

COLOR VISUAL CRYPTOGRAPHY USING MULTILEVEL THRESHOLDING AND AES ALGORITHM

Pravitha PS¹, Rajkumar K K²

¹Department of Information and Technology, Kannur University, India

²Department of Information and Technology, Kannur University, India

Abstract - Visual cryptography is a secret sharing approach to encrypt a secret image into n visual shares printed on transparencies, where decryption is performed by superimposing all these shares together. In this paper, we proposed a Visual Cryptography technique for encrypting color images using multilevel thresholding and the AES algorithm. Initially, the image is decomposed to its primary color elements then multilevel thresholding is applied to each of the color components individually. Multilevel threshold values are extracted in 10 different levels derived empirically. Once the thresholding is done, shares are constructed in such a way that, the first share contains the pixel values of Red Halftone and Green Halftone, share 2 is created by combining pixel values of Green Halftone and Blue Halftone and share 3 is the pixel values of Red Halftone and Blue Halftone respectively. Finally, an AES algorithm is applied to each of these shares to guarantee further security of the Data. In the Decryption process, the AES algorithm is performed on each of the encrypted shares. RGB components of the images are retrieved by extracting the Red values from share1, Green values from Share2 and finally Blue values from Share3. By stacking each RGB planes all together will reconstruct the original image back. The quality of the reconstructed image is compared with the original image by evaluating the PSNR and SSIM values of both the original and reconstructed image and it found that the reconstructed image retains almost the same quality as that of the original image that was encrypted.

Key Words: Visual Cryptography Scheme (VCS), multilevel thresholding, AES algorithm, Halftone image.

1. INTRODUCTION

Nowadays, with the rapid change in the networking scenario, the transmission of secret data over the Internet becomes more and more popular and challenging due to the dangerous situation of the eavesdroppers who try to hack the data or secret information during transmission over the Internet. While exchanging secret data or information to different parties through the networking system, the security issue is to be mulled over it. To oversee the security issue of secret messages in the form of

pictures, text, audio or video etc., we need a secure information system through which data can be transmitted to the web without leaking the information. With the help of Visual Cryptography (VC), visual information can be securely sent over the web. VC is a secret sharing scheme that permits visual data to be encoded and decoded with Human Visual System (HVS). It encodes Secret image (SI) into different transparencies called shares and superimposing a qualified number of shares to disclose the Secret image (SI). Naor and Shamir [1] proposed a simple and secure secret sharing approach without any cryptographic computation. The Secret image (SI) is broken into different shares and these shares are transmitted to n different participants through the medium. On the decryption phase, the recipients may disclose the SI by stacking a sufficient number of shares [1][2].

Color is the peculiarity of any visual perception system which is described through primary colors as Red (R), Green (G) and Blue (B). Visual cryptography is extended to color visual cryptography and it provides a mechanism for transmitting color images through the Internet by splitting the images into different shares as done by Naor and Shamir by extending their concept to color images. This was initially achieved by Verheul and Van Tilborg. They presented a Color Visual Cryptography (CVC) scheme for encrypting colored secret images (SI) into different color halftoned shares and the original color image can be reconstructed by superposing all these transparent shares together according to Naor and Shamir principle. So in this paper, we propose color visual cryptographic schemes using multilevel thresholding techniques with AES algorithm for providing better security to the secret information [2][8].

The paper is arranged as follows; In section II Standard Color visual cryptographic schemes followed by multilevel thresholding and AES algorithm are explained. In section III we discuss the related study conducted in this domain. Section IV explains the proposed method for color visual cryptographic schemes for transferring secret color image through the network. Sections V discuss the results and

performance Analysis about the outcome of the proposed procedure subsequently conclusion in section VI [4].

2. LITERATURE REVIEW

Visual cryptography (VC) is a secret sharing scheme which is introduced by Naor and Shamir in 1994[1]. It proposed a (k,n) VC scheme, a secret image(SI) is encrypted by splitting into various transparencies named shares[11]. Those shares are distributed among n participants. No participants know the shares given by another participant and by superimposing 'k' shares reveal the secret image and less than k shares cannot retrieve the secret image. The authors explained and implemented this scheme using binary images [1][11][22].

