International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 6 382 – 386

# (N,N) Share Generation using Key Share approach for RGB image in VCS

Shivam S. Upadhyay
Computer Science Engineering
RKDFIST
Bhopal, India
*Shivam91092@gmail.com*

Niresh Sharma,Ritesh Yadav
Assistant Professor, Assistant Professor
RKDFIST
Bhopal,India
*er.ritesh1987@gmail.com*

***Abstract*—**Visual Cryptography is a secure and unique image encryption technique which protects image based secret. In visual cryptography image is encrypted into shares and in decryption process all or some of shares are super imposed with each other to decrypt the original secret image. In this technique no complex computation is needed for decryption of secret image which is the best advantage of Visual Cryptography Scheme. In this report various types of visual cryptographic techniques are discussed from previous research area. In this proposed system (N, N) VCS is used for encryption. It takes color image as an input and extracts in R, G and B components. After that it generates Key-Mask using Key-Mask generation algorithm which XOR-ed with R, G and B components and gives the key shares. Further XOR operation of these key shares with key mask generates the color shares. In decryption process image is recovered by XOR operation between key mask and color shares. It has a better security features compared to previous one.

***Keywords*-***VCS, (N,N) Encryption, XOR operation*

*****

## I. INTRODUCTION

Visual cryptography is a cryptographic technique in which visual information (pictures, text, documents, etc.) is encrypted in such a way that decryption can be done by human eyes via sight reading.

All the credit goes to Moni Naor and Adi Shamir for developing one of the best-known techniques in 1994. Authors introduced a visual secret sharing scheme, where an original secret image was divided into n shares so that someone who has all the n shares could decode the secret, where as any n − 1 shares disclosed no information about the secret image. Each share was printed on a different transparency, and decoding was done by combining the shares. Original secret image is recovered when all the n shares are combined together.

Visual cryptography is a special kind of image encryption technique, in which image is divided into shares using Simple XOR operation.

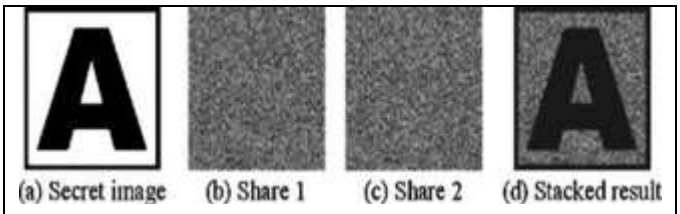


Figure 1 Example of Visual Cryptography Scheme.

This paper provides overview of various visual cryptography schemes. Taking limited bandwidth and storage into consideration two criteria pixel expansion and number of shares encoded is of significance. Smaller pixel expansion results in smaller size of the share. Encoding multiple secret images into the same share images requires less overhead while sharing multiple secrets. Meaningful shares avoid attention of hacker considering the security issues over the communication channels. To meet the demand of today's multimedia information gray and color image format should be encoded by the schemes. Other performance measures such as contrast, accuracy, security and computational complexity that affect the efficiency of visual cryptography are also discussed in this paper.

This paper is organized as follow: provides overview of black and white visual cryptography schemes, color visual cryptography scheme are elaborated in, performance of visual cryptography schemes are analyzed and last section concludes the paper.

## II. THEORYTICAL BACKGROUND

Visual cryptography is an image encryption technique, which protects image based secret. Visual Cryptography does not require any complex computation to decrypt the secret image; instead it can be done by human eyes via sight reading which the huge benefit of using visual cryptography. At present data security is a top most priority as it travelled through internet over various networks. Various methods have been researched and developed for better security of our data. Secret data can be in different forms such as image, audio, video, text, etc. Here our focus is only on image based secret. Visual cryptography plays a vital role in image security. In the encryption process of this technique image is encrypted into multiple shares and at the other hand on decryption side all or some of the shares are stacked together to reveal the secret image. Different types of visual cryptography techniques have been researched which is traditional visual cryptography, halftone visual cryptography, general access structure based visual cryptography, block based progressive visual cryptography and random grid based visual cryptography, and recently developed hierarchical visual cryptography.

