URKUND

Document Information

Analyzed document	projectreport_plagiarism.pdf (D72247423)
Submitted	5/21/2020 5:13:00 PM
Submitted by	Prof Shashi Kumar Dhiman
Submitter email	shashi.dhiman@gmail.com
Similarity	12%
Analysis address	shashi.dhiman.hpu@analysis.urkund.com

Sources included in the report

SA	URL: Thesis23.12.17.docx Fetched: 12/26/2017 2:56:00 PM	12
W	URL: https://wireilla.com/papers/ijfcst/V3N6/3613ijfcst05.pdf Fetched: 10/14/2019 6:27:50 PM	6
SA	URL: Deepika_MP_Thesis_Report.pdf Fetched: 2/14/2019 8:24:00 AM	6
W	URL: https://archive.org/stream/VisualCryptographyAndSecretImageSharingDigitalImagingAn ... Fetched: 12/12/2019 10:56:43 AM	2
SA	URL: Chapter 1 - Introduction_corrected.doc Fetched: 1/22/2017 5:04:00 PM	3
SA	URL: dissertation.docx Fetched: 5/13/2019 7:36:00 AM	3
W	URL: https://ijcat.com/archives/volume2/issue3/ijcatr02031027.pdf Fetched: 11/25/2019 4:30:21 PM	2
J	**Design of visual cryptographic methods with smoothlooking decoded images of invariant size for grey-level images** URL: f8f772db-cc0a-4118-bd26-03b8ed98c964 Fetched: 3/13/2019 1:28:06 PM	1
W	URL: https://www.spiedigitallibrary.org/conference-proceedings-of-spie/9946/99460X/Appl ... Fetched: 5/21/2020 5:16:00 PM	1
SA	URL: wrmain.pdf Fetched: 10/11/2019 5:14:00 PM	1

Digital Image Processing

A Report on Visual Cryptography Using Shamir Secret Sharing

BY

Utkarsh Suryaman
Roll No. 101603366

Under the Guidance
Dr. Shivendra Shivani, Department Of Computer Science
Thapar Institute of Engineering And Technology, Patiala, INDIA

THAPAR INSTITUTE
OF ENGINEERING & TECHNOLOGY
(Deemed to be University)

Submitted to the

Computer Science and Engineering Department, Thapar Institute of Engineering and Technology, Patiala.

In Partial Fulfilment of the Requirement for the Degree of Bachelor of Engineering in Computer Engineering at Thapar Institute of Engineering and Technology, Patiala

September 2020

Visual Cryptography Using Shamir Secret Shares

*Note: Shamir Secret K Out-Of N Shares

Utkarsh Suryaman
Deptartment of Computer Science
Thapar Institute Of Engineering And Technology
Patiala, India
utkarshsuryaman@gmail.com

Submitted to Dr. Satvindra Shivani
Deptartment of Computer Science
Thapar Institute Of Engineering And Technology
Patiala, India
satvindra.shivani@thapar.edu

***Abstract*—Visual Cryptography is a secret sharing technique which allows the encryption of asecret image amonst a number pf participants. This scheme can be applied toa secret sharing, information hiding, identification/ authentication, copyright protection, etc. In this scheme low level of calculations are required.**

***Index Terms*—K−Shares,N−Participants,HammingWeight** C_0, C_1, α, γ, π

I. Introduction

The idea of cryptography by sharing was freely presented by [1] Shamir and Blakely in 1979. [2]In 1995, Naor and Shamir developed another sort of share sharing plan, called visual cryptography (VC). Visual cryptography is a sort of share picture sharing plan that utilizes the human visual framework to play out the decoding calculation.A visual cryptography conspire (VCS) permits classified messages to be encoded into n share sharing plans. VC is intriguing on the grounds that unscrambling should be possible with no earlier information on cryptography and can be performed with no cryptographic calculation [1]. The requirement for share sharing emerges if the capacity framework is not solid and secure. share sharing is likewise prominently helpful if the proprietor of the share does not confide in any single individual.