In 2002, Young Chang Hou has proposed "visual cryptography schemes with three methods for color images". In this scheme, *color decomposition* and *halftoning* approach are used to generate the shares, when the shares are stacked altogether to rebuild the secret image. This was the principal paper which utilized the decomposition and half toning procedure [6].

Yanhua Zhang [10] presented the first color transfer visual cryptography scheme. The proposed method needs a key for encoding and decoding CTVCS. This paper proposes a color transfer scheme that can be consolidated into the (k, n) visual cryptography model. In the encoder, a color picture is scrambled into n binary share images. When any k shares are collected, the secret picture can be reproduced with low complexity computations [10].

Q. Zhang and Q.Ding [11] proposed a digital image encryption technique using Advanced Encryption Standard (AES). AES is a symmetric block cipher used for encrypting a 128-bit block of data using a key length of 128 bits, 192 bits, or 256 bits. This paper puts forward a strategy that utilizes the AES algorithm with a key to encrypt the image. This strategy could accomplish a very good impact on image encryption and decryption algorithm. By using this strategy the original image can be effectively retrieved by the decryption algorithm which utilizes the same access structure that used in the encryption process. Further AES algorithm is simple to implement in both hardware and software and has laid a good foundation for subsequent image encryption process if any required [11].

Li Shundong, LI Jiliang, Wang Daoshun[12] executed the Region Incrementing Visual Cryptography Scheme (RIVCS) where the secrets of multiple regions can be uncovered by human visual frameworks in RIVCS since various areas

have diverse contrast. They have utilized a linear programming concept to design a binary (k, n) -RIVCS with the same contrast for all secrecy regions. The compromise is that this scheme includes bigger pixel development [12][13].

Pooja Kashyap and Renuka[14] proposed a "Visual Cryptography for color images by using multilevel thresholding" to enhance the contrast of the reconstructed images. The Secret image (SI) is half toned and then decomposed into different levels using multilevel thresholding. This framework uses five levels of threshold for share generation which utilizes HoU's second method. As it uses pixel expansion in share generation and the reconstructed image has twice the size of the original image. At the decryption process, the shares are combined to reveal the original image [14].

In the earlier visual encryption strategies, most of them utilizes binary half toning to construct shares that bear only two shades of any color(RGB), shade1 being the color with its highest pixel value as 255 and shade 2 being its lowest pixel value i.e. 0. Further Pooja Kashyap[14] also proposed a method through which the secrecy of the shares are accomplished by the primary level of encryption and it is transformed through the internet by ensuring the security of data with a stronger encryption algorithm. This share generated by this method also has pixel expansion and therefore the rebuild image has a size twice than that of the original image.

3. PROPOSED METHOD

In the proposed method of color visual cryptography using multilevel thresholding utilizes the decomposition and multilevel thresholding procedure to build shares from the half toned original RGB image. Once the shares are constructed then applied Advanced Encryption Standard algorithm (AES) on these shares to guarantee a more significant level of safety to the shares [14] The Encryption process initially decomposes the secret image (SI) into its color primaries dependent on the Additive color model. After this, three distinctive color segments of the secret image are obtained(R, G, B)[1]. Then multilevel thresholding is applied to each of the color components individually. Multilevel threshold values (RH, GH, and BH) are extracted in 10 different levels derived empirically. Shares are then formed in such a way that the first share has red and green pixel values extracted from RH and GH, the same way, share 2 contains green and blue pixel values extracted from GH and BH and finally share 3 contains red

and blue pixel values extracted from BH and RH respectively.

