)
crbin = IntToBin(Cr)
Step6: Divide the binary vector for all color band in the secret image into four-part.
Step7:Whilenot EOF
Cbshare1 = Mid(cbsecret, 1, 2)
Cbshare2 = Mid(cbsecret, 3, 2)
Cbshare3 = Mid(cbsecret, 5, 2)
Cbshare4 = Mid(cbsecret, 7, 2)

Crshare1 = Mid(crsecret, 7, 2)
Crshare2 = Mid(crsecret, 5, 2)
Crshare3 = Mid(crsecret, 3, 2)
Crshare4 = Mid(crsecret, 1, 2)

Yshare1 = Mid(Ysecret, 3, 2)
Yshare2 = Mid(Ysecret, 1, 2)
Yshare3 = Mid(Ysecret, 7, 2)
Yshare4 = Mid(Ysecret, 5, 2)
EndWhile

Step 8: each color band from binary to decimal for all images
y = BinToInt(ybin)
Cb = BinToInt(cbbin)
Cr = BinToInt(crbin)

Step9: convert the color space from YC_bC_r to RGB color space using the equations (6), (7) and (8)

Step10: A generated shares hidden with covers are ready to transmitted over the network.
End

In the reconstruction process, the original image value can be retrieved from variable locations of Y, C_b, and C_r color bands then these shares are combined together to reconstruct the secret image as shown in algorithm2. Figure2 describes the reconstruction of the original image.

Algorithm 2: Reconstruction Process
Input: Covered images
Output: Original secret image or text file

Begin
Step1: *For all shares*Do Until not EOF(image file or text file).
Step2: Separate the color component to three channels (R,G,B).
Step3: Convert RGB color space to YCbCr color space using equations (3), (4) and (5)
Step4: Convert YCbCr color band to binary vector for all images.
ybin = IntToBin(y)
cbbin = IntToBin(Cb)
crbin = IntToBin(Cr)
Step5*: Retrieve the value of the original image from shares by*
Step6:Whilenot EOF
Cb1 = Mid(Cbshare1, 1, 2)
Cb2 = Mid(Cbshare2, 3, 2)
Cb3 = Mid(Cbshare3, 5, 2)
Cb4 = Mid(Cbshare4, 7, 2)

Cbsecret = Cb1 & Cb2 & Cb3 & Cb4

Cr1 = Mid(Crshare1, 7, 2)
Cr2 = Mid(Crshare2, 5, 2)
Cr3 = Mid(Crshare3, 3, 2)
Cr4 = Mid(Crshare4, 1, 2)
Crsecret = Cr1& Cr2& Cr3& Cr4

Y1 = Mid(Yshare1, 3, 2)
Y2 = Mid(Yshare2, 1, 2)
Y3 = Mid(Yshare3, 7, 2)
Y4 = Mid(Yshare4, 5, 2)
Cr = Y1 &Y2 &Y3&Y4
EndWhile

Step 7:convert each color band from binary to decimal for all images
y = BinToInt(ybin)
Cb = BinToInt(cbbin)
Cr = BinToInt(crbin)

Step8: convert the color space from $YC_bC_r$to RGB color space using the equations (6), (7) and (8)

Step9:*Reconstructing the original image* or text file

End

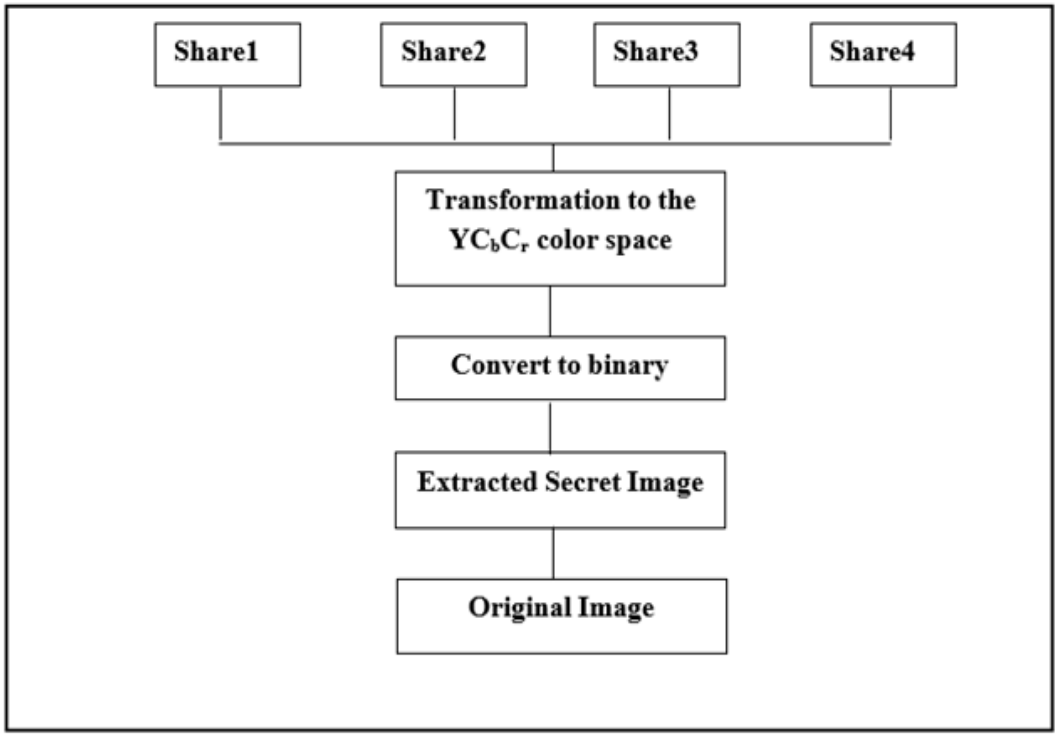

Figure 2. Reconstruction of Original Image

Example: This example in figure 3 shows the location of hiding the YCbCr color band of the secret image that is hidden in four cover images.

