I J C T A, 10(8), 2017, pp. 827-838 ISSN: 0974-5572

Efficient Visual Cryptography Technique for Authentication of Facial Images

Gopal D. Dalvi* and D.G. Wakade**

ABSTRACT

Security in this present reality is a vital issue to be taken care and to be experienced with different perspectives and preventive measures. In the present time, entire web is coming nearer from content information to mixed media information, one of the real security concerns is the insurance of this sight and sound information. Picture, which covers the most noteworthy rate of the media information, its assurance is essential. These might incorporate Military Secrets, Commercial Secrets and Information of people. This can be accomplished by visual Cryptography. It is one sort of picture encryption. In current innovation, the greater part of visual cryptography are implanted a mystery utilizing various shares.

Keywords: Visual Cryptography, Pixel-Sharing, sterilization Algorithm.

1. INTRODUCTION

Area of VC (Visual Cryptography) is ending up being fundamental in the present range in which information security is of most extraordinary concern. Security is a Basic part of Digital world [1]. Cryptography is of two sorts, basic Cryptography performs on content and Visual Cryptography performs on visual data (i.e. pictures, content). Fundamentally Cryptography is the investigation of keeping private data whether imparted over secured or unsecured channel from unapproved access, of guaranteeing information classification, trustworthiness and validation, and different undertakings [2].

Cryptography contains two stages' encryption and decoding. Sender scrambles (change over plain content into figure message) the message utilizing the mystery key and afterward sends it to the beneficiary. The collector unscrambles (change over figure content into plain content) the message to get the mystery data. Like cryptography, Visual Cryptography (VC) is a procedure which encodes the picture and changes over it into muddled arrangement and by unscrambling the picture unique mystery picture is acquired. Encryption is the way toward changing the picture into some other picture utilizing a calculation so that any unapproved individual can't remember it. Visual cryptography is reached out up to mystery sharing [3]-[4]. Visual mystery sharing scramble a mystery picture into straightforward parts which are called as shares with the end goal that stacking an adequate number of shares uncovers the mystery image [5]. It is an acquire from mystery sharing plan given by Adi Shamir in 1979. in which they demonstrated to partition information G as c parts r that G is effectively assemble from any C pieces, however even entire learning of c – 1 pieces uncovers definitely no data about information G[6] –[9].

Visual cryptography can likewise be fairly misleading to the unpracticed eye, in a manner that, if a picture share were to fall into the people hands, it would resemble a picture of arbitrary commotion or awful workmanship. Shading visual Cryptography is the novel approach in which shading picture is changed over to incoherent arrangement. RGB and its subset CMY shape the most fundamental and surely understood shading model Subtractive hues are apparent if shades in a catechism digest assertive wavelengths of white

* PhD Scholar SGBAU, *Email: Amravatidalvigopal80@gmail.com*

** Director, P.R.Pote College pf Engineering & Technology, Amravati, *Email: dr_dgwakade@rediffmail.com*

ablaze while apery the rest. Any brave question, whether accepted or man-made, ingests a few wavelengths of ablaze and reflects or transmits others; the wavelengths larboard in the reflected/transmitted ablaze accomplish up the concealment that can be seen. Red, green, and dejected are the capital jolts for animal concealment acceptance and are the capital added actuality hues. The abetting shades of RGB, cyan, maroon, and yellow, are affected by the alloy of two of the primaries and the abstention of the third. Red and blooming consolidate to accomplish yellow, blooming and dejected accomplish cyan, dejected and red accomplish fuchsia. The alloy of red, green, and dejected in abounding ability makes white. White ablaze is fabricated if all shades of the EM ambit accompany in abounding force [10]-[13].

2. DIFFERENT VISUAL CRYPTOGRAPHY SCHEME:

1. Visual Cryptography framework utilizing Cover Image Share installed security Algorithm (CISEA) [3].
2. Securing Visual Cryptography Shares utilizing Public Key Encryption [10].