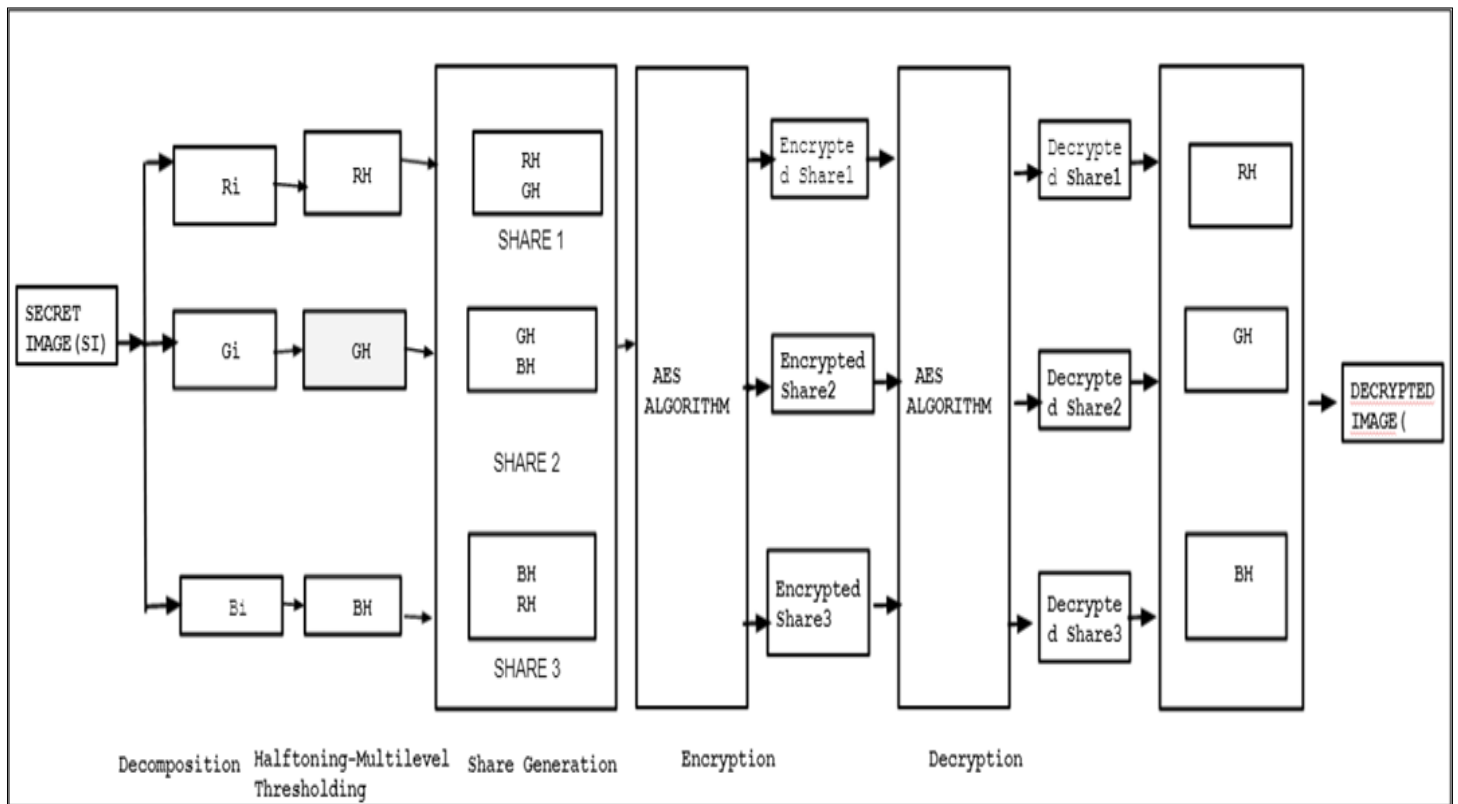
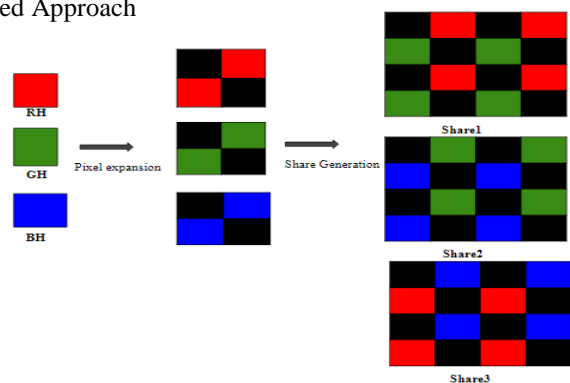


Fig. 1 Proposed Approach

Then, an AES algorithm is applied to each of these shares: Share1, share2, share3. During the Decryption process, the entire process is repeated in the reverse order such a way that the AES decryption algorithm is performed on each of the encrypted shares. Retrieve Red pixel values from share1, Green Pixel values from Share2 and Blue pixel values from Share3 respectively.