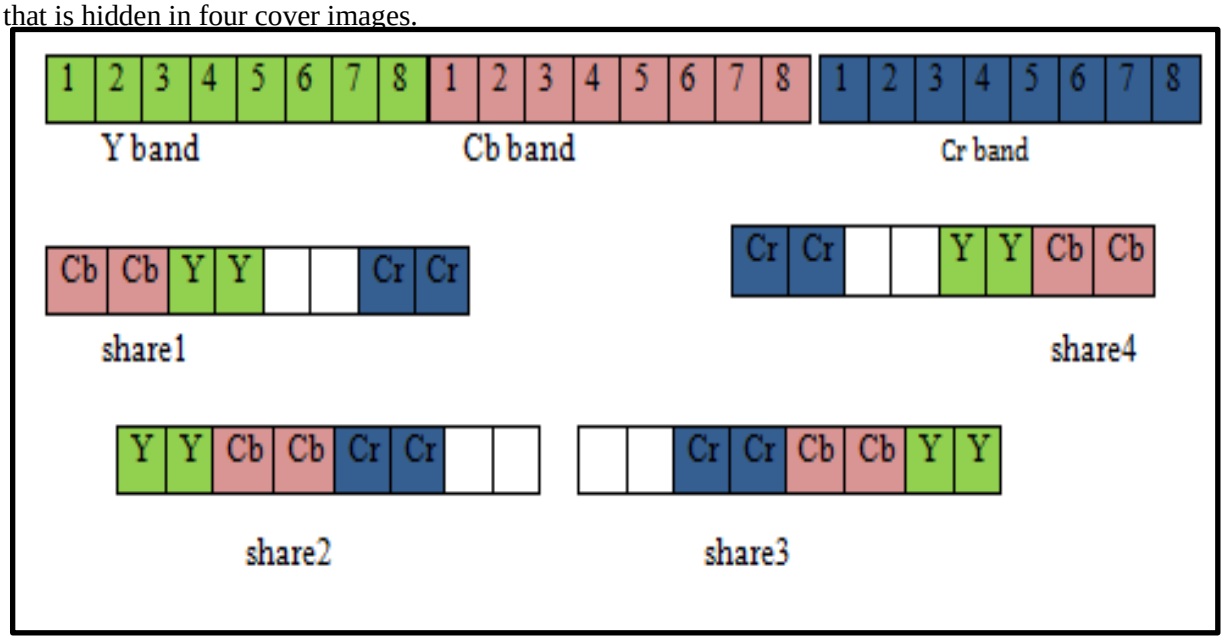

Figure 3. Location of hiding the YCbCr color band of the secret image

6. Experimental results

In this section, the results show that the proposed scheme is efficient in ensuring security. Figure 4 and Figure 5 show the secret and covered images.

Figure 4. Original images

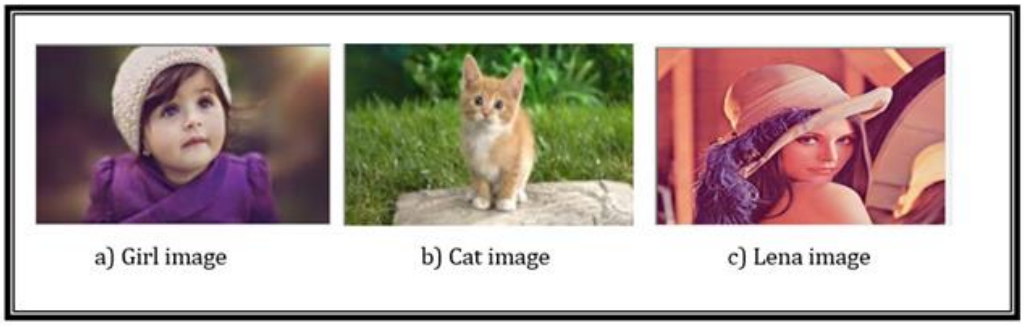

Figure 5. Cover images

The visual cryptography shares in YCbCr color spaces, generated by converting RGB to YCbCr color space equations (3), (4), and (5), the secret images in YCbCr color band are generated as illustrated in Figures (6),(7), and (8).