3. COMPARATIVE STUDY OF DIFFERENT VISUAL CRYPTOGRAPHY METHODS

Sr. No	*Authors*	*Year*	*Secret Images*	*Pixel Expansion*	*Image Format*	*Share Generated*
1.	Naor and Shamir	1995	1	4	Binary	Random
2.	Wu and Chen	1998	2	4	Binary	Random
3.	Hsu et al	2004	2	4	Binary	Random
4.	Wu and Chang	2005	2	4	Binary	Random
5.	Chin-Chen Chang et	2005	1	4	Binary	Meaningful
6.	Liguo Fang et al	2006	1	2	Binary	Random
7.	S.J.Shyu et al	2007	n(n>=2)	2n	Binary	Random
8.	W. P. Fang	2007	2	9	Binary	Random
9.	Jen-Bang Fengel al	2008	n(n>=2)	3n	Binary	Random
10.	Mustafa Ulutas	2008	2	4	Binary	Random
11.	Tzung-Her Chen et al in	2008	2	1	Binary	Random
12.	Tzung-Her Chen et al	2008	n(n>=2)	4	Binary,	Random
13.	Wen-Pinn Fang	2009	2	1	Binary	Random
14.	Zhengxin Fu	2009	4	9	Binary	Random
15.	Jonathan Weir et a	l2009	n	4	Binary	Random
16.	Xiao-qing Tan	2009	1	1	Binary	Random
17.	Verheul Tilborg	1997	1	C*3	Color	Random
18.	Yang & Liah	2000	1	C*2	Color	Random
19.	Chang and Tsai	2000	1	529	Color	Meaningful
20.	Chin Chen Chang et al	2002	1	9	Gray	Meaningful
21.	Lukacand Plataniotis	2005	1	2	Color	Random
22.	R. Younmaran	2006	1	9	Color	Meaningful
23.	S.J.Shyu	2006	1	$[\log_2 c*m]$	Color	Random
24.	Mohsen Heidarinejad et al	2008	1	9/16	Color	Random
25.	Haibo Zhange et al	2008	1	1	Gray	Random
26.	F. Liu et al	2008	1	1	Color	Random
27.	Wei Qiao et al	2008	1	M	Color	Random
28.	Du-Shiau Tsai et al	2009	1	9	Color	Meaningful
29.	Roberto De Priso and Alfredo De Santis	2011	1	$m=[\log_3 n]$	Binary	Meaningful
30.	Chun-Yuan Hsiao and Hao-Ji Wang	2012	2	4	Binary	Meaningful
31.	Shyong Jian Shyu and Hung- Weg Jiang	2013	2	*m*	Binary	Random
32.	Kai-Hui Lee and Pei Ling Chin	2014	1	*n*	Color	Random

4. COMPARISON STUDY OF MSE & PSNR

Title of Paper	*Year*	*Author*	*MSE*	*PSNR*
Region Incrementing Visual Cryptography	August 2009	Ran-Zan Wang	0.0023	11.73dB
Visual cryptography for gray-level images by dithering techniques	2003	Chang-Chou Lin and Wen-Hsiang Tsai	0.00347	4.14dB
Visual cryptography for color images	August 2002.	Young-Chang Hou	0.00045	8.89dB
(2,n) secret sharing scheme for gray and color images based on Boolean operation	July2010	Lin Dong, DaoShun Wang, ShunDong	0.00087	33 to 41.1dB
Digital Image Sharing by Diverse Image Media	Jan 2014	Kai-Hui Lee & Pei-Ling Chiu	…… ……	19.74dB
Cheating prevention in visual cryptography using stenography scheme	2014	Biswapati Jana	…… ……	70 dB

5. SUMMARY OF DIFFERENT VISUAL CRYPTOGRAPHY TECHNIQUES.

Sr. No	*Year*	*Author*	*Schemes and methodology*	*Advantages*
1	1994	Moni Naor and Adi Shamir[9]	(k, n) Visual Cryptography Scheme by Boolean OR function	First visual cryptography scheme, secure and easy to implement.
2	1996	G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson[19]	General access structure scheme using forbidden and qualified shares	It is more secure than previous schemes and pixel expansion is reduced to log n.
3	1997	Verheul and Van Tilborg [20]	Colored visual cryptography scheme using arcs	First Visual cryptography technique performed on color images.
4	2002	Nakajima, M. and Yamaguchi, Y. [21]	Extended visual cryptography scheme for natural images	The shares generated are meaningful and improve the quality of output image.
5	2003	Chang -Chou Lin, Wen-Hsiang Tsai [22]	Visual Cryptography Scheme for Gray images by dithering technique	It inheriting any developed cryptographic technique for binary images and having less increase of image size as compared to others.
6	2006	Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo[23]	Halftone visual cryptography using void and cluster algorithm to encode a secret binary image into n halftone shares.	The visual quality obtained better than available method. It maintains good contrast and security and increases quality of the shares.
7	2007	Shyong Jian Shyua, et al [24]	Multiple secrets sharing scheme	The first true result that discusses sharing ability in visual cryptography of multiple secrets in two circle shares.
8	2008	Hsien-Chu Wu, Hao-Cheng Wang and Rui-Wen Yu[25]	Color visual cryptography scheme using halftone technique, secret coding table and cover coding table	It generates meaningful shares without increasing the security risks on the secret image. It is for color images.
9	2009	Wen-Pinn Fang[26]	Reversible visual secret sharing scheme using random grid method	Non-expansion visual secret sharing method with reversible property.