To maintain the privacy and secrecy of images is a spirited space of analysis so the Visual Cryptography planned by Naor and Shamir could be a technique that safely shares a secret image to several participants [7]. " Visual Cryptography is a special kind of cryptographic technique in which the decryption can perform by the human visual capability". In Visual Cryptography original image which carries the secret information is encrypted into multipleshares so that no one could recover the secret information in absence of other shares. In

 ISSN: 2321-8169
382 – 386

Decryption process all or qualified set of shares are required to be stacked together to reveal the secret. The encryption takes place in such a way so that at decryption side no mathematical equation is needed to decrypt the secret image. The original image which is to be encrypted is referred as secret image. Once the encryption is completed, ciphers are generated which is referred as shares. Share is a scramble form of original input image from single share anyone could not recover any idea about the original secret image. To share the secret among group of n participants is the fundamental idea behind visual cryptography [11]. The protected secret is separated into n number of parts, referred as shares, in order to share the secret. After that, these shares are distributed among n participants. Each participant provides his own share, to reveal the original secret. The flow of visual cryptography is shown in figure: 2.

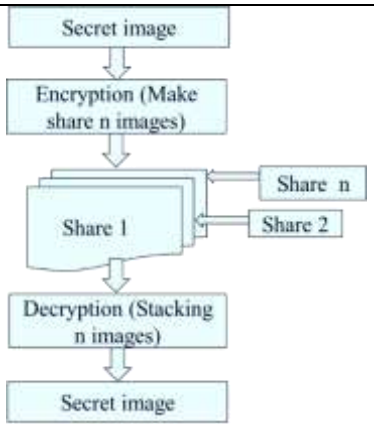


Figure 2 Flow of VCS [11]

There are 3 visual cryptographic schemes are available which is listed below:-

1. (2,2) visual cryptographic scheme
2. (k, n) visual cryptographic scheme
3. (n, n) visual cryptographic scheme

The (2, 2) visual cryptographic scheme is basic scheme proposed by naor [1]. In this scheme the secret is separated into exactly two parts. These two shares must participate to reveal the secret. Another scheme, in which secret is encoded into n shares. To recover the original secret image both two shares are participate in decryption process. This scheme is known as 2 out of n scheme.

In (k, n) VCS the original secret is separated into n number of shares and to reveal the secret k or more shares must be participate in decryption process. This scheme is known as k out of n (k, n) scheme. Third scheme is (n, n) VCS is extension of third visual cryptography scheme, called n out of n, in which secret is encrypted into n shares. All n shares are participating in decryption process to get original secret image. More number of shares can be generated in (n, n) visual cryptography scheme [6].

Hierarchical Visual Cryptography is an extended version of traditional VCS. In HVCS secret image is encrypted in hierarchical manner. In the beginning secret image is encrypted to generate share 1 and share 2. Later on both shares are encoded independently generating share11, share12, share21, share22, then after share12, share21 and share22 are collected to generate the key-share. This encoding scheme finally generates two shares: the key share and one other share11 which is handed over to the user. Shares created by this process are random in nature and does not reveals any secret by visual site reading. At decryption side the key share and user share are super imposed with each other and the original secret image is generated [1].

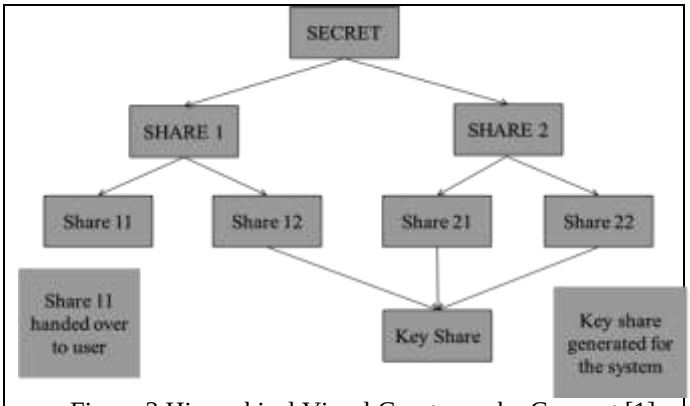


Figure 3 Hierarchical Visual Cryptography Concept [1]

## III. PROPOSED WORD

In this proposed system (N, N) visual cryptography scheme is used for security. This technique is applied on a color image. First color image is added as an input then next phase is R, G, and B component extraction. Then color shares are generated by XOR operation with Key Mask. Key mask generation algorithm is used for generating key mask. In decoding process all color shares are XOR-ed with each other and generate Master share. Master share is XOR-ed with key mask to get the recovered image. By using this method user get better security, so hacker cannot get any idea about the secret.