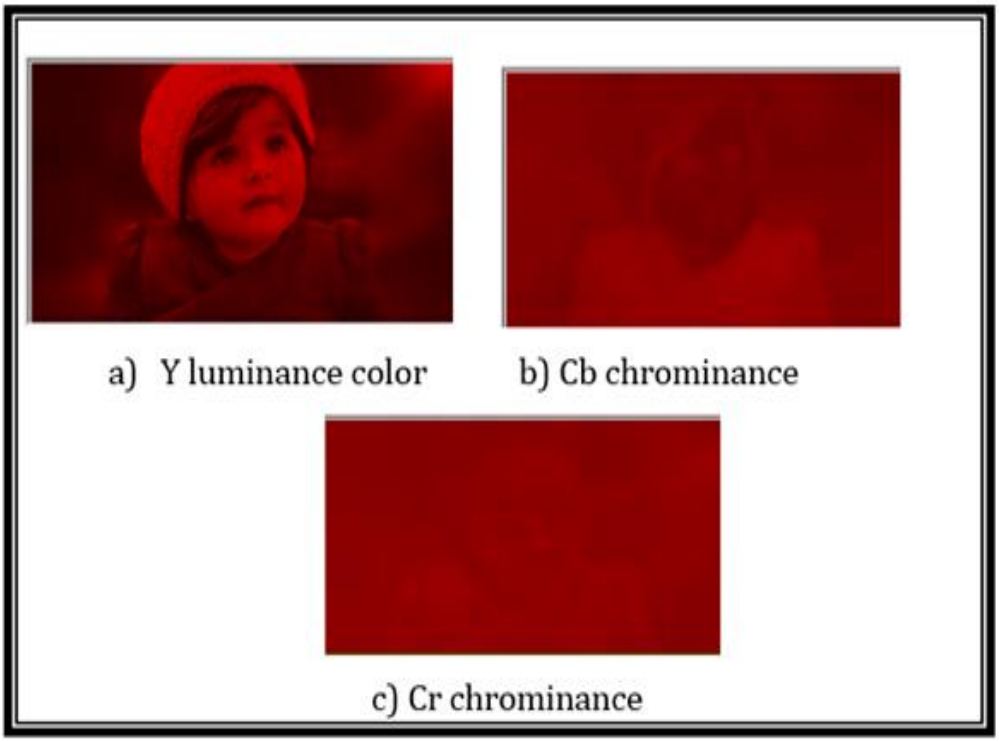

Figure 6. YCbCr color space of girl image

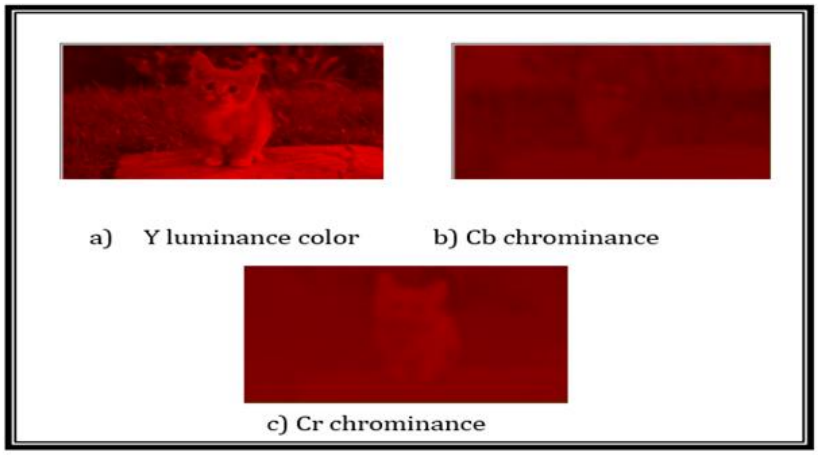

Figure 7. YCbCr color space of cat image

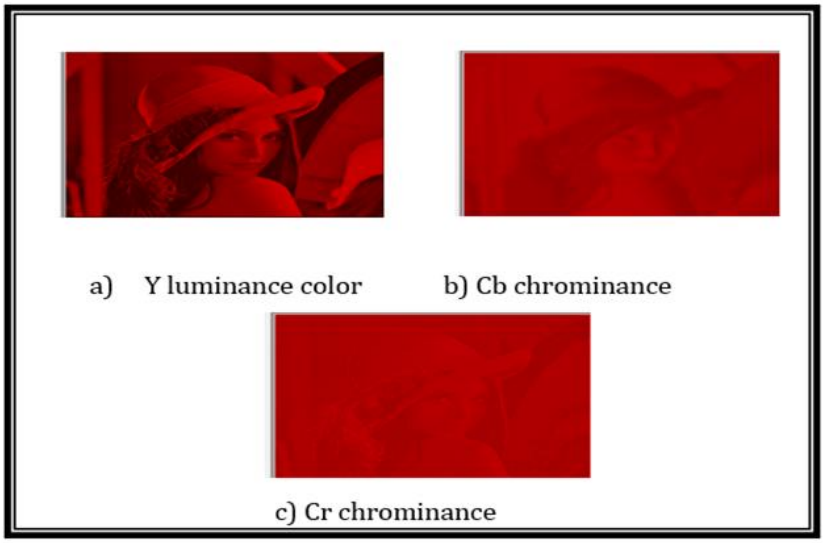

Figure 8. YCbCr color space of Lena image

After the conversion of the secret and cover images from RGB to YC_bC_r color space, each color band is converted to a binary vector for all images then dividing this secret image information into 4 parts for generating the four shares; the created shares are presented in Figures (9),(10), and (11).

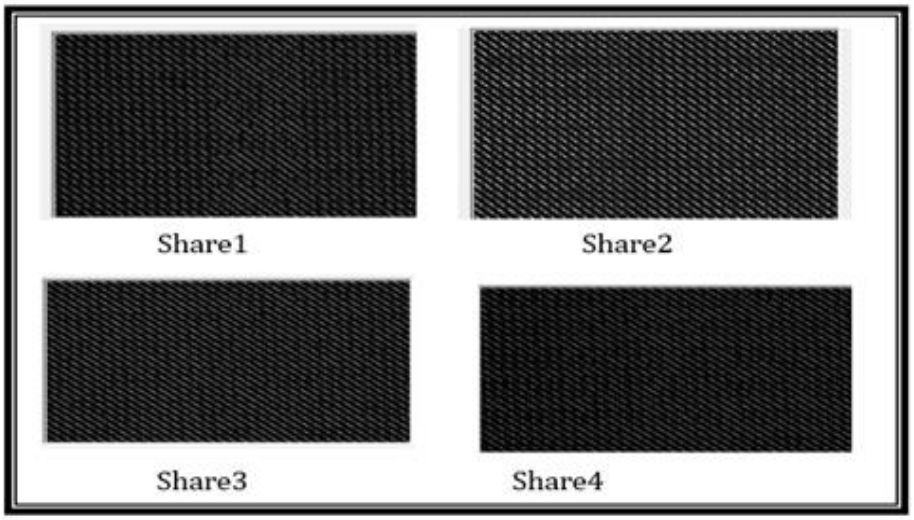

Figure 9. The 4 shares of girl image

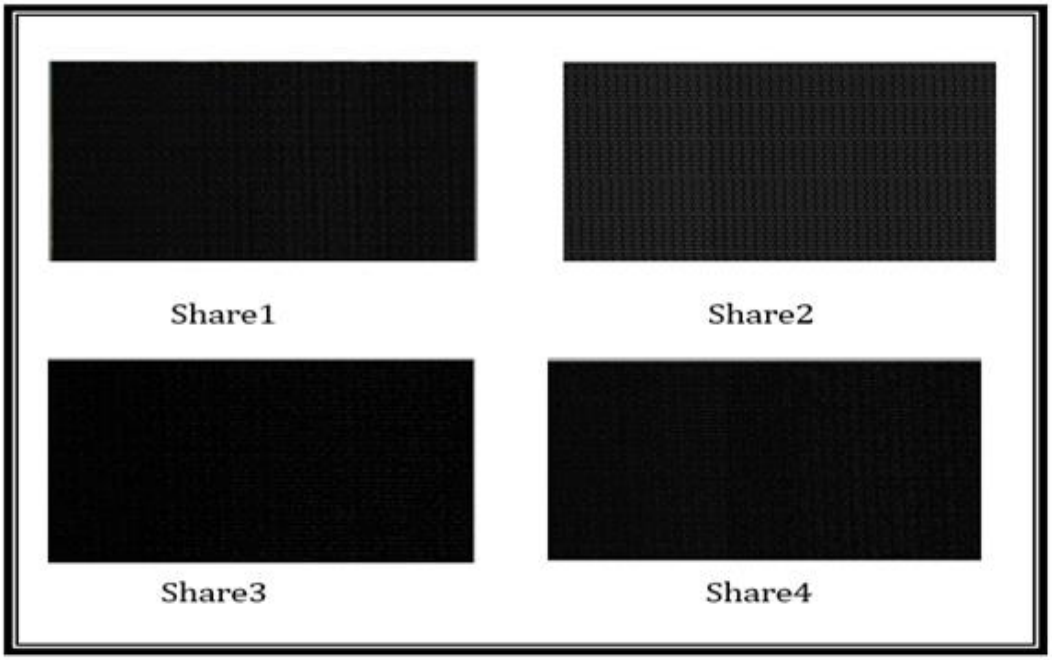

Figure 10**.** The 4 shares of cat image

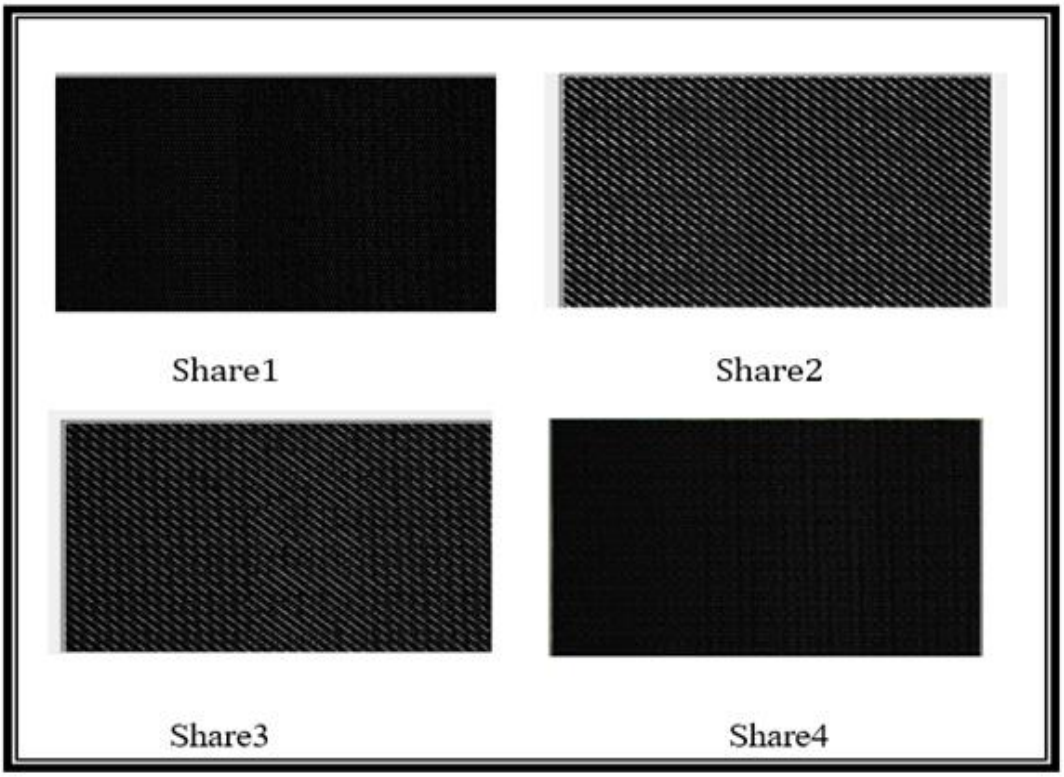

Figure 11**.** The 4 shares of Lena image

The shares generated from the secret image are hidden in cover images, the hiding process is done in variable locations where C_b color band hide in ascending order, C_r color band hide in descending order, Y color band hide after (C_b, C_r) locations depending on covers. The secret shares, embedded with covers, are shown in Figures (12),(13), and (14).