(*contd...Table*)

Sr. No	*Year*	*Author*	*Schemes and methodology*	*Advantages*
10	2011	Rezvan Dastanian and Hadi Shahriar Shahhoseini [27]	Multi Secret Sharing Scheme for Encrypting two Secret Images into two Shares using halftone technique	Two secret images are encrypted using this scheme hence storage capacity and bandwidth required is less.
11	2012	Somdip Dey[28]	Image is encrypted using three steps. It consists of hill cipher technique.	The inclusion of modified bits rotation and reversal technique, and modified Cyclic Bit Manipulation, made the system even stronger than it used to be before
12	2013	Manika Sharma, Rekha Saraswat[29]	New cryptographic technique in which shares are developed using Random number and color diffusion.	The quality of the decrypted image is improved
13	2013	Anupam Bhakta, Sandip Maity, Ramkrishna Das, Saurabh Dutta[30]	Variable length image key and bit sieve operation is used to encrypt image.	Multiple level of encryption is used thus the security is increased.

6. IMPLICATIONS

The result of the proposed explore work may have a few application in the field of picture processing, Secure confirmation and numerous increasingly and will affect security applications. Proposed technique will help in execution of this examination for picture preparing application.

- Authentication will be more secure in constant applications.
- Proposed Sterilization calculation can be utilized as a part of outlining devoted framework equipment.
- Proposed framework will help in security application outlining.
- Low PSNR and high MSE for Encrypted picture and High PSNR and low MSE for unscrambled picture can be useful for precision.

7. PROPOSED METHODOLOGY

1. The flow chart of the design process is as mentioned below.
2. Data Flow for Encryption:
3. Algorithm for Encryption:

Step 1: Select Image.

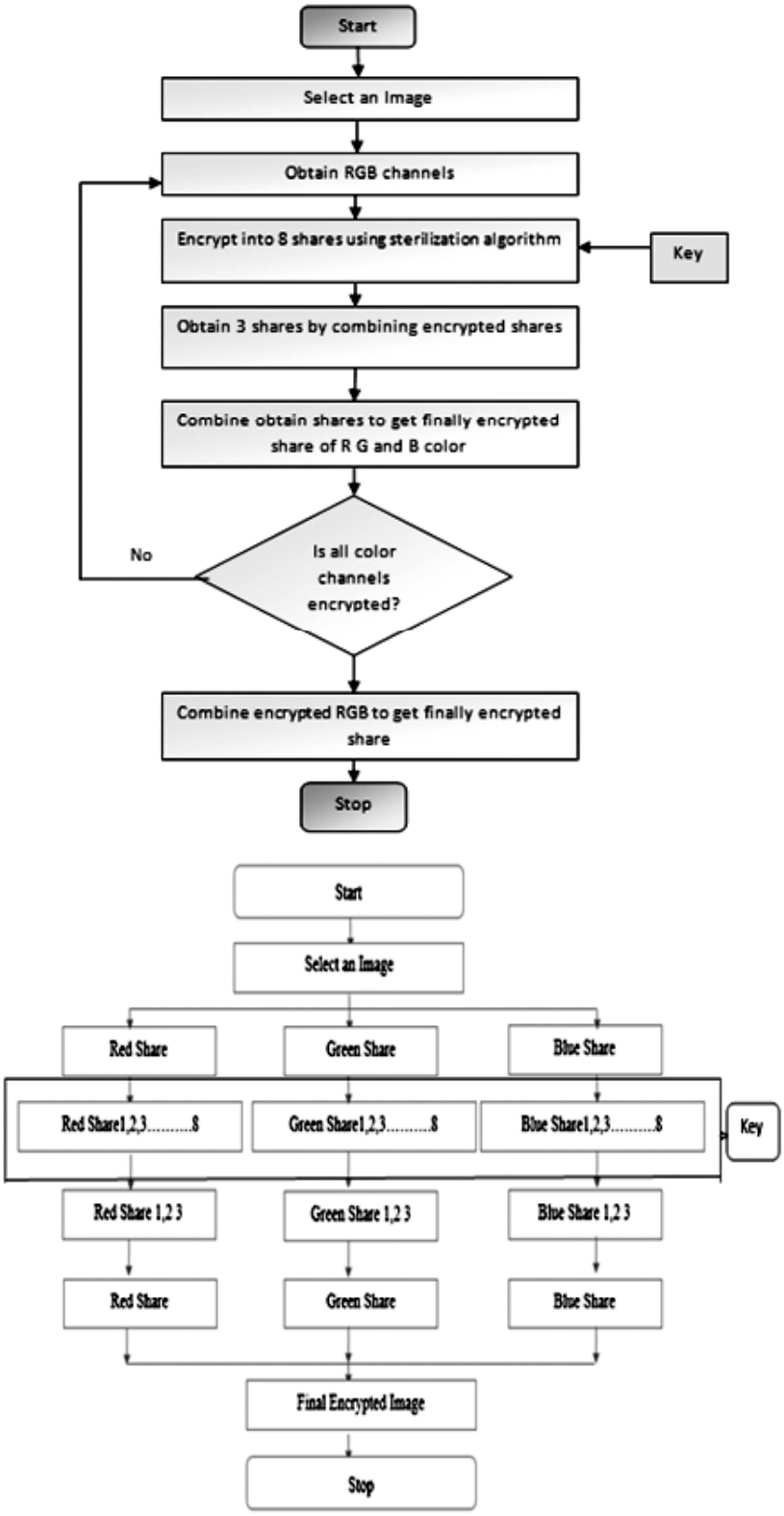
Step 2: Separate Red, Green and Blue Channels.

