Implementation of Random Grid Visual Cryptography for Color Images

Snehal N. Meshram[1], Sneha U. Bohra[2]

[1]ME Scholar, Department of CSE, GHRCEM, Maharashtra, India

[2]Professor, Guide, Department of CSE, GHRCEM, Maharashtra, India

Abstract: ***Visual Cryptography is a special encryption technique that encrypts the secret image into n numbers of shares to hide information in images in such a way that it can be decrypted by the human visual system. It is imperceptible to reveal the secret information unless a certain number of shares (K) or more are superimposed. Simple Visual Cryptography is very insecure. Variable length key based Visual Cryptography for color image uses a variable length Symmetric key based Visual Cryptography scheme for color images where a secret key is used to encrypt the image and division of the encrypted image is done using Random Number. Unless the secret key is known, the original image will not be decrypted. Here secret key ensures the security of images. The proposed method introduces the concept of above scheme. Encryption process encrypts Original Image using variable length Symmetric key, gives encrypted image. Share generation process divides the encrypted images into n number of shares using random number. Decryption process stacks k number of shares out of n to reconstruct encrypted image and uses the same key for decryption.***

Keyword: Visual Cryptography (VS), Random Numbers, Secret Sharing, Symmetric key

1. Introduction

Visual cryptography is a cryptographic technique where visual information (Image, text, etc) gets encrypted in such a way that the decryption can be performed by the human visual system without aid of computers. Like other multimedia components, image sensed by human. Pixel is the smallest unit constructing a digital image. Each pixel of a 32 bit digital color image are divided into four parts, namely Alpha, Red, Green and Blue; each with 8 bits. Alpha part represents degree of transparency. Human visual system acts as an OR function. Two transparent objects stacked together, produce transparent object. But changing any of them to non-transparent, final objects will be seen non-transparent. In k-n secret sharing visual cryptography scheme an image is divided into n number of shares such that minimum k number of shares is sufficient to reconstruct the image. The division is done by Random Number generator. Visual Cryptography is a perfect way to provide the security for the confidential information. where binary pictures were considered in the encryption of pictures by two random grids. The encryption of a secret picture or shape into two random grids which are printed on transparencies such that the areas containing the secret information in the two grids are inter-correlated. Visual cryptography is based on cryptography where n images are encoded in a way that only the human visual system can decrypt the hidden message without any cryptographic computations when all shares are stacked together. Visual cryptography is a very secure and unique way to protect secrets.

Visual cryptography has two important features. The first feature is its perfect secrecy, and the second feature is its decryption method which requires neither complex decryption algorithms nor the aid of computers. Consider a binary secret image B and a set of n participants sharing B. A k out of n visual secret sharing scheme encrypts B into n transparencies (called shares) which are distributed to the n participants one by one in such a way that only when k or more shares are stacked together can the participants see B by their visual system; while any group of less than k shares obtains nothing about B. The additive and subtractive color models are widely used to describe the constitutions of colors. In the additive color model, the three primary colors are red, green, and blue (RGB), with desired colors being obtained by mixing different RGB channels. By controlling the intensity of red, green, blue channels, we can modulate the amount of red, green, blue in the compound light. The more the colors are mixed, the more the brightness of the light. When mixing all red, green and blue channels with equal intensity, white color will result. The computer screen is a good example of the additive color model. In the subtractive model, color is represented by applying the combination of colored-lights reflected from the surface of an object.

2. Related Work

In paper [1], Naor and Shamir: Proposed a serves as a basic model and has been applied to many applications. Aside from the obvious applications to information hiding, there are many applications of VC, which include general access structures, copyright protection, watermarking, visual authentication and identification, print and scan applications. In paper [2],Kafri and Keren: Proposed a similar technique, called random grid encryption, in 1987. Roughly speaking, the model proposed by Naor and Shamir. A secret image, known by a trusted party called the dealer, has to be shared among a set of participants in such a way that some subsets of participants, called qualified sets are able to visually recover the images while others, called forbidden sets, do not have any information about the secret image. In order to share the image, the dealer creates a share for each participant. In paper [3], Rijmen and Preneel : proposed a visual cryptography approach for color images. In their approach, each pixel of the color secret image is expanded into a 2×2 block to form two sharing images.