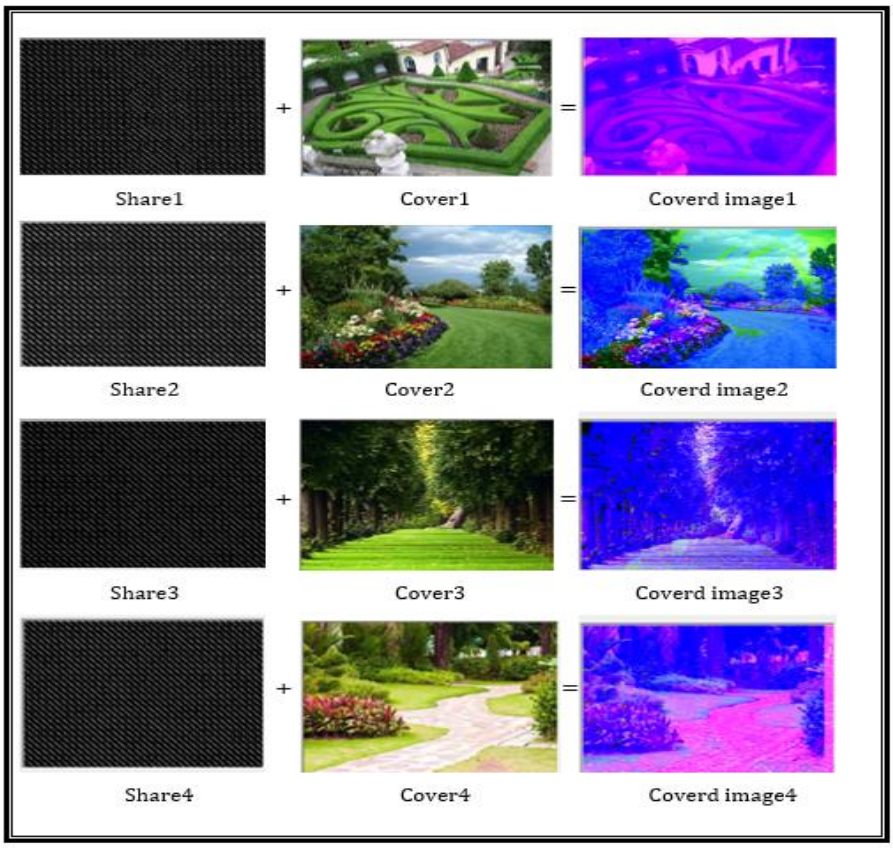

Figure 12. The embedded shares of girl image with covers

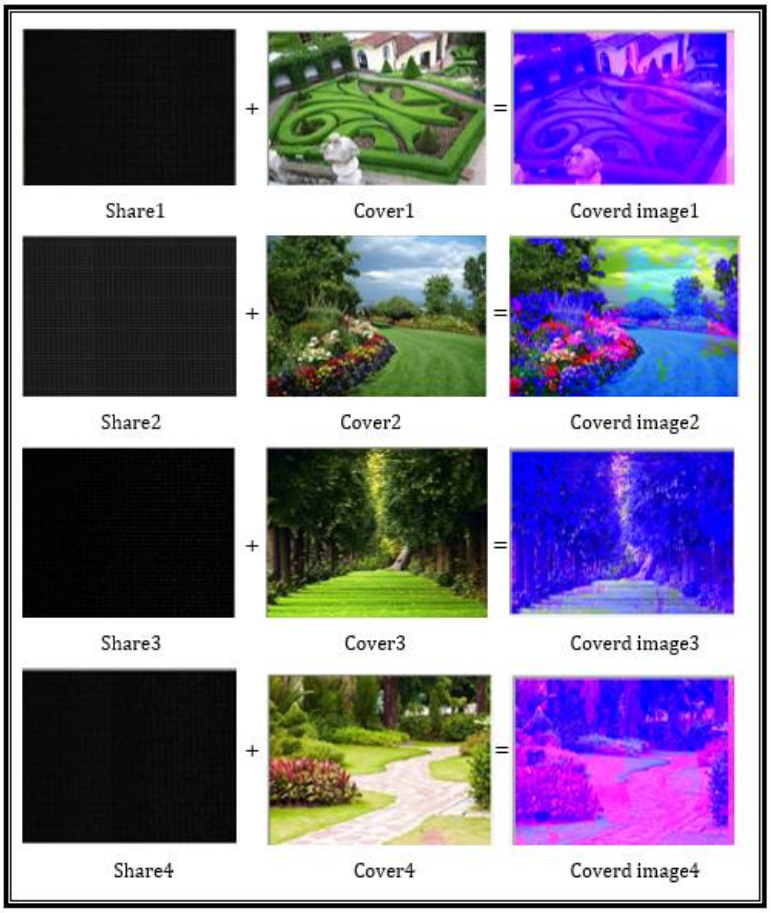

Figure 13. The embedded shares of the cat image with covers

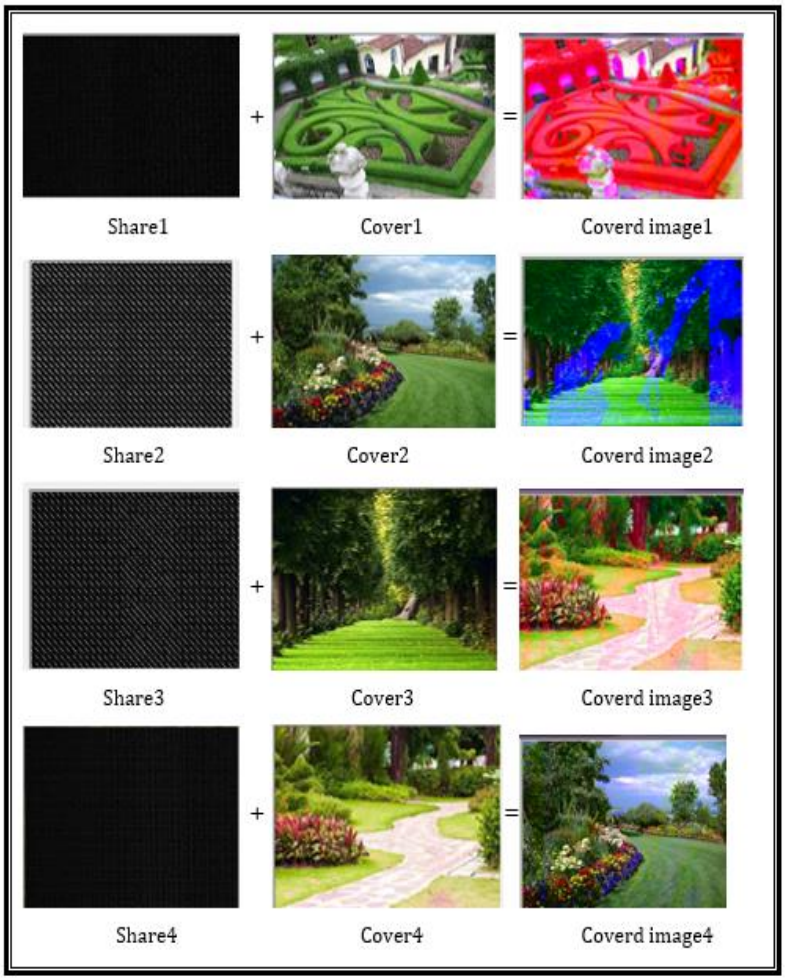

Figure 14. The embedded shares of the Lena image with covers

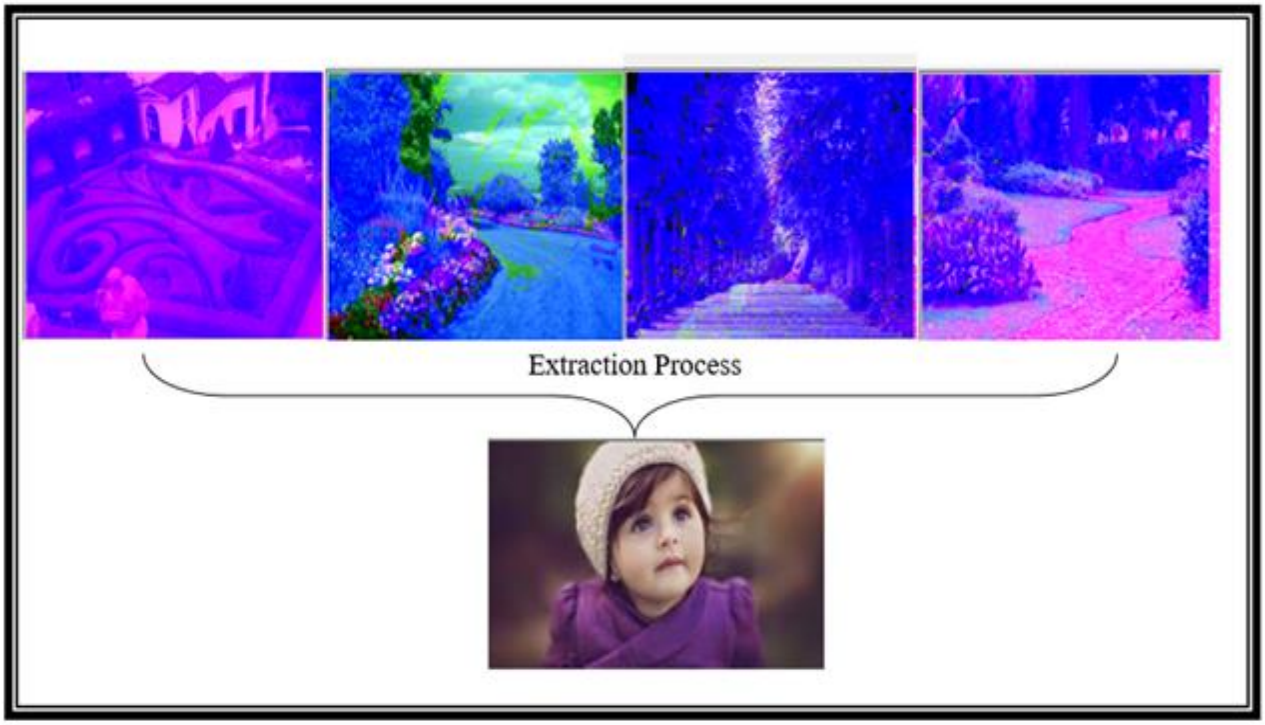

Figure 15. Reconstruction of girl image

In the reconstruction process, the shares are combined together for