Step 3: R+G+B=8+8+8=24 shares. This encryption is done with the key provided by sterilization process.

Step 4: In this level 8 encrypted shares of each channel make group of 3, 3 and 2 shares.

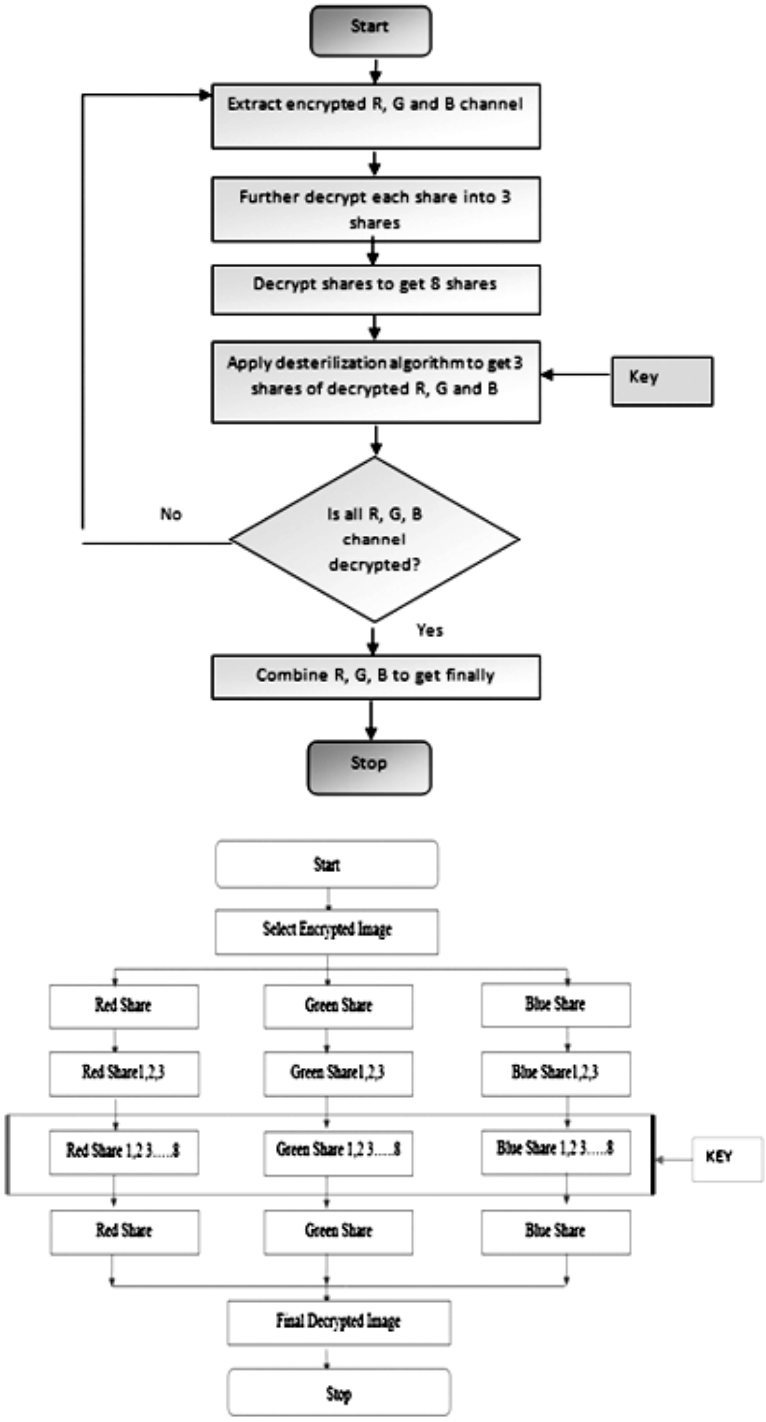
Step 5: 3 shares are obtained for each channel from previous step, using this share finally encrypted R, G, and B obtained. This operation is perform at level 3

Step 6: It checks the condition for encrypting all the 3 shares. Unless all the 3 shares are encrypted it process in loop.