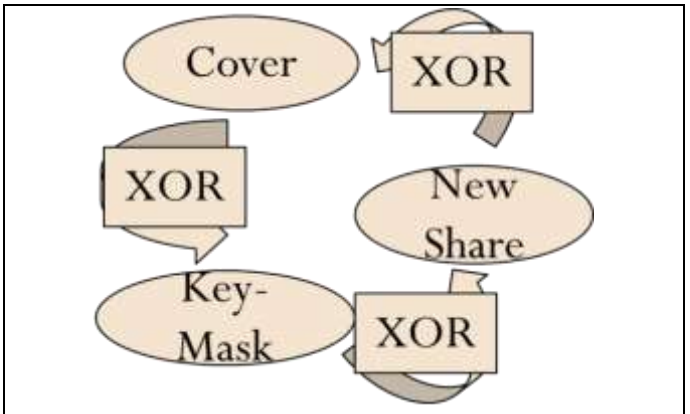


Figure 4 Flow of Proposed System

In the proposed system new shares are generated by XOR operation between Original image and Key-Mask. Key-Mask is created with the help of Key-Mask generation algorithm. At the end secret is revealed by XOR operation between new shares and Key-Mask.

 ISSN: 2321-8169
382 – 386

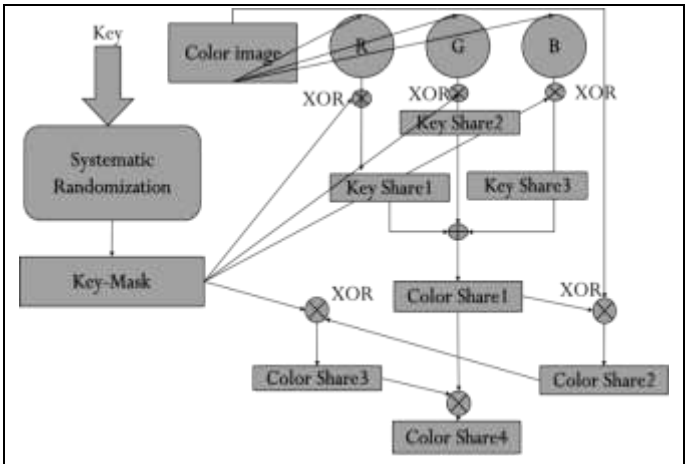

Figure 5 Proposed Work Flow (Encoding)

### *A. Encoding Algorithm of Proposed Work*

Step1: KEY-MASK is generated using systematic randomization.
Step2: Color share divided into RGB channel separate channel is XOR with KEY-MASK and Generate KEY-SHARE.
Step3: All KEY-SHARE combine will make one SHARE1.
Step4: Now Cover image and SHARE1 XOR produce New SHARE2.
Step5: SHARE2 and KEY-MASK XOR produce SHARE3.
Step6: SHARE3 and SHARE1 XOR generate another SHARE4.
Step7: The sequence Color image – Key-Mask – New Share will be repeated to generated new shares.

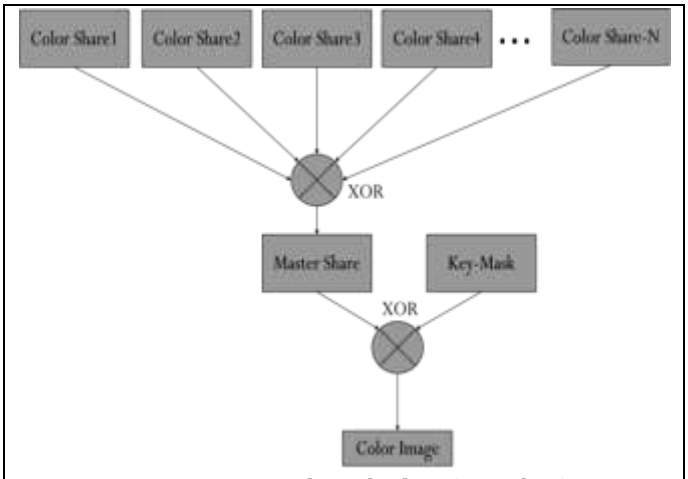

Figure 6 Proposed Work Flow (Decoding)

### *B. Decoding Algorithm of Proposed Work*

Step1: All SHAREs are combining with XOR and make MASTER SHARE.
Step2: Master SHARE and KEY-MASK Combine with XOR will GENERATE the COLOR image.