In secret sharing schemes, [2] the number of the participants in the reconstruction phase is important for recovering the secret. A solution to the k out of n visual secret sharing scheme consists of two collections of $n * m$ Boolean matrices C_0 and C_1. To share a white pixels, the user have to choose one of the matrices in C_0, and to share a black pixel, the dealer randomly chooses one of the matrices in C_1. Shamirs scheme is based on polynomial interpolation. Given an k pairs $(x_1, y_1), (x_2, y_2), ..., (x_k, y_k)$ with $x_i \neq x_j$ for all $1 \geq i > j \leq k$, there is one and only one [2] polynomial $P(x)$ of degree $k - 1$ such that $P(x_i) = y_i$, for all $1 \leq i \leq k$. [2]

$$C_0 = \left\| \begin{matrix} 1 & 0 \\ 1 & 0 \end{matrix} \middle\| \begin{matrix} 0 & 1 \\ 0 & 1 \end{matrix} \right\| \tag{1}$$

$$C_1 = \left\| \begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix} \middle\| \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \right\| \tag{2}$$

The secret S is chosen as the free coefficient of a random polynomial P of degree$k - 1$ over the field of positive integers modulo a large prime. The shares $I_1, ..., I_n$ are chosen as $I_i = P(x_i)$, for all $1 \leq k \leq n$, where $x_1, ..., x_n$are pairwise distinct public values. Having the shares $I_i : i_A$, for some group A with —A— = k, the secret can be obtained using Lagranges interpolation formula

$$S = \sum_{i \in A} \left(I_i \prod_{j \in A/\{i\}} \frac{x_i}{x_j - x_i} \right) \tag{3}$$

Shamir has proposed choosing $x_i = I$, for all $1 \leq I \leq n$. In this case, the secret can be

$$S = \sum_{i \in A} \left(I_i \prod_{j \in A/\{i\}} \frac{i}{j - i} \right) \tag{4}$$

Noar and Shamir were the inventers of secret sharing scheme, called visual cryptography(VC). Visual cryptography is a kind of secret image sharing scheme that uses the human visual system to perform the decryption computation. It is used to decode the message with only minute of colculations. A visual cryptography scheme (VCS) allows confidential string/integer/binary as well as colored images to be encrypted into k out of n secret sharing schemes. Whenever the number of participants from the group(n) is larger than or equal to the predetermined threshold values (k) [2]. The confidential message can be obtained by these participants. The key feature of VCS is that, decryption can be done with no prior knowledge of cryptography.The visual cryptography scheme eliminates the problem of complex computation in the decryption process, and the secret images can be restored by stacking (x-oring)operation. This property makes visual cryptography useful especially for the low computation load requirement. The simplest version of the visual secret sharing problem makes assumptions that the message consists of a collection of black and white pixels and each pixel is handled separately. Each original pixel appears in n modified versions (called shares), one for each transparency. Each share is a collection of m black and white sub-pixels, which are printed in close proximity to each other so that the human visual system averages their individual black/white contributions.

Identify applicable funding agency here. If none, delete this.

The resulting structure can be described by $n * m$ Boolean matrix $S = [s_{ij}]$ where $s_{ij} = 1$ iff the j^{th} subpixel in the i^{th} transparency is black. When transparencies $i_1, i_2, \cdots, i_r$ are stacked together in a way which properly aligns the subpixels, we see a combined share whose black subpixels are represented by the Boolean *or* of rows $i_1, i_2 ....., i_r$ in S. The grey level of this combined share is proportional to the Hamming weight $H(V)$ of the *or* ed m-vector V. This gray level is interpreted by the visual system of the users as black if $H(V) \geq d$ and as white if $H(V) < d - \alpha m$ [2] for some fixed threshold $1 \leq d \leq m$ and relative difference $\alpha > 0$