Licensed Under Creative Commons Attribution CC BY

Each 2×2 block on the sharing image is Elled with red, green, blue and white (transparent), respectively, and hence no clue about the secret image can be identified from any one of these two shares alone. In paper [4], Chang and Hou et al: proposed a binary encoding to represent the subpixels selected for each block and applied the AND/OR operation randomly to compute the binary code for the stacking subpixels of every block in the cover images. The code ranges from 0 to 255, but it can be even larger depending on the expanding factor. Consequently, a secret image can be a 256 color or true-color one. In paper [5], Y.C. Hou, C.Y. Chang, F. Lin: proposed the concepts of color decomposition and contrast adjustment to produce two shares needed by visual cryptography. Overlapping these two shares will reveal the secret information automatically. Although this method requires no mass computation to reconstruct secret images, it is nonetheless difficult to obtain totally random noise shares. Some image boundaries might be found on each share, thus compromising the secrecy required.

3. Proposed Algorithm

3.1 Implementation of Proposed System

The system is implemented in the form of three main modules. These modules are as follows:

1. Variable length key based encryption.
2. k-n Secret sharing visual cryptography scheme on the encrypted image
3. Decryption process

The description and working of each of these modules is as follows.

Module1: Variable length key based encryption

Description:- Any combination of characters [Characters, Numbers and Special Symbol] of any length is taken as KEY, which is XOR ed with the pixel array computed from the original image. This makes the image blur to some extent.

Working:- The working of the module is as follows:

- This module first reads input image from user.
- Create an array STORE of size w*h*24 to store the binary pixel values of the image using the loop
- Enter a key of any length from keyboard. Calculate the length (len) of the key. Convert the key into binary string let CONVERTED_KEY.
- Create an array KEY of size len*7 to store the binary values of the key by the following process.
- Calculate ITERATION = (w*h*24)/(len*7). KEY array is XOR ed with the STORE array.

Module 2: k-n Secret sharing visual cryptography scheme on the encrypted image

Description: This module is The encrypted image obtained from Section 3, number of shares it will be divided (n) and number of shares to be taken to reconstruct the encrypted image (k) are taken as input.

- Input the number of shares you want to create (n), suppose 3
- Number of shares required for reconstruction (k) is 2
- Calculate recons =(n-k)+1
- Predefine the n shares i.e 3 shares, size of shares equal to 24-bit encrypted image size(w*h*24)
- Process continues until total image is scanned
- Reconstruct each share to get size of share equal to original image size.

Module 3: Decryption Process

Description**:** The decryption process consists of into two steps. First step is done by human visual system where at least k number of shares out of n number of shares is superimposed, and the second step is decryption by the key taken in section 3. It is already discussed that human visual system acts as an EXOR function. For computer generated process; EXOR function can be used for the case of stacking k number of shares out of n.

- Input the number of shares you have = 3.
- Convert each share into 24-bit binary format.
- Bit or all the shares.
- Bit or 1 1 0 0 1 0
  0 1 0 1 0 0
  1 1 0 1 1 0
- Bit oring all the shares we get single reconstructed image.
- Enter the key and convert it into 7-bit binary format.
- XOR this key and 24-bit reconstructed image to get 24-bit decrypted image.
- Reconstruct 24-bit binary decrypted image to get decrypted image.

4. Experimental Results

This section briefly describes the result obtained when various types of images are provided as input to the proposed system. In this section, we evaluate the proposed system with three cases. The entire images are chosen from the data base. All the cases explained below, describes, the sample image and its corresponding workspace after the encryption, shares generation and decryption of the original image.

Case 1: Time taken for the image at the time of encryption, share generation and decryption process. The following table shows the character key entries from user and its time rate for encryption, share generation process, and decryption process.