## IV. IMPLEMENTATION RESULTS

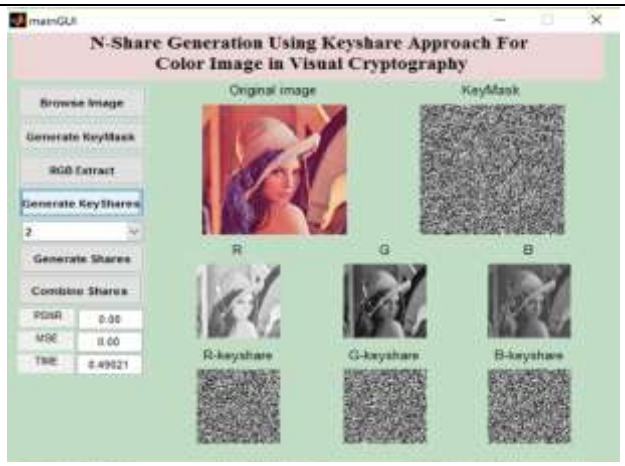

Figure 7 System GUI

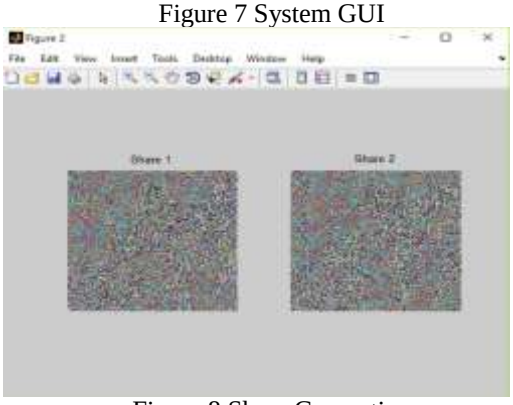
Figure 8 Share Generation


Figure 9 Recover Lena Image

## V. ANALYSIS

Table 1: PSNR and MSE

| Image Name | MSE | PSNR |
|---|---|---|
| Car | 1.04170 | 47.9535 |
| Flower | 0.50863 | 51.0668 |
| Lena | 0.71235 | 49.6039 |
| Leaf | 0.86549 | 48.7582 |
| Bird | 0.57941 | 50.5009 |
| Fruit | 1.0746 | 47.8184 |
| Text | 1.0999 | 47.7171 |
| Fish | 0.2691 | 53.8316 |
| Plane | 0.92783 | 48.4561 |
| Kiwi | 0.53973 | 50.8091 |

Table 2: Key Value Analysis

| Image Name | Key Value | MSE | PSNR |
|---|---|---|---|
| Car | 0.1 | 0.049989 | 61.1421 |
| | 0.2 | 1.0417 | 47.9535 |
| | 0.3 | 0.9085 | 48.5475 |
| | 0.4 | 0.52758 | 50.9079 |
| | 0.5 | 1.0417 | 47.9535 |
| | 0.6 | 1.0995 | 47.7187 |
| | 0.7 | 0.64734 | 50.0195 |
| | 0.8 | 1.0295 | 48.0046 |
| | 0.9 | 2.0833 | 44.9432 |
| | 1.0 | 0.52083 | 50.9638 |

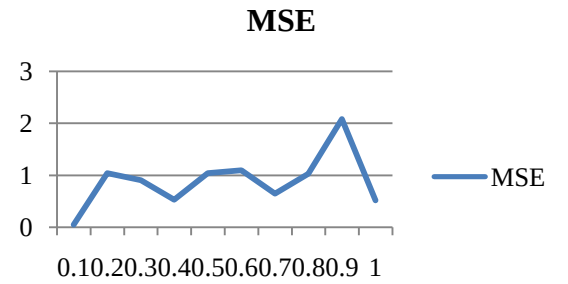


Figure 10MSE

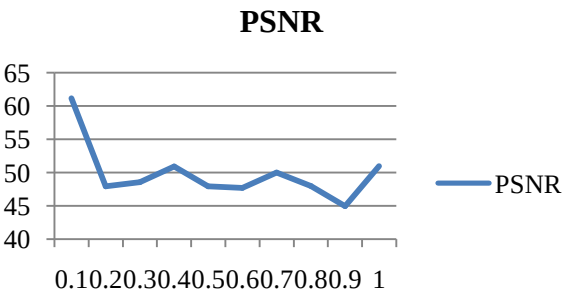


Figure 11 PSNR

Table 3: Key Value generation time

| Image Name | Key Value | Encoding Time(s) | Decoding Time(s) |
|---|---|---|---|
| Car | 0.1 | 0.382803 | 0.024351 |
| | 0.2 | 0.37015 | 0.020428 |
| | 0.3 | 0.339637 | 0.033969 |
| | 0.4 | 0.379305 | 0.036731 |
| | 0.5 | 0.375005 | 0.039099 |
| | 0.6 | 0.375181 | 0.022031 |
| | 0.7 | 0.413382 | 0.022125 |
| | 0.8 | 0.377317 | 0.036264 |
| | 0.9 | 0.34926 | 0.02208 |
| | 1.0 | 0.37936 | 0.035775 |