As a result of this step, RGB values of the decrypted images are obtained. At last stacking all three RGB planes together recover the original image back[8][13][14]. The Architecture of the proposed approach is Illustrated in Figure 1 ,Figure 2 shows the Overview of encryption technique . Initially secret image SI is decomposed into three primary color components as shown below,



$$\left. \begin{aligned} R &= SI(:, :, 1) \\ G &= SI(:, :, 2) \\ B &= SI(:, :, 3) \end{aligned} \right\} \quad (1)$$

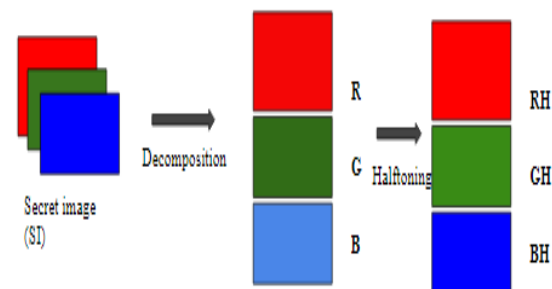


Fig.2 –Overview of Encryption without AES

Decomposition and Halftoning

Then basis matrices RH, GH, BH are constructed using the equation (8). Here multilevel thresholding is accomplished by 10 levels for every color component. At every level, the threshold value is derived empirically. The Threshold value is derived from every color plane ranging from 0-255 For MLT ,Extract pixel values in all the three planes R,G,B .if pixel value, Pij is 255 or 0 keep the same otherwise check whether pixel value is less than the thresholds, if Pij is less than threshold put the new pixel (Cij) value to Pij otherwise remains the same. To set thresholds select a 'd' and adjust the threshold and Cij is in the following format,

$$th = 0, d, 2d, 3d, \dots, \dots, 255 \text{ [16-19]},$$

$$\left. \begin{aligned} RH &= \text{Multithresh}(R, \text{Level}) \\ GH &= \text{Multithresh}(G, \text{Level}) \\ BH &= \text{Multithresh}(B, \text{Level}) \end{aligned} \right\} \quad (2)$$

Based upon the three halftones RHij, GHij, BHij [14], three distinctive shares are created, share1 is created by combining RH and GH components, share2 is created by combining GH and BH components and finally share3 is created by combining RH and BH components respectively[14][15][19][22] as shown in figure2. The entire share creation process is accomplished as follows:

Share Generation

$$\left. \begin{aligned} \text{Share1} &= RH \oplus GH \\ \text{Share2} &= GH \oplus BH \\ \text{Share3} &= RH \oplus BH \end{aligned} \right\} \quad (3)$$

After constructing the shares, every share is further encrypted using the AES algorithm which provides better security.

$$\left. \begin{aligned} \text{Share1} &= \text{AES}(\text{Share1}) \\ \text{Share2} &= \text{AES}(\text{Share2}) \\ \text{Share3} &= \text{AES}(\text{Share3}) \end{aligned} \right\} \quad (4)$$

In the decryption phase, first of all, the AES algorithm is applied to decrypt all the shares that are encrypted using the AES algorithm in the encryption phase.

$$\left. \begin{aligned} \text{Share1} &= \text{Decrypt_AES}(\text{Share1}) \\ \text{Share2} &= \text{Decrypt_AES}(\text{Share2}) \\ \text{Share3} &= \text{Decrypt_AES}(\text{Share3}) \end{aligned} \right\} \quad (5)$$

Once the shares are encrypted using AES, pixel-wise information of the image is extracted from share1, share2, share3 respectively, ie, retrieve Red Component values from share1, Green Component values from Share2, and Blue component values from Share3. As a result of this step, RGB Component values of the decrypted images are obtained.