secret image reconstruction. Figures (15), (16), and (17) show the reconstruction of the secret image.

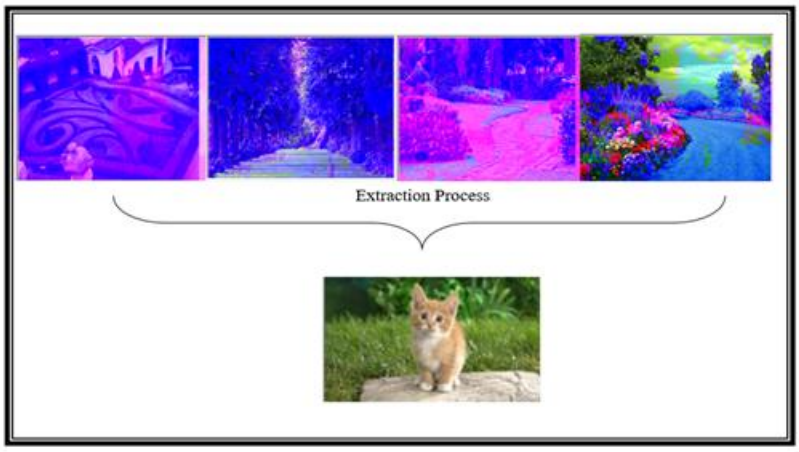

Figure 16. Reconstruction of cat image

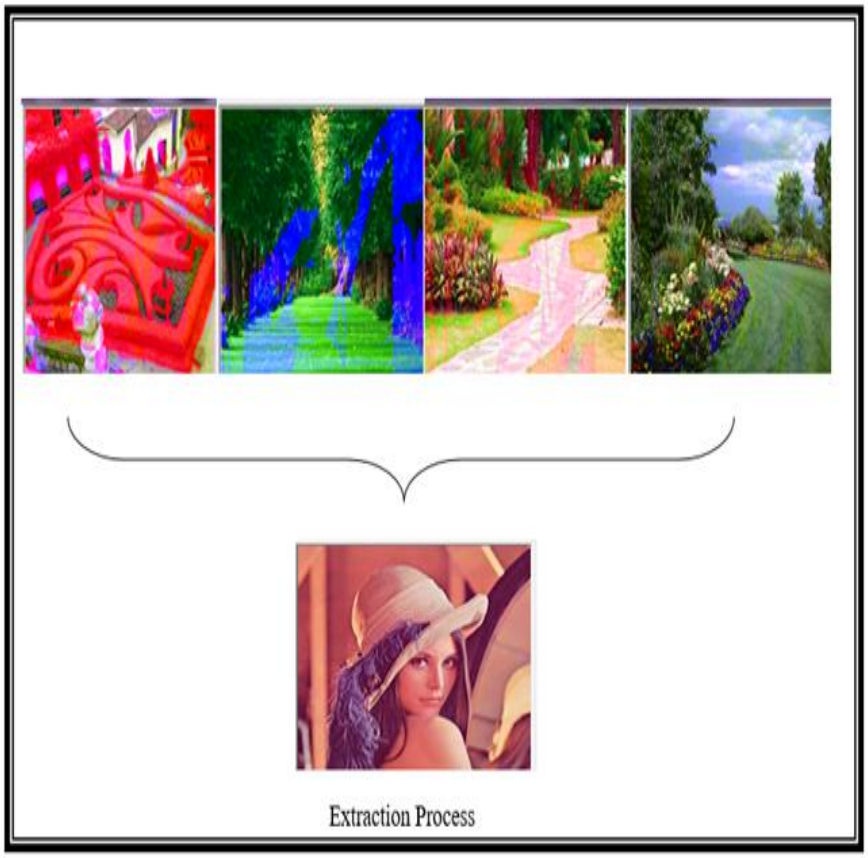

Figure 17. Reconstruction of Lena image

7. The discussion and measurement

To measure and ensure the method performance and image quality, many standard metrics such as PSNR, MSE, histogram, correlation are used and explained below:

1) PSNR

The PSNR (Peak Signal to Noise Ratio) is employed for measuring the quality of the image after embedding secret information in covers. The term (PSNR) represents the ratio between maximum signal value and distorting noise power that affects the quality of representation. Where PSNR is calculated as:

$$PSNR = 10\ log\ \frac{255^2}{MSE} \qquad (9)$$

Where *MSE* represents the mean square error between secret and reconstructed images. *MSE* is defined as:

$$MSE = \frac{1}{i\ x\ j}\sum_{m=1}^{i}\sum_{n=1}^{j}(H_{m\,x\,n} - H'_{m\,x\,n}) \qquad (10)$$

Where; $H_{m\,x\,n}$ denotes color pixel of the original image, $H'_{m\,x\,n}$ denotes color pixel of the reconstructed image, *i x j* denotes image size. For evaluating the performance of the proposed secret sharing schemes, Table 1, figure 18 show PSNR, MSE values for (girl, cat, Lena, baboon, plane, peppers, Barbara, and boat) images. Table 2, figure 19 show a comparison of the *MSE*, *PSNR* among the proposed approach in this work and other approaches.

Table 1. PSNR, MSE values

Image	PSNR	MSE
girl	44.731	2.913
cat	43.611	2.520
Lena	45.083	2.707
Baboon	45.586	2.864
Plane	43.016	3.268
Peppers	43.851	2.011
Barbara	45.903	3.284
Boat	45.624	3.807

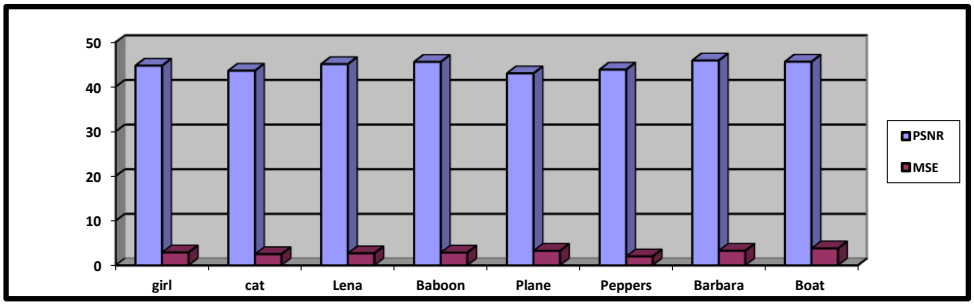

Figure 18. PSNR, MSE values

Table 2. Comparison of MSE, PSNR values

	D.Wang	Chang method	J. Ida Christy	Proposed method
Estimated MSE	7.54	10.5	6.7	3.12
Estimated PSNR	39.39	37.9	42.2	43.71

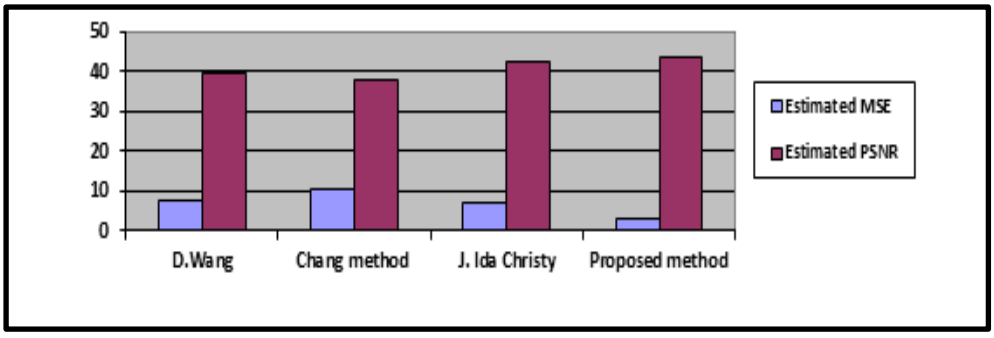

Figure 19. The *MSE*, *PSNR* among the proposed approach and other approaches.

2) The Histogram

The probability distribution of pixel values is drawn from the histograms for ensuring the security and the efficiency of the construction process, as shown in Figures (20), (21), and (22).