Step 7: In this last level of encryption all the 3 share get combined and finally encrypted share obtained. Save the encrypted image to database.

4. Flow Chart for Decryption of Image:
5. Data Flow for Decryption:
6. Algorithm for Decryption



Step 1: Select encrypted pictured.

Step 2: Differentiate the shares.

Step 3: Further decrypt each R,G and B into 3 shares. I.e. R+G+B=3+3+3=9 shares.

Step 4: Decrypt each share into 8 shares, i.e. for decrypting red share split first share into 3 shares, second into 3 shares and third into 2 shares.

Step 5: By using the 8 shares of each color obtain single share in next step using desterilization algorithm.

Step 6: The condition has to be check that all color shares are decrypted or not, if all the shares decrypted then go for next process, otherwise set the process in loop.

Step 7: At this last stage of decryption combine all the decrypted Red, Green and blue share and finally decrypted image is going to be revealed.

7. Sterilization algorithm:

Step 1: Select share from level 0

Step 2: For Red process first 8 bits|| green process middle 8 bits|| blue process last 8bits

Step 3: For encrypting share

i. Create 8 blank shares.

ii. Apply 8-integer key to first pixel of share from left to right.

iii. Set bit value from step 0 to the blank share associated with key value.

iv. If bit value of share=1 then set blank share=255 else set blank share=0

v. If key=end then apply it in circular pattern to next pixel.

vi. Repeat step i to v for each pixel.

Step 4: Repeat step 2 and 3 for each share from step 1.

Step 5: stop

- Key Generation: - In this section, 8 integer key is generated. Here multiple keys are going to be generated as each pixel is encrypted using keys. Maximum number of keys provides more security as it required more prediction and complexity for decryption process to an intruder. Each pixel required three keys as each component is encrypted with different key. User can select any number of keys manually or randomly. If one want to remove keys then there is separate option provided for removal of selected keys. After selecting keys user have to save them.
- Bitwise Operation :

  Each Pixel is represented in binary format.

1. Red Channel Pixel – [213,0,0] - 11010101
2. Green Channel Pixel - [0,198,0] - 11000110
3. Blue Channel Pixel - [0,0,222] – 11011110

Implementation with example is as follows:

- Splitting image into Red, Green and blue channel.

  I = /(dI_R.dI_G.dI_B), Where R = Red, G = Green and B = Blue.

- Level 0:

$$dI_R = \frac{dI}{dR} = \text{Where G = B = 0}$$

$$dI_G = \frac{dI}{dG} \text{ Where R = B = 0}$$

$$dI_B = \frac{dI}{dB} = \text{Where R = G = 0}$$

Figure 1: Level 0

Each pixel is separated .For example first pixel value is [213 198 222]

- Level 1:
- For Red channel:

  Process 8 blank shares and set the first level encrypted shares by using key and sterilization algorithm.

$$dIL_{1R} = \frac{dI_1}{dz} + \frac{dI_2}{dz} + \frac{dI_3}{dz} + \cdots\cdots \frac{dI_8}{dz}$$

$$= \frac{1}{dz}\left(dI_1 + dI_2 + dI_3 \ldots\ldots dI_8\right)$$

Key: 48127536

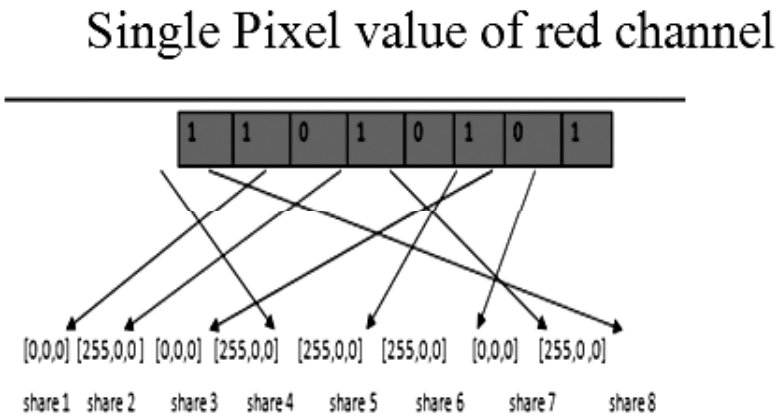


Figure 2: Sterilization for Red Channel

As key provided is 48127536 for red component of first pixel of image. As green and blue are zero hence only red component is process by using this key. Take first number from string of key it is 4 then set the blank share no.4,second number is 8 then 8th number share is set, Next key number is 1 then set 1st number share is set and so on. If bit number of original red component is 1 then set red component of particular blank share as 255, otherwise set it 0. Repeate this Procedure for red component of every pixel.