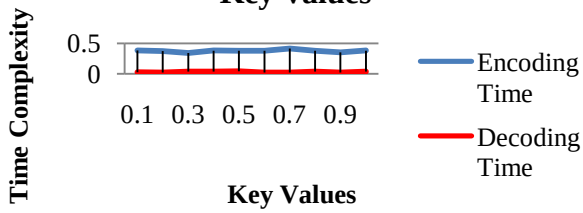


Figure 12 Time Complexity

## CONCLUSION

Hereby it is concluded that system will generate color share VCS with novel key share approach. It will provide better security in confidential data so hacker cannot hack our important data when we will share data in secured transmission channel media.

## REFERENCES

[1] Pallavi Vijay Chavan, Dr. Mohammad Atique, Dr. Latesh Malik, "Signature Based Authentication using Contrast Enhanced Hierarchical Visual Cryptography" IEEE: Students' Conference on Electrical, Electronics and Computer Science: 2014

[2] M. Sukumar Reddy, S. Murali Mohan,"Visual Cryptography Scheme for Secret Image Retrieval" IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.6, June 2014

[3] Mohamed Fathimal. P and Arockia Jansi Rani .P ,"(N, N) Secret Color Image Sharing Scheme with Dynamic Group " I. J. Computer Network and Information Security, 2015, 7, 46-52

[4] Shubhra Dixit, Deepak Kumar Jain,Ankita Saxena, "An Approach for Secret Sharing Using Randomised Visual Secret Sharing" Fourth International Conference on Communication Systems and Network Technologies: 2014

[5] Hao Luo a, Hua Chen a, Yongheng Shang a, Zhenfei Zhao b, Yanhua Zhang b, "Color transfer in visual cryptography" Elsevier Ltd. All rights reserved: 2014

[6] Farzin Ahammed T, M.K Sulaiman "A Master Share (2, n) XOR based Visual Cryptography Scheme by Random Grids" ,International Conference on Control, Communication & Computing India (ICCC) | 19-21 November 2015 | Trivandrum: 2015

[7] Shamir A," How to share a secret", Communication of the ACM 22(11):612–3,1979

[8] P.Mohamed Fathimal1 , Dr.P.Arockia Jansi Rani2, "Bidirectional Serpentine Scan Based Error Diffusion Technique for Color Image Visual Cryptography " ,International Journal of Science, Engineering and Technology Research, Volume 3, Issue 9, September 2014

[9] Chih-Ching Thien, Ja-Chen Lin* , "Secret image sharing" , 0097-8493/02/$ - see front matter r 2002 Elsevier Science Ltd.

[10] Aarti, Pushpendra K Rajput, "An EVCS for Color Images with Real Size Image Recovery and Ideal Contrast Using Bit Plane Encoding ", I.J.Computer Network and Information Security, 2014, 2, 54-60

[11] Trupti Patel , "A Review on Different Visual Cryptography Techniques ", IJSRD - International Journal for Scientific Research & Development| Vol. 4, Issue 06, 2016

[12] Moni Naor and Adi Shamir, "Visual Cryptography", Eurocrypt, 1994

[13] Shyong Jian Shyu and Ming Chiang Chen," Minimizing Pixel Expansion in Visual Cryptographic Scheme for General Access Structures" , 1051-8215 (c) 2015 IEEE

[14] Angelina Espejel-Trujillo, Mariko Nakano-Miyatake, and Hector Perez-Meana," New Condition for Hierarchical Secret Image Sharing Scheme", 1550-445X/14 $31.00 © 2014 IEEE

[15] Rajendra Ajjipura Basavegowda and Sheshadri Holalu Seenappa,"Secret Code Authentication Using Enhanced Visual Cryptography", _ Springer India 2014

[16] Farzin Ahammed T, M.K Sulaiman, "A Master Share (2, n) XOR based Visual Cryptography Scheme by Random Grids", ICCC 2015

[17] Divya Chaudhary, Shailender Gupta and Sweety Deswal,"Origin of Hybrid Security Mechanisms and Ways of Improvement" ,IJBDSI 2015