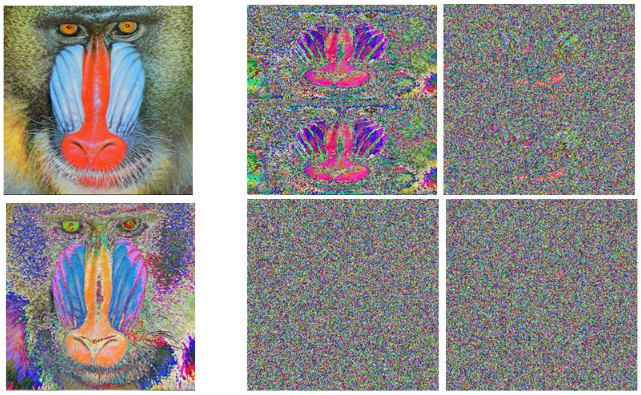


Fig. 1. Sequence from original picture to decrypted picture.

II. The Model

A. Value parameters

The resulting structure can be described by a Boolean matrix $M = (m_{ij})n \times m$ where $m_{ij} = 1$ if and only if the j^{th} subpixels of the i^{th} share (transparency) is black. Usually, we will use R_0 to refer to constructed M when the pixels in the original images is white, and similarly R_1 when the pixel in the original image is black. The important parameters of the scheme are:

- m: the count of number of pixels in a share. This parameter represents the loss in resolution from the original image to the recovered one.
- α: the relative difference in the weight between the combined shares that come from a white pixel and a black pixel in the original image. WE can represent change in contrast before and after encryption process.
- γ: the size of the collection of C_0 and C_1 . C_0 refers to the sub-pixel patterns in the shares for a white pixel and black refers to the sub-pixel patterns in the shares for the 1 pixel.
- Hamming weight: It is the count for the number of number of Zero elements in an array of elements defined over Galois Field.GF [5]

B. Shamir's Model

To share a white pixel, the dealer randomly chooses one of the matrices in C_0, and to share a black pixel, the dealer randomly chooses one of the matrices in C_1. The solution is considered valid if the following conditions are met:

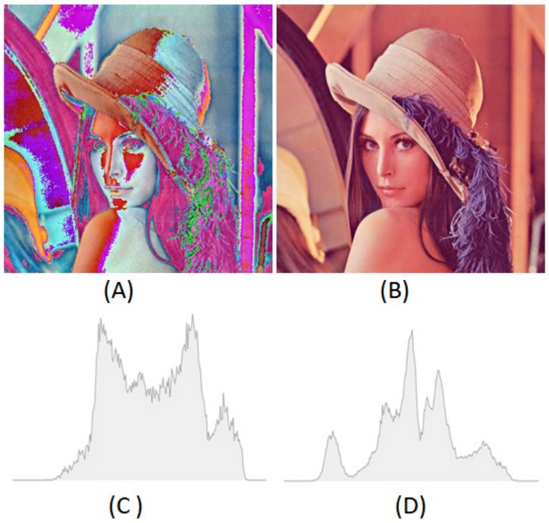


Fig. 2. Figure Showing relative difference

- For any S in C_0, the *or* V of any k of the n rows satisfies $H(V) \leq d - \alpha \times m$.
- For any S in C_1, the *or* V of any k of the n rows satisfies $H(V) \geq d$ There two properties are called contrast.

For any subset $i_1, i_2 \cdots, i_q$ of $1, 2, \cdots, n$ with $q < k$, the collections of $g * m$ matrices D_t for $t \in 1, 0$ obtained by restricting each $n * m$ matrix in $c_t(where t = 0, 1)$ to rows $i_1, i_2 \cdots, i_q$ are indistinguishable in the sense that they contain the same matrices with the same frequencies. The third condition is called security.