- For Green Channel:

Similar operation is going to perform on green channel. Create 8 blank shares. Here only green component is active hence key is provided to it.

$$dIL_{1G} = \frac{dI_9}{dz} + \frac{dI_{10}}{dz} + \frac{dI_{11}}{dz} + \ldots\ldots \frac{dI_{16}}{dz}$$

$$= \frac{1}{dz}\left(dI_9 + dI_{10} + dI_{11} \ldots\ldots dI_{16}\right)$$

Key: 75861324

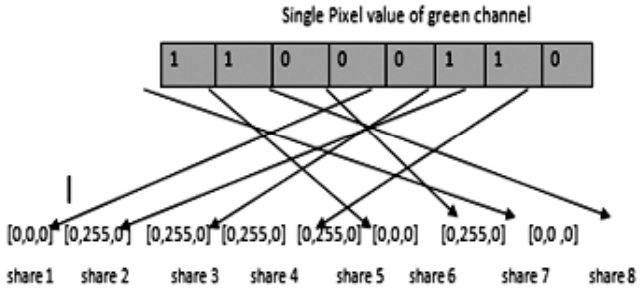


Figure 3: Sterilization for Green Channel

Here the operation perform is similar to that of encryption of red channel. Key provided for the pixel is 75861324.so set 7th share by using same technique. As next key number is 5 hence fifth number blank share is going to be set. Now green shares are going to create hence put R=B=0.and set only green bits. Repeat procedure for every pixel.

- For blue channel:

  Similar operation that is perform for red and green encryption is used here.

$$dIL_{1B} = \frac{dI_{17}}{dz} + \frac{dI_{18}}{dz} + \frac{dI_{19}}{dz} + \ldots\ldots \frac{dI_{24}}{dz}$$

$$= \frac{1}{dz}\left(dI_{17} + dI_{18} + dI_{19} \ldots\ldots dI_{24}\right)$$

Key: 84127536

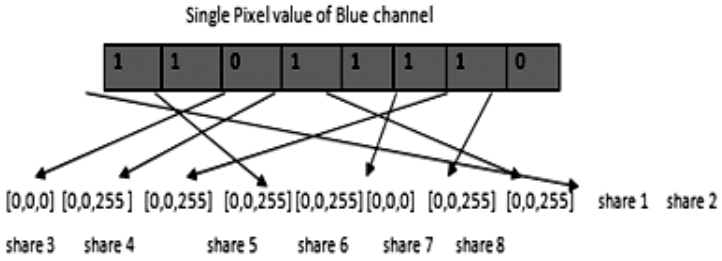


Figure 4: Sterilization for Blue Channel

The sterilization algorithm works on this blue channel is exactly similar to that of red and green channel. As first number in string of key is 8, hence eight number blank share is going to be set with respect to first bit of original blue component. As here R=G=0.So set the value of green share only. The shares obtained are store in database for further encryption.

- Level 2:

By using database from previous step at second level total 9 shares are obtained. Each red, green and blue component gives three shares. The result obtain from this step is going to be stored in database for

further encryption. Encrypted red shares are obtained as follows:

$$dIL_{21R} = \int_1^3 \left(dI_1 + dI_2 + dI_3 \right)$$

$$dIL_{22R} = \int_1^3 \left(dI_4 + dI_5 + dI_6 \right)$$

$$dIL_{23R} = \int_1^2 \left(dI_7 + dI_8 \right)$$

Encrypted green shares are obtained as follows

$$dIL_{21G} = \int_1^3 \left(dI_9 + dI_{10} + dI_{11} \right)$$

$$dIL_{22G} = \int_1^3 \left(dI_{12} + dI_{13} + dI_{14} \right)$$

$$dIL_{23G} = \int_1^2 \left(dI_{15} + dI_{16} \right)$$

Encrypted blue shares are obtained as follows:

$$dIL_{21B} = \int_1^3 \left(dI_{17} + dI_{18} + dI_{19} \right)$$

$$dIL_{22B} = \int_1^3 \left(dI_{20} + dI_{21} + dI_{22} \right)$$

$$dIL_{23B} = \int_1^2 \left(dI_{23} + dI_{24} \right)$$

- Level 3:

The database of previous shares is used to produce new encrypted shares. Previous red shares are combined to give encrypted red share, previous green shares are combined to give encrypted green share and blue shares from previous step are combining to give finally encrypted blue share. At this step finally encrypted red, green and blue channels are obtained which are as follows:

$$dIL_{3R} = \int_1^3 \left(dIL_{21R} + dIL_{22R} + dIL_{23R} \right)$$

$$dIL_{3G} = \int_1^3 \left(dIL_{21G} + dIL_{22G} + dIL_{23G} \right)$$

$$dIL_{3B} = \int_1^3 \left(dIL_{21B} + dIL_{22B} + dIL_{23B} \right)$$

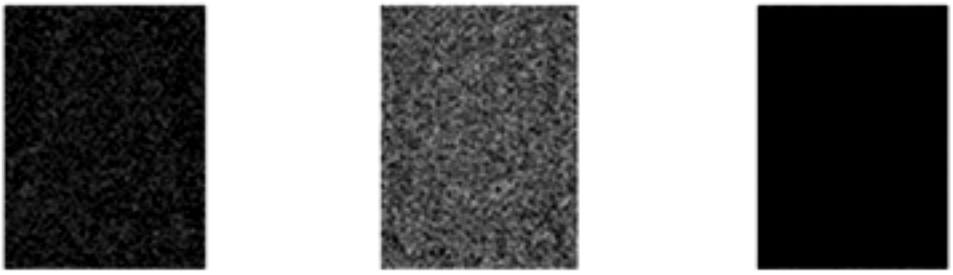


Figure 5: Encrypted Channels

- Level 4:

In this step all the encrypted channels from previous level combined to give finally encrypted share.

$$dIL_f = \int_1^3 \left(dIL_{3R} + dIL_{3G} + dIL_{3B} \right)$$

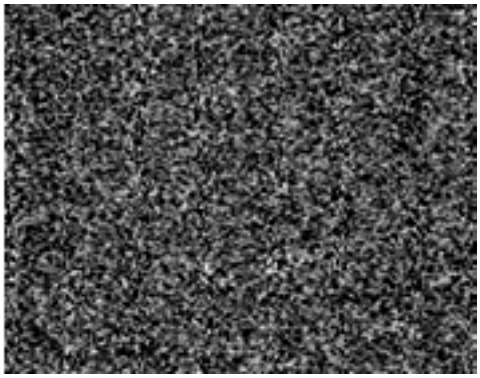


Figure 6: Finally Encrypted Share

8. IMPLEMENTATION OF DECRYPTION ALGORITHM

This module focuses on the implementation aspects of decryption. Following are the steps for the image decryption.

Step1: (Initialization Process): To perform decryption of an image the decryption menu has to be selected and load the image which has to be decrypted here

Step2: (Decryption at level 4): Separate encrypted channels from an encrypted input image.

Step3: (Decryption at level 3): At this step each Red, Green and Blue channel is decrypted to 3 shares. i.e. total 9 shares are obtained. i.e. R+G+B=3+3+3=9

Step4: (Decryption at level 2): From previous step, decrypted 8 shares will obtained from each red, green and blue channel. Here the key is provided to desterilized the process and get the decrypted shares. i.e. R+G+B=8+8+8=24

Step5: (Decryption at level 1): Combining shares from above step finally decrypted Red Green and Blue channels are obtained. These channels are original channel which has been encrypted during encryption. i.e. R+G+B=1+1+1=3

Step6: (Decryption at level 0): All the channels are combining to get the finally decrypted image.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," Advances in Cry ptology - EUROCRYPT'94, Springer-Verlag,1995, Vol-950, pp. 1-12.

[2] Himanshu Sharma , Neeraj Kumar, Govind Kumar Jha, "Enhancement of security in Visual Cryptography system using Cover Image share embedded security algorithm (CISEA)", 978-1-4577-1386-611©2011 IEEE, 2011, pp. 462-467.

[3] Zhongmin Wang and Gonzalo R. Arce, "Halftone visual cryptography through error diffusion", IEEE Transaction on Information Forensics and security, ISBN 1-4244-0481-9/06 © 2006 IEEE, pp. 109-112.

[4] J. K. Mandal and Subhankar Ghatak, "Constant Aspect Ratio based (2, 2) Visual Cryptography through Meaningful Shares (CARVCMS)". IEEE 1ST International conference on communication and Industrial application (ICCIA-2011 Paper ID 92), December 2011, pp. 01-04.