Table 2.1: Images uses from the user and its time rate

Image no.	Type of image	Image size	key	No. Of shares generation	Execution time (sec) for encryption	Execution time (sec) for shares generation	Execution time (sec) for decryption
1	JPG	60*60	xyz	4	5.4170	2.8732	50.0469
2	JPG	40*40	are	6	0.8523	2.1528	16.6000
3	JPG	50*50	std	7	1.3508	2.8299	34.0117
4	JPG	40*40	pqr	2	2.0872	1.70288	14.6871
5	JPG	90*90	jajoo	3	15.2083	21.2118	43.8165
6	JPG	50*50	cat	4	21.2118	18.0871	7.9080
7	JPG	55*55	raja	4	12.2989	32.5660	85.119
8	JPG	90*90	jajoo	3	15.2083	21.2118	43.8165
9	JPG	50*50	cat	4	21.2118	18.0871	7.9080
10	JPG	42*42	baloo	3	24.6835	1.8962	45.8769
11	JPG	55*55	raja	4	12.2989	32.5660	85.119
12	JPG	50*50	abhi	4	15.2083	3.017	2.1568
13	JPG	42*42	baloo	3	24.6835	1.8962	45.8769
14	JPG	40*40	vishal	6	20.8795	1.1743	43.8165
15	JPG	40*40	neha	2	20.1978	1.5631	7.9080

Licensed Under Creative Commons Attribution CC BY

When the encryptions of the image are used as the key which is given from user, it is observed that time required for encryption process. By using encrypted image time required for the share generation process, and all so time for decryption process shown in above table.

Case 2: PSNR ratio image at the time of encryption, share generation and decryption process.

The following table shows the PSNR ratio of the encryption process, share generation process and decryption process. By using PSNR function calculate the signal to noise ratio of the image. When user enter the correct key and wrong key and calculate average ratio of the image.

Table 2.2: PSNR ratio of the image at the time of correct key and wrong key

Sr No.	Image Size	Key at the time of Encryption	Correct Key at the time of Decryption	PSNR For Red	PSNR For Green	PSNR For Blue	Wrong key at the time of Decryption	PSNR For Red	PSNR For Green	PSNR For Blue
1	50*50	Snehal	Snehal	0	0	0	sneha	10.2986	9.3593	8.2629
2	40*40	Akhir	Akhir	0	0	0	akhi	11.7179	14.8000	9.7179
3	50*50	Ashwini	Ashwini	0	0	0	ashwi	18.8984	7.94281	18.8984
4	40*40	Nishant	Nishant	0	0	0	nihant	10.3821	8.06112	12.3721
5	60*60	Anjali	Anjali	0	0	0	anali	11.6441	13.1932	11.6441
6	70*70	Rina	Rina	0	0	0	rin	10.8752	9.4509	10.8052
7	80*80	Riya	Riya	0	0	0	ria	10.8230	10.8000	7.94281
8	90*90	Jajoo	Jajoo	0	0	0	jaoo	7.9421	7.94281	8.06112
9	50*50	Cat	Cat	0	0	0	at	4.06112	5.06112	8.19320
10	45*45	Will	Will	0	0	0	wll	6.19320	8.19320	9.4509
11	55*55	Raja	Raja	0	0	0	raj	10.4509	9.4509	18.234
12	40*40	Ravi	Ravi	0	0	0	rvi	19.7863	10.4656	11.1231
13	42*42	Baloo	Baloo	0	0	0	blo	8.8013	9.97391	9.7179
14	40*40	Vishal	Vishal	0	0	0	vish	9.6603	12.1990	18.8984
15	40*40	Neha	Neha	0	0	0	eha	11.5567	11.0032	12.3721

By using correct key and wrong key calculate the PSNR ratio. when the correct key enter from user psnr ratio is produced some noise on the image, but when correct key enter at the time of decryption process the psnr ratio is calculate is 0. That is the psnr ratio is small at the time of correct key used.