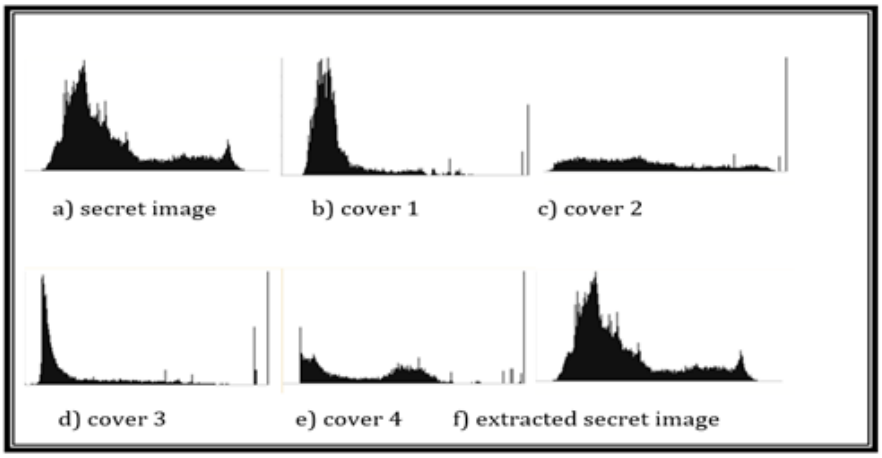

Figure20. Histogram of girl secret image

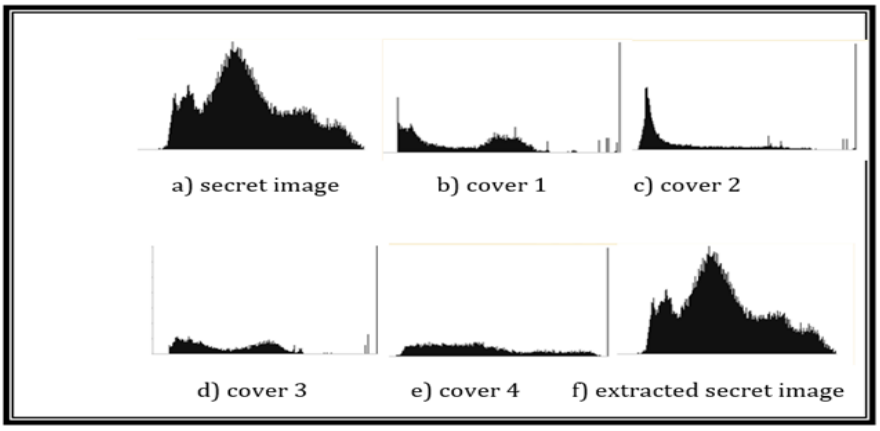

Figure 21. Histogram of cat secret image

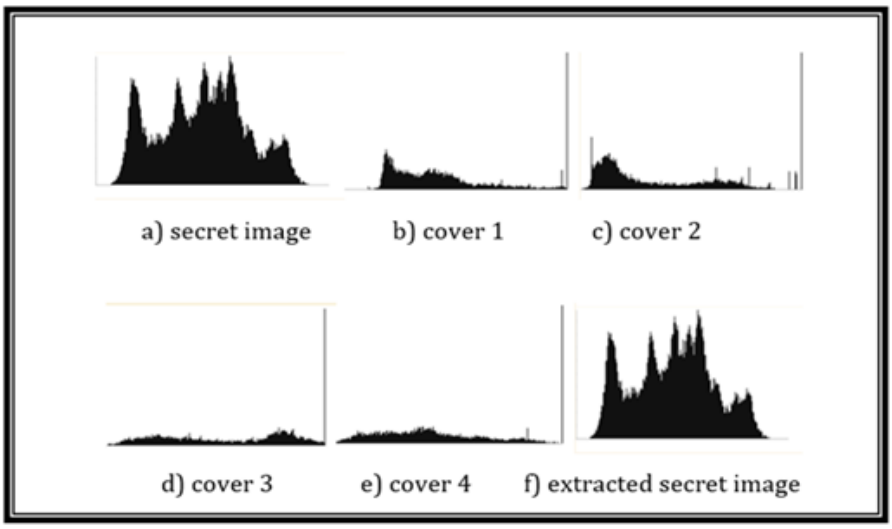

Figure 22. Histogram of Lena secret image

3) Correlation

Correlation shows the relationship between the secret and reconstructed images. The equation is defined as :

$$corr = \frac{\sum_{n=1}^{j}(X_n - X')-(Y_n - Y')}{\sqrt{\sum_{n=1}^{j}(X_n - X')^2}\sqrt{\sum_{n=1}^{j}(Y_n - Y')^2}} \quad (9)$$

where X ,Y are data of N values. X',Y' are mean data that given by:

$$X' = \frac{1}{i}\sum_{n=1}^{i} Xi \quad (10)$$

$$Y' = \frac{1}{i}\sum_{n=1}^{i} Yi \quad (11)$$

The correlation range between two images is between the interval [-1, +1]. The value 0 represents that no correlation exists between images, +1 represents the positive images' correlation, and -1 represents the negative images' correlation. Table 3, figure 23.show the correlation results.

Table 3. Correlation value between secret and reconstructed images

Image	correlation
girl	0.9623
cat	0.9741
Lena	0.9915
Baboon	0.9619
Plane	0.9443
Peppers	0.9705
Barbara	0.9530
Boat	0.9627

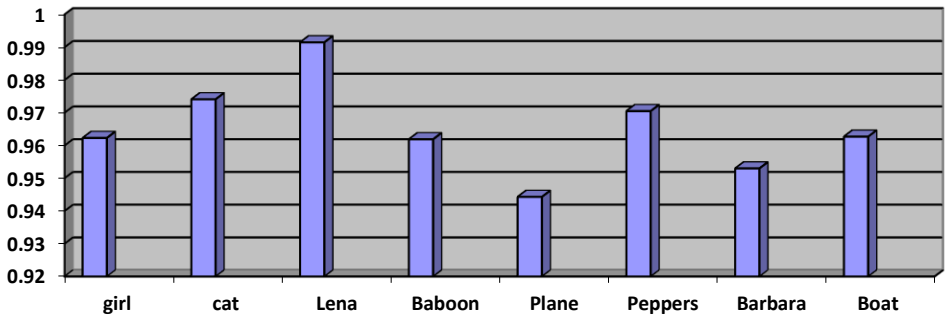

Figure 23. Correlation value between secret and reconstructed images

4) Entropy

Entropy is the statistical measurement of the randomness that is used for characterizing the texture of secret and reconstructed images. The Entropy equation is defined as:

$$H = -\sum_{k=0}^{G-1} P(k)\log_2(P(k)) \quad (12)$$

Table 4, figure 24 show the results of the Entropy between secret and reconstructed images.

Table 4. Entropy of secret, reconstructed images

Image name	secret image	reconstructed image
girl	7.27	7.31
cat	7.29	7.40
Lena	7.224	7.374
Baboon	7.477	7.885
Plane	7.631	7.994
Peppers	7.375	7.943
Barbara	7.445	7.452
Boat	7.12	7.479

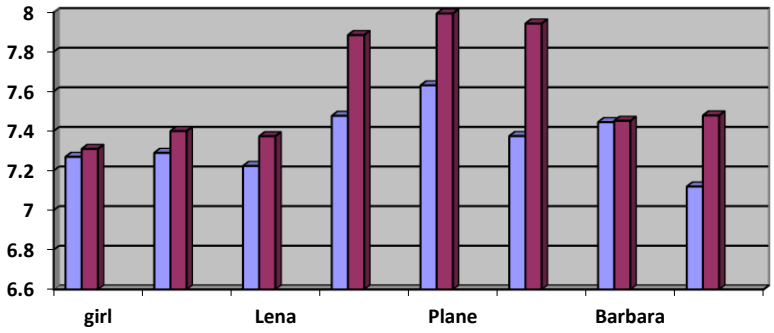

Figure 24. Entropy of secret, reconstructed images

8. Conclusions

In this paper, the secret-sharing method with a digital hiding technique, based on YCbCr color space, is proposed. The secret text file or image information is split into a number of shares; these shares are hidden in covers and distributed to many receivers. In the reconstruction process, the original image or text file value is retrieved from variable locations of Y, $C_{b,}$ and C_r color bands, and then these shares are combined together for reconstructing the secret image of text. Even if the hackers get a piece of data or even all, they cannot retrieve the whole picture because it does not know where to hide the information. The results of the proposed method guarantee sending and receiving data of any length. The proposed method provides more security and reliability. The effectiveness of the proposed algorithm is verified by the experimental results. These results show MSE with value (3.12) and PSNR is (43.74) that the correlation coefficient between secret and retrieved images is (0.96 to 0.99). The Entropy of the original and reconstructed images are 7.224,7.374 respectively. where these results show that the proposed algorithm has more security, verifiability, and low complexity.
As future work, we suggest many improvement models to Image Secret Sharing with Hiding based on Color Feature, such as encryption algorithm using Fourier transform and DNA [33]or encrypting the image by using the chaotic system and S-box optimization [34] and so on. The proposed algorithm can be extended for hiding multiple secrets with multiple shares.

Declaration of competing interest

The authors declare that they have no any known financial or non-financial competing interests in any material discussed in this paper.