By stacking RGB planes all together retrieve the original secret image back [14][23].

$$\left. \begin{aligned} SI(R, :, :) &= \text{Share1}(:, :, 1) \\ SI(:, G, :) &= \text{Share2}(:, :, 2) \\ SI(:, :, B) &= \text{Share3}(:, :, 3) \end{aligned} \right\} \quad (6)$$

3.1 Encryption and Decryption of shares

The work proposed in this paper uses encryption and decryption of shares. This is achieved through the multilevel thresholding and AES algorithm. In the Encryption process, first decomposes the RGB color images into three color planes after this, Applying multilevel thresholding on each of these three color planes individually. To apply multilevel thresholding, we used ten levels of threshold values computed empirically. For generating shares, we used hou's first method that creates three shares namely shares1, share2 and share3 from the half toned color planes. Finally, an AES algorithm is applied to each of these shares. Thus, encryptions of shares provide better and reliable data transmission through the network. In the decryption process, the encrypted shares are decrypted by stacking the half toned color planes together to recover the picture back, Just if all of the shares are stacked together, it is attainable to uncover the secret image. On the off chance that any of the portions of the encoded share is missing, it is hard to recuperate the secret image. [7][8].

3.1.1 Multilevel Thresholding

Multi-level thresholding (MLT) is a process in which pixels of an image are classified into sets or classes relying on their pixel values. For this classification, we need to choose a threshold value (th) and based on that threshold value, we have to classify the pixel values into different levels.

$$Cij = \text{Median}[th_n, th_{n+1}] \quad \text{if } Pij < th \quad (7)$$

Cij' represents the new Color pixel value, 'th' represents the threshold value," Pij' is the pixel value. In this work, we have used

10 different threshold values, to do MLT, Extract pixel values in all the three planes,if the pixel value, Pij is 255 or 0 keep the same otherwise check whether pixel value is less than the thresholds, if Pij is less than threshold put the new color pixel value(Cij) as shown in equation (1), otherwise keep the same pixel value. To set threshold values we have to select a 'd'.

$$d = \frac{Max-Min}{Level} \quad (8)$$

To set threshold we have to adjust d in the following format,

$$th=0,d,2d,3d,\dots,255 \quad (9)$$

Where Max is 255 and Min is 0, Level=1, 2,3,..N .By default, binary half toning have 2 threshold values (2level), 0and 255[7][9] .

3.2 Proposed Algorithm

ENCRYPTION

Input: Secret Color Image

Output: Encrypted Share

Steps1: Input secret image (SI)

Steps2: $R=SI(;;1)$

$G=SI(;;2)$

$B=SI(;;3)$

// Extract RGB pixel band values and create separate R, G,B matrices.

Steps3: $R=Multithresh(R,Level)$

$G=Multithresh(G,Level)$

$B=Multithresh(B,Level)$

//create basis matrices RH,GH,BH by applying Multilevel thresholding on each plane.

Steps4: $Share\ 1=Combine_pix(RH, GH)$

$Share\ 2=Combine_pix(GH, BH)$

$Share\ 3=Combine_pix(RH, BH)$

//Generate shares by combining RH,GH into Share1,GH,BH into Share2,RH and BH into share3.

Steps5: $Share1=AES(Share1)$

$Share\ 2=AES(Share2)$

$Share3=AES(Share3)$

//Use the AES algorithm to encrypt share1 , share and share3.

DECRIPTION

Input: Encrypted Shares

Output: Original Color image

Steps1: $Share1=Decry_AES(Share1)$

$Share2=Decry_AES(Share2)$

$Share3=Decry_AES(Share3)$

//Decrypt Share1,Share2 and Share3 using AES.

Step2: $SI(;;R)=Share1(;;1)$

$SI(;;G) = Share2(;;2)$































































































































$SI(;;B) =share3(;;3)$

//Extracts Red pixel value from Share1,Green pixel value from Share2,Blue pixel value from Share3.

Step 3: $D_SI(1;2;3)=SI(R;G;B)$

//combine the pixel values to reveal the original secret image.

Table 1 Examples of Proposed method

SL	SECRET IMAGE	RED	GREEN	BLUE	RH	GH	BH	SHARE 1	SHARE 2	SHARE 3	SHARE-AES	SHARE-AES	SHARE-AES	RECONSTRUCTED IMAGE
1														
2														
3														
4														
5														
6														
7														
8														
9														

