International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 5, Issue 5 (May 2016), PP.07-14

Visual Cryptography Scheme with Authentication Using Shamir Andmk Reddy Techniques

Neha K. Lakde [1], Prof. P. B. Shelke [2]
[1](P. G . Scholar, Dept Of Computer Science And Engg, Plitms, Buldana, India)
[2](Professor , Hod Of Electrical E & P Engg, Plitms, Buldana, India)

Abstract:- In our daily life Information is increasingly important. Information gets more value when shared with others. Due to advances in technologies related to networking and communication, it is possible to share the information like audio, video and image easily. There are lots of security related issues. Hacker's may try to access unauthorized data and misuse it. Various techinques are required to solve this problem. Techniques to provide security, while sharing information are termed as Secret sharing schemes. When it comes to visual information like image and video, it is termed as Visual secret sharing scheme. Visual cryptography (VC) is a technique used for protecting image-based secrets.This paper presents a detail survey of different visual cryptography scheme used for visual cryptography . The basic concept of visual cryptography scheme is, to split secret image into some shares, which separately reveals no knowledge about the secret information. Shares are then distributed to participants. By stacking these shares directly, secret information can be revealed and visually recognized. All shares are necessary to combine to reveal the secret image. In this paper we have introduced a technique for visual cryptography in which
any type of image can be chosen as a passward, images then divided and then apply Shamir and M K Reddy encryption and decryption techniques . After decryption system get match with original image then system give result as the user is authenticate otherwise non authenticate. The system introduced in this paper satisfy the needs of authentication.

Keywords:- Visual Cryptography , Visual Secret Sharing Scheme

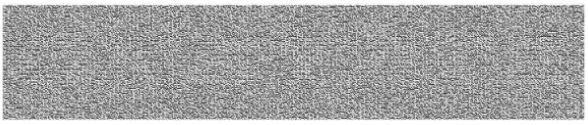
I. INTRODUCTION

Nowadays, information gets more value when shared with others. Due to internet, it is possible to share information like audio, video, images easily .There are security related issues. Hacker’s access unauthorized data. Various techniques can be used to solve this problem. Today, in computer-aided environment sharing visual secrets images has becomes an important issue today. The secret images can be various types such as handwritten documents, photographs and others. Naor and Shamir [1] proposed the concept of Visual cryptography (VC) which allows the encryption of secret information in the image form. Visual cryptography is a technique that encrypts a secret image into n shares with each participant holding one or more shares. By using the concept of visual cryptography, a secret image was broken up into some shares and then distributed to the n participants. By stacking their n shares, the secret information can be revealed and visually recognized by human visual system. There has been a steadily growing interest in visual cryptography. Visual cryptography is simple, secure, effective cryptographic scheme and very easy to implement.G.R. Blakley and Adi Shamir independently invented secret sharing scheme in 1979[1, 2]. When it comes to visual information like image and video, it is termed as Visual secret sharing scheme.

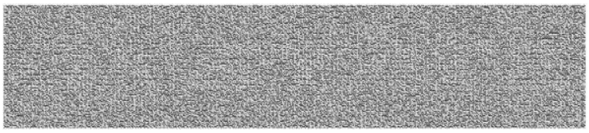
The outlined of this paper is as follows : Section 2. Describes How Visual Cryptography Works , Section 3 Describes Modules , Section 4 : Results and Discussions , Section 5 : Comparative Analysis, Section 6 : Conclusion, Section 7: Future work, Section 8 contains Acknowledgement , Section 9: References .

II. HOW VISUAL CRYPTOGRAPHY WORKS

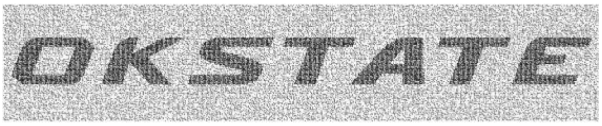
Each pixel of the image is divided into smaller blocks and always has the same number of black and white (transparent) blocks. For example if a pixel is divided into two parts (2 subpixels), there will be one white and one black blocks. Similarly if the same pixel is divided intofour equal parts (4 subpixels), there will be two white and two black blocks. Here is a simple example that explains the idea of how visual cryptography works.