C. Theorem

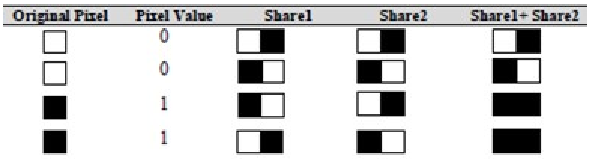
Any black and white VCS can be given using two $n \times m$ Boolean matrices s^0 and s^1, called basis matrix, to describe the subpixels in the share. The basis matrix s^0 is used if the pixels in the original image is white, and the basis matrix s^1 is used if the pixels in the original image is black. The use of the basis matrices S^0 and S^1 can have small memory requirements (it keeps only the basis matrices S^0 and S^1), and it is efficient (to choose a matrix in C_0 or C_1) because it only generates a permutation of the columns of S^0 or S^1. Where ω H (V) is the hamming weight (the number of ones) of the m-vector V of any k of the n rows, m is the pixel expansion and α is the relative difference.

Relative difference 1: Let $\omega_H(S^0)$ and $\omega_H(S^1)$ be the Hamming weight respectively to the matrices S^0 and S^1. The relative difference α is defined as: $\alpha = (\omega_H(S^1) - \omega_H(S^0)/m)$

Contrast 1: Let α be the relative difference and m be the pixel expansion. The formula to compute contrast in different VCS is: $\beta = \alpha \times m, \beta \geq 1$

III. The Construction of 2-out-of-2 VCS And Observations

We have a binary image S having exactly m pixels. The scheme proposed creates two share (binary images), S_1 and



Original Pixel	Pixel Value	Share1	Share2	Share1+ Share2
□	0	□■	□■	□■
□	0	■□	■□	■□
■	1	■□	□■	■■
■	1	□■	■□	■■

Fig. 3. Pixels pattern for 2 out of 2 VCS with 2 -subpixels

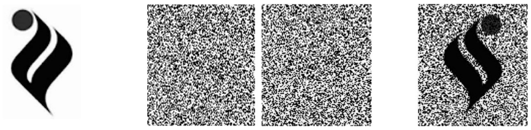


Fig. 4. 2-out-of-2 VCS with consistent share size using the image S^{I2} (a) S^{I2} (b) S^1 (c) S^2 and (d) $S^1 + S^2$

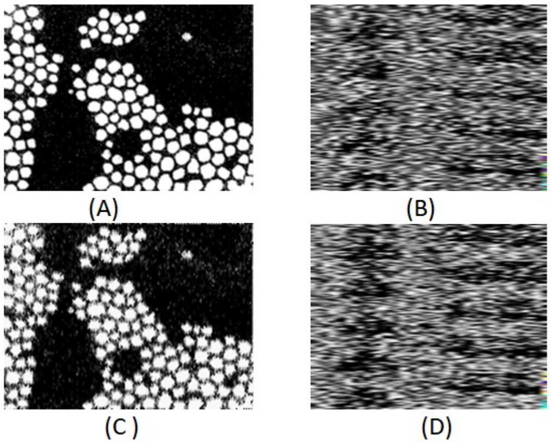


Fig. 5. Construction of 2-out-of-2 VCS for coloured images

S_2, consisting of exactly two pixels for each pixels in the secret image as mentioned below. If the pixels in S is white, the dealer randomly chooses on row from the first two rows of figure 3. If the pixel in S is black, the dealer randomly chooses one row from the last two rows of figure.

To analyze the security of the 2-out-of-2 VCS, the dealer randomly chooses one of the pixel patterns (black or white) from the image above for the shares S1 and S2. The pixel selection is random so that the shares S_1 and S_2 consists of an equal number of black and white subpixels. The individual pixel cannot be segregated as black or white. This method provides perfect security. The two participants can recover the secret pixels by superimposing the two shares subpixels. If the superimposition results in two black subpixels, the original pixel was black; if the superimposition creates one black and one white subpixel, it indicated that the original pixel was white.