4. EXPERIMENTAL RESULTS

The approach is implemented in Python 3.0 by using a local data set which comprises 10 different color images of sizes ranging from 256 x 256 to 1156 x 867. Initially, every image of the dataset is decomposed into its primary color plane as Red, Green, and Blue (R,G,B) using the additive color model. Once the decomposition process is over, apply multilevel thresholding on each of these three color planes separately. For applying multilevel thresholding on each color plane, we used 10 different levels of threshold values as shown in table 3 derived empirically (RH, GH, BH). Then three individual shares are constructed in such a way that by combining the red pixel and green pixel values of RH and GH for share1, share 2 is formed by combining the green and blue pixel values of GH and BH, and share 3 is formed by combining the red and blue pixel values of BH and RH respectively. Finally, the AES algorithm is applied to each of these three shares to provide higher level security. In the reconstruction phase, all the processes that we applied in the encryption phase are done in the reverse order to recover the image back [16]. Once the AES decryption process is applied on the three shares, the original color image is constructed by extracting the Red plane pixel values from share 1, Green pixel values from

Encrypted shares using AES i.e., Share1+AES, Share2+AES, Share3+AES. From the table(3), It very well may be effectively seen that no share uncovers any data about the mysterious image which shows that the secrecy of the shares is so well flawless. The decrypted image gotten has so much more color details within the image that is not conceivable without MLT. This is really a direct result of the quantity of levels (10) staggered thresholding present, inside the calculation proposed. Coming back to the secrecy of the shares, it is easily seen that no share can reveal any information conjointly the SI is uncovered as it were when all the three shares are together [1][18]. By considering the experimental results as shown in table4, secret image, its three-color halftone images,

Corresponding shares such as Share1, Share2, Share3, at the point of acquisition have additionally appeared in that table individually. It will in general be easily seen that no share reveals any information about the mysterious image, Which shows that the secrecy of the shares is so well flawless [1][18]

By analyzing the two quality parameters, PSNR and SSIM as shown in table 5, the results (By using the 10th level thresholding) obtained is promising and the quality of the reconstructed image is very close to the original image even though the image is half toned using Multi level thresholding and also we can easily see than proposed work is better than the existing (Binary –halftoning) algorithm [1][24].

Table 2 PSNR and SSIM of different images

Sl NO	IMAGE NAME	ORIGINAL IMAGE		SHARE GENERATION						SHARES ENCRYPTED USING AES						RECONSTRUCTED IMAGE	
				SHARE1		SHARE2		SHARE3		SHARE1		SHARE2		SHARE3			
		PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
1	Image 1	100	1	27.2	0.025	26.5	0.025	27.3	0.005	27.1	0.008	26.4	0.008	27.3	0.008	68.5	0.81
2	Image 2	100	1	26.5	0.023	25.9	0.025	26.4	0.005	26.1	0.009	25.8	0.009	27.3	0.009	69.12	0.8
3	Image 3	100	1	23.9	0.015	23.5	0.025	26.3	0.005	23.9	0.008	23.4	0.008	27.3	0.008	60	0.89
4	Image 4	100	1	23.2	0.02	23.5	0.025	26.3	0.005	23.2	0.008	23.4	0.008	27.3	0.008	68.22	0.87
5	Image 5	100	1	25.2	0.023	25.5	0.025	25.3	0.005	25.1	0.009	25.8	0.009	27.3	0.009	63.22	0.85
6	Image 6	100	1	25.3	0.023	25.5	0.025	25.3	0.005	25.1	0.009	23.4	0.009	25.1	0.009	68.22	0.82
7	Image 7	100	1	22.2	0.023	23.2	0.025	25.3	0.005	25.1	0.009	24.4	0.009	26.3	0.009	64.22	0.85
8	Image 8	100	1	24.2	0.023	25.1	0.025	25.3	0.005	25.1	0.009	25.2	0.009	25.1	0.009	60.22	0.83
9	Image 9	100	1	23.2	0.023	25.5	0.025	25.3	0.005	25.1	0.009	26.4	0.009	25.3	0.009	50.22	0.85
10	Image 10	100	1	25.2	0.023	22.5	0.025	25.3	0.005	25.1	0.009	24.4	0.009	24.3	0.009	68.22	0.85

Share 2 and Blue pixel values from Share 3. The individual color plane components R, G, and B as obtained from the shares as described above are then superimposed together to reveal the original image back [1][8][14].