Share 1



Share 2



Overlay (Share 1 + Share 2)

Fig.1. Example to show how VC works

From Fig.1 we can observe that the original image is broken up into two parts which are its shares. Separately these shares look like random noise but when combining reveals animage. Every single pixel is split into subpixels andthe humanvision still perceives them as one pixel.

III. MODULES

The work can be divided into the following modules,
3.1 Collection of image dataset
3.2 Development of encryption technique
3.3 Development of decryption algorithm
3.4 System integration for authentication application

3.1 Collection Of Image Dataset

In this system, the implementation of Visual Cryptography is done. In visual Cryptography we require image as the key or we can say the accessing password. Since the passwords are graphical. We need image as an input. In this case the images can be selected from any of the local drive may it be the internal memory or external memory. The file will be uploaded in the system for processing.

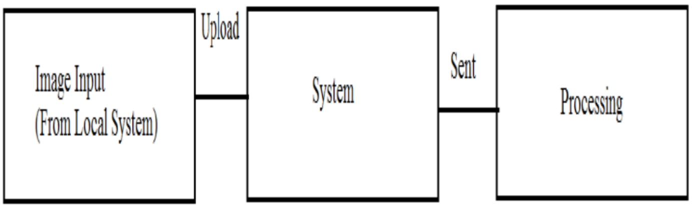


Fig. 2. Representation of how selection of image is done

The above fig. 2 shows the image is selected which is to be keep as the key and the system uploads the file and sends it for further processing. The other sections gives how this image is going to get processed.

3.2 Development of Encryption Technique

In this system two of the important techniques are used one of which is the Shamir encryption and the second one is the M K Reddy encryption, both of the techniques are explained as follows:

3.2.1 Shamir:

This Scheme divides a secret data, in this case the image into "n" number of shares Such as S_1, S_2 … S_n. the knowledge of k or more shares among S_i (where I <= n) can reveal the secret information. In this system the "i" is majorly 3. If the receiver gets 3 of the correct and important pieces then the traction can be done. If the knowledge of less than k shares reveals no information about the data. Therefore if the system doesn't present a good pain then the information is not disclosed.

This technique is also termed as k n secret sharing it comes from the concept that k points are necessary to define a polynomial of degree (k−1). Now to construct a polynomial coefficients a_1, a_2 … $a_{k-1}$are required, constant a0 is always S, which is the secret data. The polynomial $f(x)= a0 + a1x +a_2x^2 + . . . + a_{k-1}x^{k-1}$. The equation is always constructed from the coefficients. The total n points from 0 to n are taken and corresponding f(x) are also calculated. From these values a large number of pairs are created and the original coefficients are retrieved by interpolation method from at least k number of pairs.

3.2.2 M K Reddy:

It is also an encryption scheme which encrypts the secret image into two shares and obtains the secret image when two shares are superimposed. It relies

upon breaking of pixels into sub pixels, in other words we can say expansion of pixels. The scheme not only relies on 2 , n scheme but n , n scheme therefore this scheme can encrypts the secret image into n shares and obtains the secret image when all n of the shares are overlaid, but any n -1 of them will not produce any hint about the secret image. The user has to give the value of n, the number of participants. In this proposed system we can generate three shares from three secret images using basic (2, 2) scheme.