Following process shows the workspace of PSNR ratio for the red, green and blue frame. At the time of Decryption process.

Case 3: Percentages of accuracy image at the time decryption process. The following table shows 2.3 the total no. percentages for encryption, share generation, decryption process. Table shows that the accuracy of image at the time of user enter correct key.

Table 2.3: Total number of accuracy in percentage of image

Sr. No.	Image Size	Key at the time of Encryption	Key at the time of Decryption	Percentages of accuracy for decrypted image
1	50*50	snehal	Snehal	92.26
2	40*40	akhir	Akhir	89.96
3	50*50	ashwini	Ashwini	69.04
4	40*40	nishant	Nishant	77.94
5	60*60	anjali	Anjali	91.67
6	70*70	rina	Rina	98.60
7	80*80	riya	Riya	51.92
8	90*90	jajoo	Jajoo	81.50
9	50*50	cat	Cat	71.68
10	45*45	will	Will	65.00
11	55*55	raja	Raja	89.21
12	40*40	ravi	Ravi	55.25
13	42*42	baloo	Baloo	90.81
14	40*40	vishal	Vishal	93.25
15	40*40	neha	Neha	69.71
16	30*30	rita	Rita	78.67
17	50*50	abhi	Abhi	66.04
18	40*40	sonu	Sonu	88.25
19	40*40	kitti	Kitti	98.69
20	50*50	rushu	Rushu	66.60
21	40*40	naru	Naru	50.67
22	40*40	ujawala	Ujawala	70.92
23	40*40	sushil	Sushil	80.50
24	50*50	harshu	Harshu	61.68
25	60*60	alka	Alka	94.94

When the correct key enter for the encryption process form user it is observed that the accuracy is of 85.12%.

5. Comparative Analysis of the Result

This chapter describes the comparative analysis of the observed result of the proposed system with the system studied in the literature review. This chapter is divided into two sections Results obtained from proposed system and its comparison with result of the reviewed system.

5.1 Analysis of the Result Obtained by the Proposed System

This section describes the result obtained from the proposed methodology. The following table 5.1 shows the number of correct keys and wrong keys used at the time of decryption process recognized the accuracy of the images.

Table 5.1: Table of the accuracy of the images at the time of decryption process

Sr. No.	Image Size	Key at the time of Encryption	Key at the time of Decryption	Percentages of accuracy for decrypted image
1	50*50	snehal	Snehal	92.26
2	40*40	akhir	Akhir	89.96
3	50*50	ashwini	Ashwini	69.04
4	40*40	nishant	Nishant	77.94
5	60*60	anjali	Anjali	91.67
6	70*70	rina	Rina	98.60
7	80*80	riya	Riya	51.92
8	90*90	jajoo	Jajoo	81.50
9	50*50	cat	Cat	71.68
10	45*45	will	Will	65.00
11	55*55	raja	Raja	89.21
12	40*40	ravi	Ravi	55.25
13	42*42	baloo	Baloo	90.81
14	40*40	vishal	Vishal	93.25
15	40*40	neha	Neha	69.71
16	30*30	rita	Rita	78.67
17	50*50	abhi	Abhi	66.04
18	40*40	sonu	Sonu	88.25
19	40*40	kitti	Kitti	98.69
20	50*50	rushu	Rushu	66.60
21	40*40	naru	Naru	50.67
22	40*40	ujawala	Ujawala	70.92
23	40*40	sushil	Sushil	80.50
24	50*50	harshu	Harshu	61.68
25	60*60	alka	Alka	94.94

From the above table, it can be commented that overall accuracy of recognition of the image is found to be 85.12%

Licensed Under Creative Commons Attribution CC BY

The following table 5.2 shows the number of sample images with different keys and different image sizes used for the existing system. Table 5.1 and 5.2 shows the comparison between existing system and proposed system.