In visual cryptography, the white pixel is represented by 0 and the black pixel by 1. For the 2-out-of-2 VCS, the basis matrices, S_0 and S_1 are designed as follow:

$$S^0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \tag{5}$$

$$S^1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{6}$$

There are two collections of matrices, C0 for encoding white pixels and C1 for encoding black pixels. Let C0 and C1 be the following two collections of matrices: $C_0 = \pi(S^0)$ $C_1 = \pi(S^1)$ Where $\pi(S^0)$ and $\pi(S^1)$ represents the collection of all matrices obtained by permuting the columns of matrices S^0 and S^1 respectively. That is, There are two collection of matrices, C_0 for encoding white pixels and C_1 for encoding black pixels.

$$C_0 = \Bigg\| \begin{matrix} 1 & 0 \\ 1 & 0 \end{matrix} \Bigg\| \begin{matrix} 0 & 1 \\ 0 & 1 \end{matrix} \Bigg\| \tag{7}$$

$$C_1 = \Bigg\| \begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix} \Bigg\| \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \Bigg\| \tag{8}$$

To share a white pixel, the dealer randomly selects one of the matrices in C_0, and to share a black pixels, the dealer randomly selects one of the matrices on C_1.

IV. The Construction of k-out-of-n VCS And Observations

In the k-out-of-n visual cryptography scheme, n shares will be produced to encrypt an image, and n shares must be stacked to decrypt the image. If the number of shares stacked is less than n, the original image is not revealed. Let G be the ground set given by $G = \{g_1, g_2, \cdots, g_n\}$ of n elements.

Let $E = \{\pi_1, \pi_2, \cdots, \pi_2^{n-1}\}$ be the collection of all subsets with even cardinality and let $O = \{\sigma_1, \sigma_2, \cdots, \sigma_2^{n-1}\}$ be the collection of all subsets with odd cardinality. Each of them is defined by a matrix which is denoted by S^0 and S^1 with order $n \times 2n - 1$.

For $1 \leq i \leq n$ and $1 \leq j \leq 2n - 1$, all the matrices are obtained by permuting the columns of $S^0 = [s_{ij}^0]$ and $S1 = [s_{ij}^1]$ in which
$s_{ij}^0 = 1 \Leftrightarrow g_i \in \pi_j$,
$s_{ij}^1 = 1 \Leftrightarrow g_i \in \sigma_j$.

The basis matrices for k-out-of-n visual cryptography can be described by considering 3-out-of-3 VCS parameter.The S^0 basis matrices for 3-out-of-3 VCS can be constructed as,

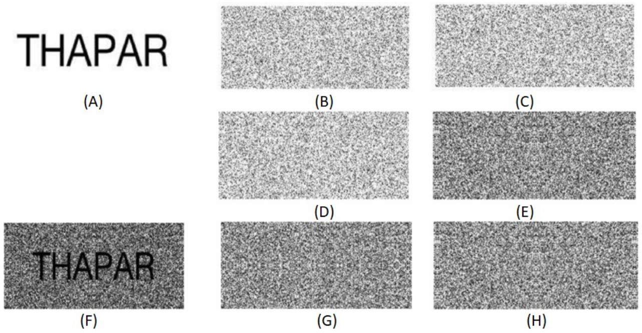


Fig. 6. The 3-out-of-3 VCS using the image SI_2 (a) SI_2 (b) S_1, (c) S_2, (d) S_3, (e) $S_1 + S_2$, (f) $S_1 + S_3$, (g) $S_2 + S_3$, and (h) $S_1 + S_2 + S_3$

$$S^0 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \tag{9}$$

The S^1 basis matrices for 3-out-of-3 VCS can be constructed as,

$$S^1 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \tag{10}$$

There are two collections of matrices,C_0 for encoding white pixels and C_1 for encoding black pixels. The matrices C_0 and C_1 can be designed as,