3.3 Development of Decryption algorithm

In this stage of the system, the decryption is needed to for the authentication. The decryption of both the techniques is explained as follows:

3.3.1. Shamir's Decryption:

For decryption only main thing is the cipher text, or in this case the image sequence then any Human visual system can encrypt. It is already discussed that Human Visual system acts as an OR function. It is also mentioned that decryption in Visual cryptography is done by stacking k number of shares out of n shares generated. For computer generated decryption process we have used OR operation. The algorithm is described below. Step I: Take s number of shares (s ≥ k) out of n number of shares generated. Step II: Select the k i. e authentication parts of each share, where 1 j w*h, to produce the final image.}

3.3.2. M K Reddy Decryption:

Let us consider two shares with the pixel positions as shown in figure above. Each share consists of a number of rows depending upon the secret image. For the first row of two shares do the following process. The first pixel (1') in the first share is overlapped with the last pixel of second share (3") and the second pixel (2") in the first share is overlapped with the last but one pixel (4") of second share and so on. The same is repeated for the remaining rows of two shares. This process is called superimposition of one share with the 180 degrees anticlockwise rotation of another share.

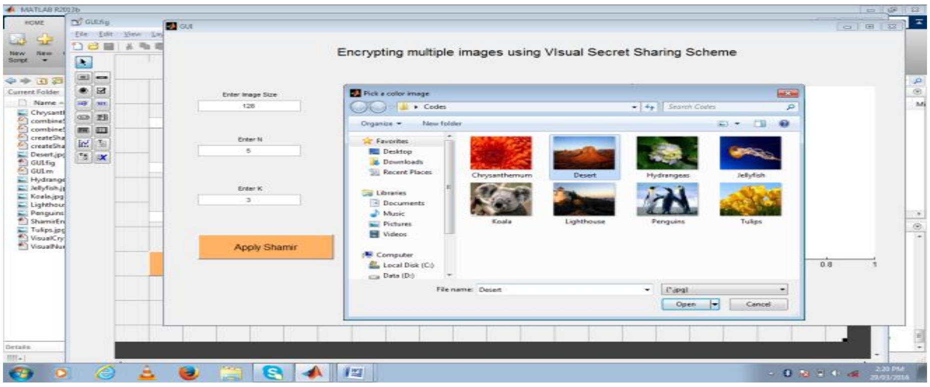
3.4 System integration for authentication application

In this system we have to combine all the module to complete the system to use the system. so that we combine module 1st off all image dataset , then encryption technique and decryption algorithm of the shamir as well as MK Reddy.

IV. RESULTS AND DISCUSSIONS

4.1 Results Of Shamir

In this section we are going to see some of the important results of the system implemented. The screenshots of the system are as follows:



Encrypting multiple images using VIsual Secret Sharing Scheme

Enter Image Size: 128

Enter N: 5

Enter K: 3

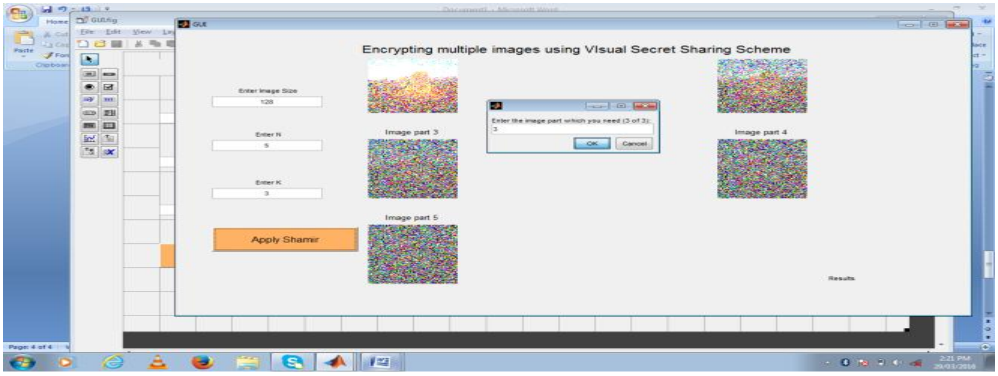
Pick a color image

File name: Desert

(*.jpg)

Fig. 3. Screenshot of Addition of Image

The above fig. 3 shows the adding of the image to the system to test the functionality of the system.