Table 5.2: Table for images accuracy of existing system

Sr. No.	Image Size	Key at the time of Encryption	Key at the time of Decryption	Percentage of accuracy for decrypted image
1	50*50	snehal	snehal	80.21
2	40*40	akhir	akhir	78.22
3	50*50	ashwini	ashwini	50.21
4	40*40	nishant	nishant	45.33
5	60*60	anjali	anjali	61.22
6	70*70	rina	rina	54.55
7	80*80	riya	riya	61.33
8	90*90	jajoo	jajoo	60.23
9	50*50	cat	cat	68.00
10	45*45	will	will	51.00
11	55*55	raja	raja	79.32
12	40*40	ravi	ravi	62.45
13	42*42	baloo	baloo	71.41
14	40*40	vishal	vishal	81.22
15	40*40	neha	neha	54.21
16	30*30	rita	rita	68.33
17	50*50	abhi	abhi	56.11
18	40*40	sonu	sonu	78.33
19	40*40	kitti	kitti	89.22
20	50*50	rushu	rushu	76.44
21	40*40	naru	naru	41.78
22	40*40	ujawala	ujawala	64.12
23	40*40	sushil	sushil	70.21
24	50*50	harshu	harshu	57.33
25	60*60	alka	alka	87.00

From the above table, it can be commented that overall image accuracy of images found to be 81.27%. The overall accuracy of the proposed system is found to be 85.12 %. The following figure 5.3 shows the graphical representation of the accuracy of images with respective images size and correct key used for decryption process.

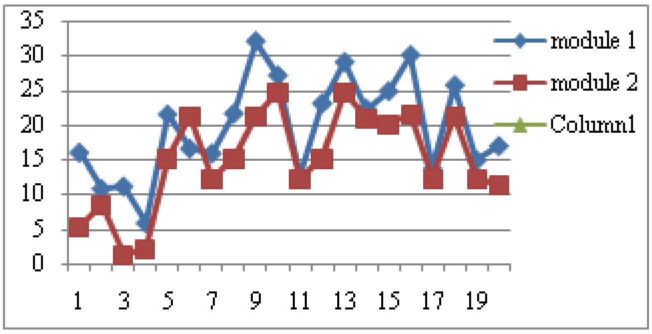

Figure 5.3: Graphical representation of accuracy of images

The following table 5.4 shows the comparison of existing system and proposed system with respective time. Time required for the encryption process, shares generation process and decryption process.

Table 5.4: Comparison of existing system and proposed system

Execution time (sec) for encryption		Execution time (sec) for shares generation		Execution time (sec) for decryption	
Existing System	Proposed System	Existing System	Proposed System	Existing System	Proposed System
16.0203	5.4170	4.7624	2.8732	23.6731	20.0469
10.8650	08.523	5.2341	2.1528	20.1274	16.6000
11.2121	1.3508	2.9899	2.8299	44.8165	24.0117
5.9080	2.0872	2.4537	1.70288	21.6754	14.6871
21.5530	15.2083	28.9675	21.2118	25.5673	23.8165
16.6006	21.2118	20.1323	18.0871	10.1567	7.9080
15.8932	12.2989	33.1256	32.5660	70.2317	81.119
21.6754	15.2083	22.1546	21.2118	44.2167	43.8165
32.1234	21.2118	24.8654	18.0871	12.8745	7.9080
27.1987	24.6835	6.1234	1.8962	46.1324	45.8769
12.4789	12.2989	36.1261	32.5660	89.1234	85.119
23.1298	15.2083	06.8965	03.0178	4.8345	2.1568
29.1065	24.6835	2.6543	1.8962	47.4189	45.8769
22.3510	20.8795	2.6754	1.1743	50.1640	43.8165
24.8976	20.1978	2.7423	1.5631	11.3025	7.9080
30.1294	21.5530	3.1425	1.1422	14.2567	11.9352
13.6754	12.3095	2.5423	1.48661	15.2369	13.6836
25.7653	21.2118	3.4567	2.0848	16.3456	11.1578
14.8974	12.3095	3.7614	1.48661	15.3467	13.6836
16.9785	11.4325	4.7351	2.27645	25.6784	23.0272
12.6758	11.3979	2.4782	0.97380	10.3567	9.95186
20.1567	19.0392	3.2745	2.22100	10.4567	7.8899