References

[1] A. Gutub and K. Alaseri, "Hiding shares of counting-based secret sharing via Arabic text steganography for personal usage," *Arabian Journal for Science Engineering*, vol. 45, no. 4, pp. 2433-2458, 2020.

[2] A. Sendhooran and R. Latha, "Data Hiding with Encrypted Multi Secret Sharing using Modified LSB Technique," *International Journal of Engineering Research & Technology (IJERT),* vol. 10, no. 2, 2021.

[3] M. K. Abdul-Hussein, I. Obod, and I. Svyd, "Evaluation of the Interference's Impact of Cooperative Surveillance Systems Signals Processing for Healthcare," *International journal of online and biomedical engineering,* vol. 18, no. 3, 2022.

[4] S. B. Pawar and N. Shahane, "Visual Secret Sharing Using Cryptography," *International Journal of Engineering Research,* vol. 3, no. 1, pp. 31-33, 2014.

[5] L. Bai, S. Biswas, A. Ortiz, and D. Dalessandro, "An image secret sharing method," in *2006 9th International Conference on Information Fusion*, 2006, pp. 1-6: IEEE.

[6] H. Salim. H. Tauma, and N. Alseelawi, "A Novel Method of Multimodal Medical Image Fusion Based on Hybrid Approach of NSCT and DTCWT," *International journal of online and biomedical engineering,* vol. 18, no. 3, 2022.

[7] A. M. Alaidi Ibtisam A. Aljazaery, "Encryption of Color Image Based on DNA Strand and Exponential Factor," *International Journal of Online and Biomedical Engineering (iJOE),* vol. 18, no. 3, 2022.

[8] R. Lukac and K. Plataniotis, "Colour image secret sharing," *Electronics Letters,* vol. 40, no. 9, pp. 529-531, 2004.

[9] H. A. Naman, M. Al-dabag, and H. Alrikabi, "Encryption System for Hiding Information Based on Internet of Things," *International Journal of Interactive Mobile Technologies (iJIM),* vol. 15, no. 2, 2021.

[10] M. Cheraghchi, "Nearly optimal robust secret sharing," *Designs, Codes Cryptography,* vol. 87, no. 8, pp. 1777-1796, 2019.

[11] R. A. Azeez, M. K. Abdul-Hussein, M. S. Mahdi, and H. T. S. ALRikabi, "Design a system for an approved video copyright over cloud based on biometric iris and random walk generator using watermark technique," *Periodicals of Engineering Natural Sciences,* vol. 10, no. 1, pp. 178-187, 2022.

[12] G. Wu, M. Wang, Q. Wang, Y. Yao, L. Yuan, and G. Miao, "A Novel Threshold Changeable Secret Image Sharing Scheme," *Symmetry,* vol. 13, no. 2, p. 286, 2021.

[13] H. T. ALRikabi and H. T. Hazim, "Enhanced Data Security of Communication System Using Combined Encryption and Steganography," *International Journal of Interactive Mobile Technologies,* vol. 15, no. 16, 2021.

[14] A. Shamir, "How to share a secret. Commun. ACM," 1979.

[15] G. R. Blakley, "Safeguarding cryptographic keys," in *Managing Requirements Knowledge, International Workshop on*, 1979, pp. 313-313: IEEE Computer Society.

[16] D. Wang, L. Zhang, N. Ma, and X. Li, "Two secret sharing schemes based on Boolean operations," *Pattern Recognition,* vol. 40, no. 10, pp. 2776-2785, 2007.

[17] C.-C. Chang and T. D. Kieu, "Secret sharing and information hiding by shadow images," in *Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2007)*, 2007, vol. 2, pp. 457-460: IEEE.

[18] J. I. Christy and V. Seenivasagam, "Construction of color Extended Visual Cryptographic scheme using Back Propagation Network for color images," in *2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET)*, 2012, pp. 1101-1108: IEEE.

[19] P. Geetha, V. Jayanthi, and A. Jayanthi, "Optimal visual cryptographic scheme with multiple share creation for multimedia applications," *computers security,* vol. 78, pp. 301-320, 2018.

[20] A. V. Dahat and P. V. Chavan, "Secret sharing based visual cryptography scheme using CMY color space," *Procedia Computer Science,* vol. 78, pp. 563-570, 2016.

[21] M. Rajput and M. Deshmukh, "Secure (n, n+ 1)-multi secret image sharing scheme using additive modulo," *Procedia Computer Science,* vol. 89, pp. 677-683, 2016.

[22] J. V. Ratnam, P. R. Reddy, and T. S. Reddy, "Design of high secure visual secret sharing scheme for gray scale images," in *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 2017, pp. 145-148: IEEE.

[23] H. C. Chao and T. Y. Fan, "Generating random grid-based visual secret sharing with multi-level encoding," *Signal Processing: Image Communication,* vol. 57, pp. 60-67, 2017.

[24] W. Ding, K. Liu, X. Yan, H. Wang, L. Liu, and Q. Gong, "An image secret sharing method based on matrix theory," *Symmetry,* vol. 10, no. 10, p. 530, 2018.

[25] X. Yan, Y. Lu, L. Liu, J. Liu, and G. Yang, "Chinese remainder theorem-based two-in-one image secret sharing with three decoding options," *Digital Signal Processing*, vol. 82, pp. 80-90, 2018.
[26] Y.-C. Chen, T.-H. Hung, S.-H. Hsieh, and C.-W. Shiu, "A new reversible data hiding in encrypted image based on multi-secret sharing and lightweight cryptographic algorithms," *IEEE Transactions on Information Forensics Security*, vol. 14, no. 12, pp. 3332-3343, 2019.
[27] M. Karolin and T. Meyyappan, "Secret multiple share creation with color images using visual cryptography," in *2019 International Conference on Communication and Signal Processing (ICCSP)*, 2019, pp. 0058-0062: IEEE.
[28] J. Blesswin, C. Raj, and R. Sukumaran, "Enhanced semantic visual secret sharing scheme for the secure image communication," *Multimedia Tools Applications*, vol. 79, no. 23, pp. 17057-17079, 2020.
[29] N. C. Mhala and A. R. Pais, "An improved and secure visual secret sharing (VSS) scheme for medical images," in *2019 11th International Conference on Communication Systems & Networks (COMSNETS)*, 2019, pp. 823-828: IEEE.
[30] A. Koschan and M. Abidi, *Digital color image processing*. John Wiley & Sons, 2008.
[31] H. Noda and M. Niimi, "Colorization in YCbCr color space and its application to JPEG images," *Pattern recognition*, vol. 40, no. 12, pp. 3714-3720, 2007.
[32] Y. Yang, P. Yuhua, and L. Zhaoguang, "A fast algorithm for YCbCr to RGB conversion," *IEEE Transactions on Consumer Electronics*, vol. 53, no. 4, pp. 1490-1493, 2007.
[33] M. Ben Farah, A. Farah, and T. Farah, "An image encryption scheme based on a new hybrid chaotic map and optimized substitution bo," *Nonlinear Dynamics*, 2019.
[34] M. Farah, R. Guesmi, A. Kachouri, and M. Samet, "A new design of cryptosystem based on S-box and chaotic permutation," *Multimedia Tools Applications*, vol. 79, no. 27, pp. 19129-19150, 2020.