Encrypting multiple images using VIsual Secret Sharing Scheme

Enter Image Size: 128

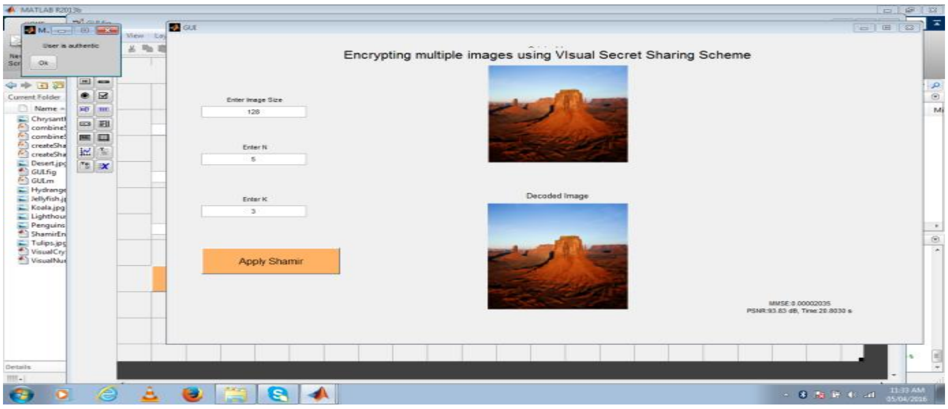
Enter N: 5

Enter K: 3

Enter the image part which you need (3 of 3): 3

Fig .4. Screenshot Dividing Original Image Into 5 Parts

In the above fig. 4, we can observe that after applying Shamir the image is divided into five parts that is N. from this we need only 3 important parts to rebuilt them which is K. in the figure the image inputted is encrypted and divided into five parts from which three parts are important and can rebuilt the whole image. If the rebuilt is possible then the authentication is successful.



User is authentic

Encrypting multiple images using VIsual Secret Sharing Scheme

Enter Image Size: 128

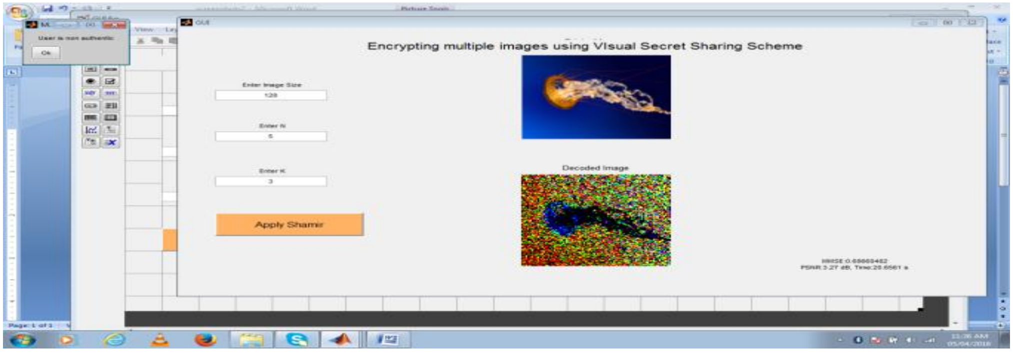
Enter N: 5

Enter K: 3

MMSE:0.00002035
PSNR:93.83 dB, Time:20.8030 s

Fig. 5. Screenshot Of Result For Authenticate Result

The above fig. 5. shows the application of the Shamir. As observed from the image the left hand side contains the Shamir’s technique, where the image size, N and K are entered and a button is provided to apply in the mid-section is the graphical image which is to be used by the system and in the right hand side we have MMSE and PSNR value calculated. Here the image is of size 128 bits and the N is 5 and the K is 3. The MMSE value calculated is 0.00002035 and the PSNR is 93083dB and the time required for the procedure is 20.8030 seconds.