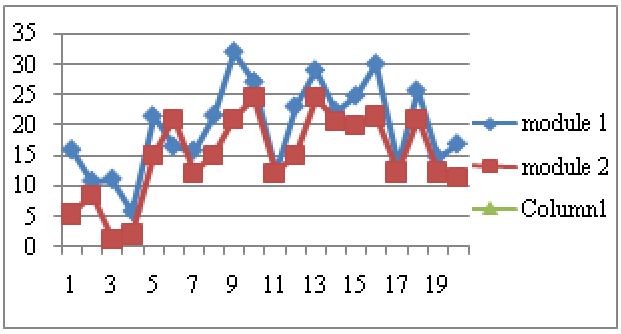

Figure 5.5: Graphical representation for Time required of the encryption process

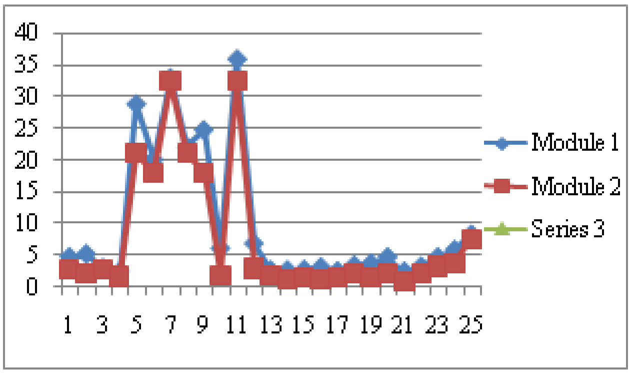

Figure 5.6: Graphical representation for Time required of the share generation process

Licensed Under Creative Commons Attribution CC BY

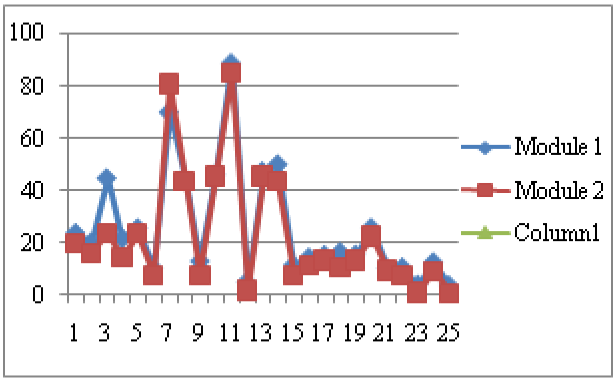

Figure 5.7: Graphical representation for Time required of the decryption process

The following table shows the comparison for PSNR ratio of existing system and proposed system. Psnr ratio for red, green and blue frame. Psnr ratio with respective of correct key enter at the time of decryption process. And wrong key enter at the time of decryption process. psnr ratio shows that the when user enter wrong key red, green, and blue frame produce lot of noise on image. Generated psnr ratios for all images shown in following table.

Table 7.8: comparison of psnr ratio for existing system and proposed system

PSNR ratio for red frame		PSNR ratio for green frame		PSNR ratio for blue frame	
Existing system	Proposed system	Existing system	Proposed system	Existing system	Proposed system
8.2310	10.2986	7.2345	9.3593	7.2569	8.2629
10.2673	11.7179	12.6724	14.8000	6.2367	9.7179
12.4526	18.8984	5.4261	7.94281	15.2456	18.8984
8.3527	10.3821	7.3526	8.06112	10.3567	12.3721
10.2894	11.6441	11.1740	13.1932	6.3562	11.6441
7.2633	10.8752	5.2754	9.4509	9.3567	10.8052
8.2087	10.8230	8.3725	10.8000	5.1562	7.94281
5.2461	7.9421	6.1345	7.94281	6.2784	8.06112
2.1768	4.06112	3.1673	5.06112	6.2436	8.19320
5.2967	6.19320	6.2343	8.19320	5.2567	9.4509
8.1452	10.4509	6.2783	9.4509	15.2678	18.234
15.2745	19.7863	5.3782	10.4656	10.3678	11.1231
6.1245	8.8013	6.1673	9.97391	8.2678	9.7179
6.2561	9.6603	10.2845	12.1990	16.2679	18.8984
10.2476	11.5567	10.2745	11.0032	10.1456	12.3721
12.3658	14.1501	5.2867	7.7744	9.2678	11.6441
9.2845	10.8000	9.1026	10.8174	9.1547	10.8052
5.2783	7.94281	5.2846	8.2875	6.2849	7.2005
6.2768	8.06112	5.3892	7.1627	5.2894	7.3031
6.2638	8.19320	9.3725	11.2204	10.3482	11.6263