Table 1 shows the Examples of Proposed Algorithm results, SI(Secret image),Decomposed SI-Red,Green,Blue, Multilevel threshold SI- RH, GH, BH and the corresponding shares such as Share1, Share2, and Share3 are also presented in the table. Next column represented the

5. CONCLUSION

We proposed an approach for color visual cryptography that mainly focused on the multilevel thresholding and AES algorithm of the color half-toned images. First, we decomposed the SI to primary components based on the additive color model [14]. After this, different color components of the secret image pull out separately from the original image and applied multilevel thresholding on every of these color components individually.

To apply multilevel thresholding, we used 10 levels of threshold values that are derived empirically. Then three shares are constructed in such a way by combining the red and green components to form share1, by combining green and blue components to form share2 and share3 is formed by combining the Red and Blue components of the picture that is obtained from three separated half toned images respectively. Finally, an AES algorithm is applied to every one of these three shares individually to ensure further security of the image [8]. In the Decryption processes decryption algorithm is performed on every one of the encrypted shares. Retrieve the Red Component values

from share1, Green Component values from Share2, and Blue component values from Share3. By stacking all these three color planes together, retrieve the original image back. The rebuild image obtained using Our proposed approach has the same size as that of the original image.

Further, we analyzed the quality of the rebuild by Using two mathematical parameters PSNR and SSIM the result obtained is promising and the quality of the rebuild image is very close to the Secret color image so HVS can't differentiate the image. While comparing contrast, the contrast of the rebuild image is improved.

REFERENCES

- [1] Naor, M and Shamir (1995) Visual Cryptography, in Advances in Cryptology - Eurocrypt. A. DeSantis, Springer-Verlag, Berlin, pp 1-12, 1995.
- [2] S.Manimurugan, K. Porkumaran. "A new fast and efficient visual cryptography scheme for medical images with forgery detection" , 2011 International Conference on Emerging Trends in Electrical and Computer Technology, 2011
- [3] Verheul, E.R., van Tilborg, H.C.A. Constructions and Properties of k out of n Visual Secret Sharing Schemes Designs, Codes and Cryptography **11**, 179-196(1997). <https://doi.org/10.1023/A:1008280705142>
- [4] Pushpendra K Rajput. "An EVCS for Color Images with Real Size Image Recovery and Ideal Contrast Using Bit Plane Encoding" , International Journal of Computer Network and Information Security, 2014
- [5] V. Rijmen, B. Preneel, Efficient colorvisual encryption for shared colors of Benetton, Eurocrypt'96, Rump Session, Berlin, 1996.
- [6] Young-Chang Hou. "Visual cryptography for colour images", Pattern Recognition, 2003
- [7] Abikoye Oluwakemi Christiana, Akande Noah Oluwatobi, Garuba Ayomide Victory, Ogundokun Roseline Oluwaseun. "A Secured One Time Password Authentication Technique using (3, 3) Visual Cryptography Scheme" , Journal of Physics: Conference Series, 2019
- [8] Shankar K., Eswaran P.. "Sharing a Secret Image with Encapsulated Shares in Visual Cryptography", Procedia Computer Science, 2015
- [9] "Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2020)", Springer Science and Business Media LLC, 2020
- [10] Luo, Hao & Chen, Hua & Shang, Yongheng & Zhao, Zhenfei & Zhang, Yanhua(2014). Color transfer in visual cryptography Measurement.51.81-90. 10.1016/j.measurement.2014.01.033.
- [11] Q. Zhang and Q. Ding, "Digital Image Encryption Based on Advanced Encryption Standard (AES)," 2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC), 2015, pp. 1218-1221, doi: 10.1109/IMCCC.2015.261
- [12] Li, Jiliang & Li, Shundong & Wang, Daoshun (2016) Region Incrementing Visual Cryptography Scheme with Same Contrast Chinese Journal of Electronics. 25. 621-624. 10.1049/cje.2016.06.002.
- [13] "Control, Computation and Information Systems", Springer Science and Business Media LLC, 2011
- [14] Pooja Kashyap, A. Renuka. "Visual Cryptography for colour images using multilevel thresholding", 2019 Third International Conference on Inventive Systems and Control (ICISC), 2019
- [15] Kaps JP., Sunar B. (2006) Energy Comparison of AES and SHA-1 for Ubiquitous Computing. In: Zhou X. et al. (eds) Emerging Directions in Embedded and Ubiquitous Computing. EUC 2006., vol 4097 Springer