User is non authentic

Encrypting multiple images using VIsual Secret Sharing Scheme

Enter Image Size: 128

Enter N: 5

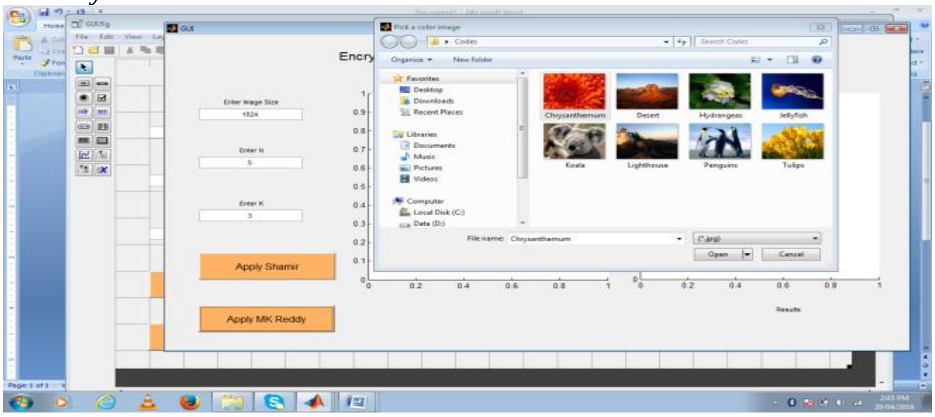
Enter K: 3

MMSE:0.68660482
PSNR:3.27 dB, Time:20.6561 s

Fig. 6. Screenshot Of Result For Non Authenticate User

In the above Fig. 6. we can see the decoded image of the system. In this case the image inputted is of 128 bit and the N and K are 5 and 3 respectively. Here when the image is sent at the receiving end the image takes which is received and will create an image to verify by the user like a puzzle. Here the MMSE value is 0.68660482, PSNR is 3.27dB and time required is approximately 20 seconds.

4.2 Results Of M K Reddy



Enter Image Size: 1024

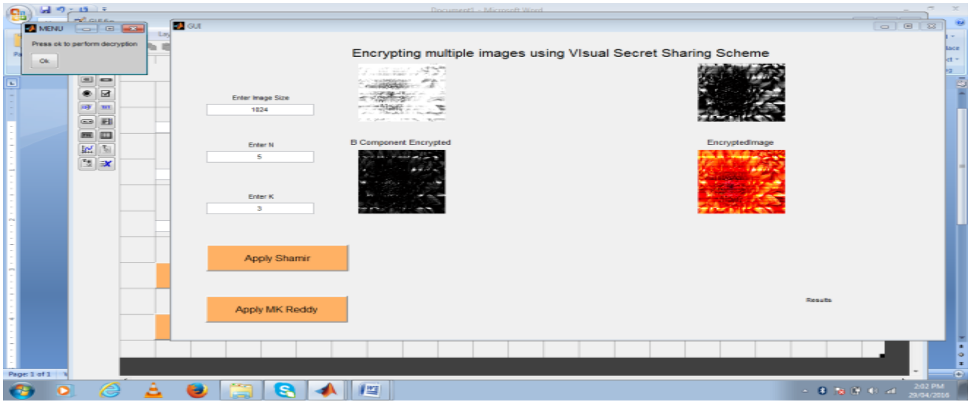
Enter N: 5

Enter K: 3

File name: Chrysanthemum

Fig : 7. Screenshot of Addition of Image

The fig . 7 shows the adding of the image to the system to test the functionality of the system. by applying M K Reddy algorithum.