[5] Meera Kamath, Arpita Parab, "Extended Visual Cryptography for Color Images Using Coding Tables", 2012 International Conference on Communication, Information & Computing Technology (ICCICT), Mumbai, India 978-1-4577-2078-9/ 12 ©2011 IEEE. Vol. 4, Issue. 5, Oct 2011, pp. 39-46.

[6] Yanyan Han and Haocong Dong, "A Verifiable Visual Cryptography Scheme Based on XOR Algorithm", 978-1-4673-2101-3/12/$31.00 ©2012IEEE.

[7] Kulvinder Kaur and Vineeta Khemchandani "Securing Visual Cryptographic Shares using Public Key Encryption", 978-1-4673-4529-3/12/$31.00c 2012 IEEE.

[8] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multi-Secrets Visual Secret Sharing", Proceedings of APCC2008, IEICE, 2008, pp. 325–333

[9] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multi-Secrets Visual Secret Sharing", Proceedings of APCC2008, IEICE, 2008, pp. 325–333

[10] C. Yang and C. Laih, "New Colored Visual Secret Sharing Schemes", Designs, Codes and cryptography, Vol-20, Springer, 2000, pp. 325–331

[11] Du-Shiau Tsai, Gwoboa Horng, Tzung-Her Chen, Yao-TeHuang, "A Novel Secret Image Sharing Scheme For True-Color Images With Size Constraint", Information Sciences 179 3247–3254 Elsevier, 2009. pp. 122– 129.

[12] Pallavi Vijay Chavan, R.S. Mangrulkar "Encrypting Informative Color Image using Color Visual Cryptography", Third International Conference on Emerging Trends in Engineering and Technology, 978-0-7695-4246-1/10 $26.00 © 2010 IEEE DOI 10.1109/ICETET.2010.94, pp. 277-281.

[13] Roberto De Prisco and Alfredo De Santis, "Using Colors to Improve Visual Cryptography for Black and White Images," ICITS 2011, LNCS 6673, 2011, pp. 182-201.

[14] Meera Kamath, Arpita Parab, "Extended Visual Cryptography for Color Images Using Coding Tables", 2012 International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-20, Mumbai, India 978-1-4577-2078-9/12 ©2011 IEEE. pp. 189-195.

[15] Chun-Yuan Hsiao, Hao-Ji Wang, "Enhancing Image Quality in Visual Cryptography with Colors", 2012 IEEE, International Conference on Information Security and Intelligence Control (ISIC),2012, pp. 103–106.

[16] Yuanfeng Liu, Zhongmin Wang; "Halftone Visual Cryptography with Color Shares", IEEE International Conference on Granular Computing (GrC), ISBN 978-1-4673-2310-9, 2012, pp. 746-749.

[17] Shyong Jian Shyu, Hung-Wei Jiang; "General Constructions for Threshold Multiple-Secret Visual Cryptographic Schemes" IEEE Transactions on Information Forensics and Security, Volume: 8, Issue: 5, 2013, pp: 733 – 743.

[18] Young-Chang Hou, Shih-Chieh Wei, and Chia-Yin Lin; "Random-grid-based Visual Cryptography Schemes" IEEE Transactions on Circuits and Systems for Video Technology, Issue: 99, 2013, pp. 195-199.

[19] Shyong Jian Shyu,"Visual Cryptograms of Random Grids for General Access Structures" IEEE Transactions on Circuits and Systems for Video Technology, Volume: 23 , Issue: 3 2013,pp. 414 – 424.

[20] Pallavi Vijay Chavan , "Signature Based Authentication using Contrast Enhanced Hierarchical Visual Cryptography" 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science,2014, pp. 205-211.

[21] Xiang Wang, Qing qi Pei, Hui Li, "A Lossless Tagged Visual Cryptography Scheme" IEEE Signal Processing Letters, Vol. 21, NO. 7, July 2014, pp. 255-259.

[22] Ching-Nung Yang, "Property Analysis of XOR-Based Visual Cryptography" IEEE Transactions on Circuits And Systems For Video Technology, Vol. 24, No. 2, February 2014, pp. 189-197.

[23] Biswapati lana, "Cheating Prevention in Visual Cryptography using Steganographic Scheme" 2014 IEEE,Vol. 4(Issue 5), pp 1724-1729.

[24] Kai-Hui Lee and Pei-Ling Chiu, "Digital Image Sharing by Diverse Image Media" IEEE Transaction on Information Forensics and Security,Vol.9,No.1,Jan 2014,pp.88-98.

[25] Faraoun Kamel Mohamed, "A parallel block-based encryption schema for digital images using reversible cellular automata" Engineering Science and Technology, an International Journal , Elsevier, 5 May 2014, pp. 85- 94.