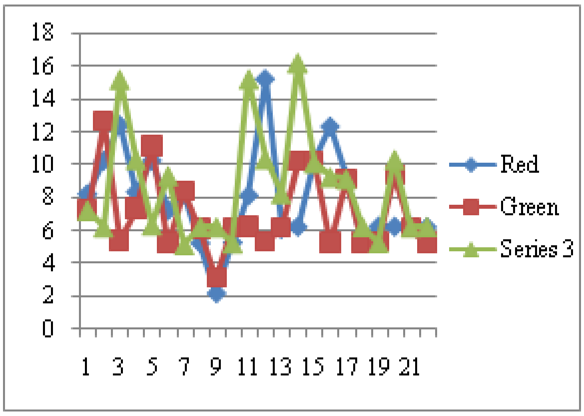

Figure 5.9: Graphical representation of PSNR for Existing system

6. Conclusion

In the "Implementation of Random Grid Visual Cryptography for Color Images", we proposed a technique of well known k-n secret sharing on color images using a variable length key with share division using random number. As we know Decryption part of visual cryptography is based on XOR operation, so if a person gets sufficient k number of shares. The image can be easily decrypted. Key adds robustness to the visual cryptography techniques and variable length of the key makes it more secure. At the time of dividing an image into n number of shares we have used random number generator, which is a new technique not available till date. This technique needs very less mathematical calculation compare with other existing techniques of visual cryptography on color images. This technique only checks "1" at the bit position and divide that "1" into (n-k+1) shares using random numbers.

References

[1] Roberto De Prisco and Alfredo De Santis," On the Relation of Random Grid and Deterministic Visual Cryptography "IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 4, APRIL 2014.

[2] R. De Prisco and A. De Santis," On the Relation of Random Grid, Probabilistic and Deterministic Visual Cryptography", December 4, 2013.

[3] Pratiksha P.Patil, Y.M. Patil," Visual Cryptography Based on Halftoning ",*IOSR Journal of Electronics and Communication Engineering*,

[4] Hsien-Chu Wu1, Hao-Cheng Wang, and Rui-Wen Yu," Color Visual Cryptography Scheme Using Meaningful Shares ", February 24,2010.

[5] Sachin Kumar and R. K. Sharma," Improving Contrast in Random Grids Based Visual Secret Sharing ", International Journal of Security and Its Applications Vol. 6, No. 1, January, 2012.

[6] Tzung-Her Chen and Kai-Hsiang Tsao," User-Friendly Random-Grid-Based Visual Secret Sharing ", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 21, NO. 11, NOVEMBER 2011

[7] Kai-Hui Lee and Pei-Ling Chiu,"An Extended Visual Cryptography Algorithm for General Access Structures", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 1, FEBRUARY 2012.

[8] Young-Chang Hou, Shih-Chieh Wei, and Chia-Yin Lin," Random-grid-based Visual Cryptography Schemes", 2013

[9] G.Deepa "The Comparative Study on Visual Cryptography and Random Grid Cryptography ", *IOSR Journal of Computer Engineering, Volume 12, Issue 2 May. - Jun.2011*

Licensed Under Creative Commons Attribution CC BY