Press ok to perform decryption

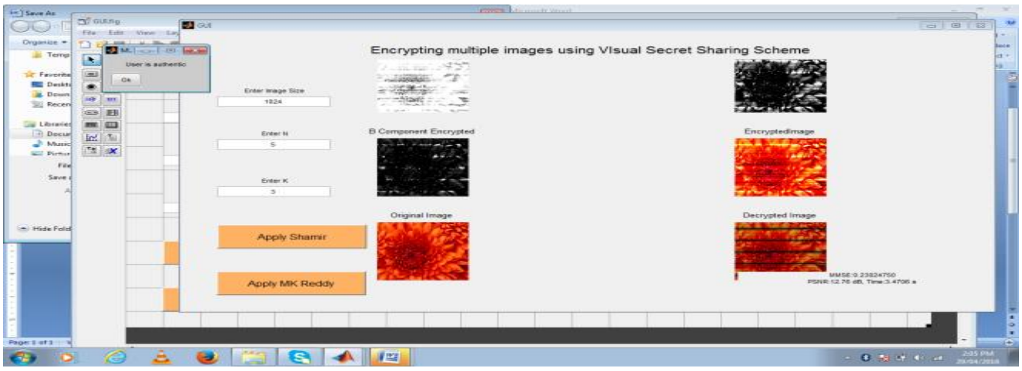
Enter Image Size: 1024

Enter N: 5

Enter K: 3

Fig . 8. Encrypting The Original Image

In the above fig . 8, we can observe that after applying MK Reddy the image is divided into 3 parts always that is N. from this 3 parts it encrypt the original image . ater pressing “ok” button in the system we get the decrypted image in which horizontal lines are appers are shown in fig. to adding horizontal lines in image is the property of MK Reddy algorithum. This is drawback of MK Reddy algorithum. Still it gives output as the user is authenticate.



User is authentic

Enter Image Size: 1024

Enter N: 5

Enter K: 3

MMSE:0.23824750

PSNR:12.76 dB, Time:3.4706 s

Fig . 9. Screenshot Of Final Result Of MK Reddy

In the above fig. 9 we can see the decoded image of the system. In this case the image inputted is of 1024 bit . But decoded image is not proper. So we can say that it is lossy algorithum. And here psnr is very low 11.58 so algorithum is insecure and time is 3.58 here time is very less because it divides the image into only 3 parts .The bellow table 1 shows the PSNR value and time required by the images. As observed from the table we have image sizes from 64 to 1028 bits and the time rages from 6 to 1328 seconds. When the 64 bit image is taken when K is 2 the time required by the system is 6.66 seconds and the time required by K = 3 is 6.4 sec without affecting the PSNR value i.e. more the number of K less time is required.

Table 1: Results of Shamir for Authentication

Sr. No	Image size	N	k	PSNR In dB	Time In Sec
1	64	6	2	81.79	6.66
2	64	6	3	81.79	6.4
3	70	6	3	83.35	7.74
4	90	7	2	87.71	13.34
5	100	5	3	89.54	12.60
6	100	6	3	89.54	13.04
7	128	5	3	93.83	28.40
8	128	10	3	93.83	26.19
9	130	5	3	94.10	28.40
10	150	3	1	96.59	27.62
11	200	4	3	101.58	64.43
12	300	9	7	108.63	214.30
13	400	6	3	113.62	251.16
14	575	3	2	119.93	452.56
15	625	7	3	121.38	624.33
16	700	8	3	123.35	687.88
17	800	6	4	125.67	1084.08
18	900	8	3	127.62	1264.79
19	1000	5	3	129.54	1603.19
20	1028	5	3	130.02	1328.61

The table 2 shows the values when the authentication is not applied. Here also the images of any size are transferred and the time is recorded with the PSNR value. When comparing the authentication and non-authentication. The system has a lower PSNR value and higher time required for the process to complete.