$$C_0 = \pi \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \tag{11}$$

$$C_1 = \pi \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \tag{12}$$

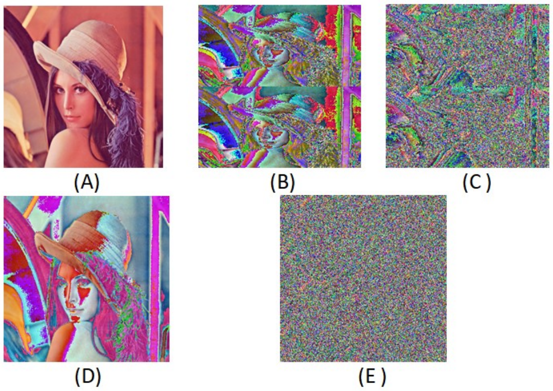


Fig. 7. Construction of 3-out-of-3 VCS for coloured images

V. Algorihm

A. Algorithm for encryption

The proposed algorithm first decomposes the original image into three primitive color images under the subtractive model, namely, R(red), G(green), B(Blue) or C(Cyan), M(Magenta), and Y(Yellow). The Figure 8 presents three primitive color components of the colored image, where each image has 256 levels of the corresponding primitive color, and each pixel represented by three bytes. Converting to (R,B,G), where R,B,$G \in 0-255$ [5].

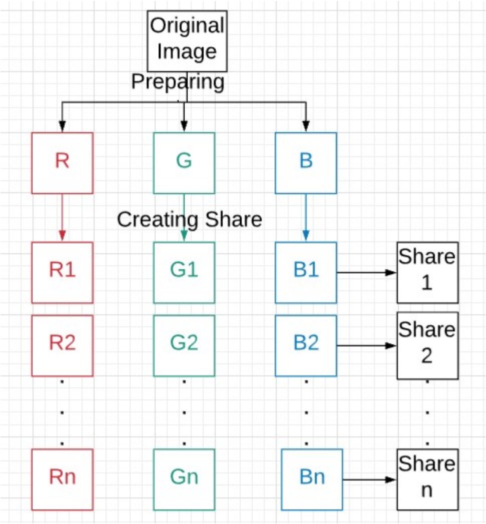


Fig. 8. Algorithm For Encryption

B. Algorithm For Decryption

Decomposing each share image into three primitive color images under the subtractive model, namely, R (red), G(green), B(Blue) and then independent subtractive colors of each share $s_1, S_2, \cdots, S_n$ are stacking over as shown in Figure 9 and, finally making the decrypted image by xoring operation of resultant primitive color images

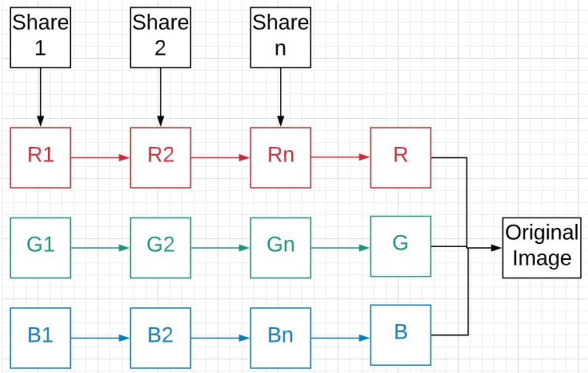


Fig. 9. Algorithms For Decryption

VI. Complexity and Demarits

A. Flow chart of Algorithm

The most important and conceptual problem in visual cryptography is pixel expansion, which results in unnecessarily increase in the dimensional size of secret share image, as any of k or more thank share are to be overlapped. The dimensional size of the share is numerically very large. This results in large computation complexity while performing image processing. [4].