Table 2: Results Of Shamir for Non Authentication

Sr. No	Image size	N	k	PSNR In dB	Time In Sec
1	64	6	2	1.95	7.42
2	64	6	3	5.03	6.93
3	70	6	3	7.91	8.21
4	90	7	2	4.29	10.86
5	100	5	3	8.47	16.10
6	100	6	3	6.81	16.53
7	128	5	3	1.91	26.29
8	128	10	3	8.64	31.37
9	130	5	3	4.98	25.88
10	150	3	2	2.79	24.80
11	200	4	3	6.74	61.05
12	300	9	7	4.34	173.18
13	400	6	3	6.34	263.03
14	575	3	2	2.13	378.67
15	625	7	3	6.46	546.85
16	700	8	3	6.89	713.51
17	800	6	4	6.64	959.06
18	900	8	3	8.59	1117.78
19	1000	5	3	4.15	1504.07
20	1028	5	3	7.80	1590.57

The table 3 shows the results of of M K Reddy Algorithum For Authentication , it always give the result that user is authenticate . From table 3 we can say that the PSNR is very low so the algorithum is insecure and lossy as well as it require the image size as power of 2 .

Table 3: Results of M K Reddy Algorithum For Authentication

Sr. No	Image size	N	k	PSNR In dB	Time In Sec
1	64	6	2	1.95	7.42
2	64	6	3	5.03	6.93
3	70	6	3	7.91	8.21
4	90	7	2	4.29	10.86
5	100	5	3	8.47	16.10
6	100	6	3	6.81	16.53
7	128	5	3	1.91	26.29
8	128	10	3	8.64	31.37
9	130	5	3	4.98	25.88

10	150	3	2	2.79	24.80
11	200	4	3	6.74	61.05
12	300	9	7	4.34	173.18
13	400	6	3	6.34	263.03
14	575	3	2	2.13	378.67
15	625	7	3	6.46	546.85
16	700	8	3	6.89	713.51
17	800	6	4	6.64	959.06
18	900	8	3	8.59	1117.78
19	1000	5	3	4.15	1504.07
20	1028	5	3	7.80	1590.57

V. COMPARATIVE ANALYSIS

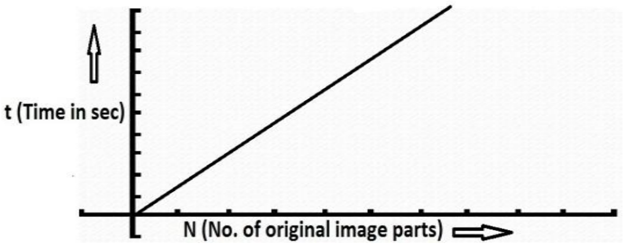


Fig. 10. General Graphical Representation For Shamir Authentication Between Time And N i.e. No Of Parts In Which Original Image Get Divided

Above fig. 10 shows if no of parts in which image is divided are increased then the time is increased .

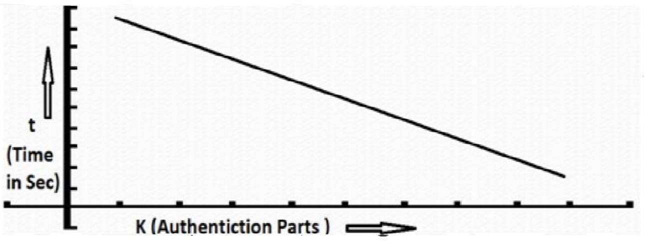


Fig. 11. General Graphical Representation For Shamir Authentication Between Time And K i.e. Authentication Parts

Above fig 11 shows if k i.e. authentication parts increased then time will be decreased .Here also time measures in seconds.

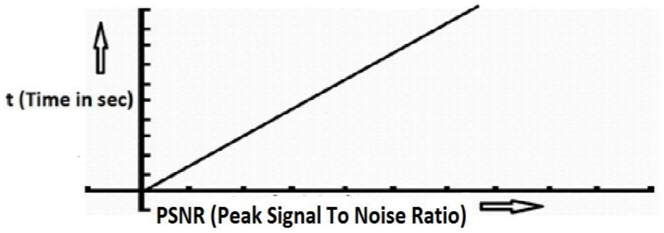


Fig. 12. General Graphical Representation For Shamir Authentication Between Time And K i.e. Authentication Parts

Above fig 12 shows if PSNR i.e. Peak Signal To Noise Ratio increased then time will be increased .

MK Reddy divides the original image into into only 3 parts where as Shamir divides it into the N no of parts due to this reason authentication using Shamir is more secure than MK Reddy' s algorithm..

PSNR is more in case of Shamir authentication so it is more secure where as MK reddy authentication results very low PSNR value so it is insecure.

MK Reddy divides the original image into into only 3 parts. These 3 parts are very less in number. So it can easily decrypted and while decryption it is easy to know from encryption which image is encrypting because it can be easily seen by Human Visual System.

MK Reddy algorithum having property to adding horizontal lines while encoding and decoding the images , it affects the original image.

MK Reddy requires image size as power of 2 while Shamir doesn't have any condition like this.

MK Reddy is lossy algorithum as compare to Shamir algorithum .

VI. CONCLUSION

In this paper we have introduced a technique for visual cryptography in which any type of image can be chosen as a passward, images then divided and then apply Shamir and M K Reddy encryption and decryption techniques . After decryption system get match with original image then system give result as the user is authenticate otherwise non authenticate. The system introduced in this paper satisfy the needs of authentication. From Implemention. And Results we can say that this system can help in using multiple size and type of images for authentication. Shamir is one of the algorithm to satisfy the needs for authentication. The PNSR value is enhanced by using the system. The time required by the system is lesser then normal system. More the number of authentication parts less is the time required. From all the results we can also say that Shamir is better than MK Reddy which satisfy the needs for authentication.

VII. FUTURE WORK

The completion of this techniques introduced in this paper provides an opportunity for future work and expansion related to the current scheme presented. The primary expansion that can be executed is implementing this current scheme on all known Visual Cryptography algorithms. This would allow the robustness and effectiveness of the scheme to be properly evaluated. This would be a large commitment as proper the analysis of the paper, in addition to implementing the algorithm and comparing the results. This would allow an overall understanding of Visual Cryptography algorithms and would remove some of the author and reviewer bias.

ACKNOWLEDGEMENT

A paper is creative work of mind. A proper synchronization is must for any project to be completed successfully. I am extremely grateful to all my well wisher for the successful completion of this paper.
I express my sincere gratitude to *Dr.P.M.Jawandhiya* , principal, PLITMS, Buldana for being constant source of inspiration and providing his valuable guidance. And thankful to *Prof. P. B. Shelke* , guide and HOD of ENTC Department, for his valuable guidance needed.

REFERENCES

[1]. Moni Naor and Adi Shamir ,"Visual cryptography", In Proceedings of Advances in Cryptology, EUROCRYPT 94, Lecture Notes in Computer Science, 1995, (950):pp. 1-12.

[2]. Blakely, G. R. 1979. Safeguarding Cryptographic Keys. Proceedings of the National Computer Conference, American Federation ofInformation Processing Societies Proceedings. 48: 313-317.

[3]. Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography," IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453,Aug. 2006.

[4]. Chang-Chou Lin, Wen-Hsiang Tsai, "Visual cryptography for graylevel images by dithering techniques", Pattern Recognition Letters, V.24 n.1-3.

[5]. F. Liu, C.K. Wu, X.J. Lin, "Colour Visual Cryptography Schemes", IET Information Security, vol. 2,No. 4, pp 151-165, 2008.

[6]. C.C. Wu, L.H. Chen, "A Study On Visual Cryptography", Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[7]. S. J. Shyu, S. Y. Huanga,Y. K. Lee, R. Z. Wang, and K. Chen, "Sharing multiple secrets in visual cryptography", Pattern Recognition, Vol. 40, Issue 12, pp. 3633 - 3651, 2007.

[8]. K. H. Lee and P. L. Chiu, "An extended visual cryptography algorithm for general access structures," IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 219–229, Feb. 2012.