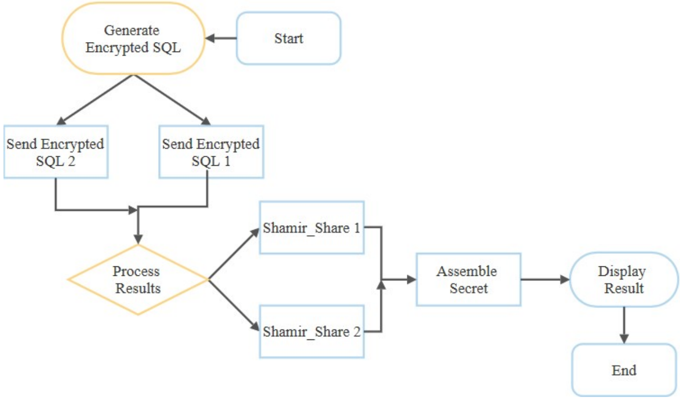


Fig. 10. Figure representing flow chart of algorithm in Shamir Secret Share

This increase in processing time and complexity practically is a limit the use of visual cryptography. The share size problem becomes even worse while maintaining their high resolution of the detailed images. We at end will need image resolution enhancement techniques to restore image size and quality . [4].

As the number of shares associated with a particular secret increases, as well as there is a noticeable increase in the requirement of resources, therefore the management of shares becomes tedious and complex. Large bandwidth requirements are there to limits the use of visual cryptography.
Complexity was improved using utilizing an extra premise lattice for white pixels in VCS and for dark pixels in VCS with PRWP.

B. Limitations

No framework is great, subsequently visual cryptographic additionally has not many confinements and these are written down as follows:

- Contrast Loss:The complexity is separated among the quantity of offers. Since the lesser the difference, lesser will be the natural eye ability to recognize arbitrary pixels and share pixels [5]
- Pixel Expansion: Single-pixel is shared among different pictures. This makes an awkward way to deal with manage. Because of this, pixel size is expanded unnecessarily. [6]
- Large Size Shares: customary visual cryptography plans make shares that are bigger than the elements of the genuine or share picture itself. These bigger offers themselves, difficult to deal with, as immaculate arrangement is extreme is greater offer case. [2]
- One of the primary respectability is Memory wastefulness, If each pixel were seen as a different share, each the produced shadow would have indistinguishable pixels from unique and consumed would rise to memory space. During the remaking of the first pictures, would should be utilized $k\times$size of the underlying picture memory space.
By taking gatherings of k pixels shadows of size $1/k$ are gotten starting images.
That is the means by which it is going recreation utilizes as much memory space what amount involves the first picture

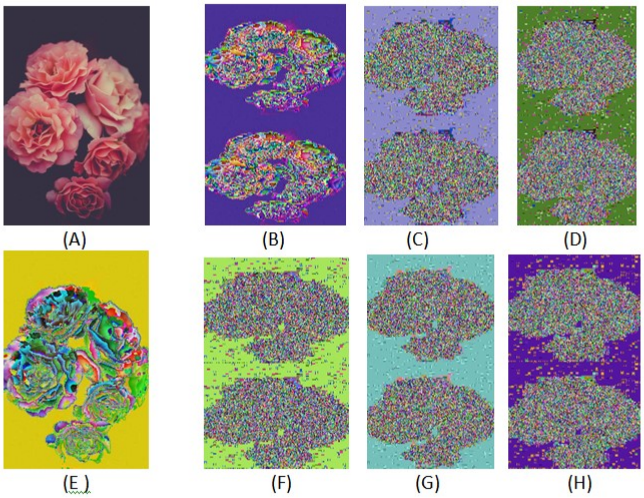


Fig. 11. Construction of 3-out-of-6 VCS for coloured images

- Other respectability is Computational wastefulness .In the event that every individual pixel seen as a share, it would be it is important to perform Lagrange interpolation for each pixel Lagrangian addition is executes the quantity of pixels of the first pictures $/k$ times
- Problem if neighboring pixels are in Homogeneous districts: In the event that the first picture has homogeneous districts, happens that the shadows resemble the first.
- The likelihood of recreation without information on k parts is, the place x and y measurements of the picture, so it is for all intents and purposes difficult to play out the reproduction without k parts
- The execution time of the calculation relies upon the picture measurements, k, and n.

VII. Conclusion And Future Scope

A. Conclusion

The significance of data security in advanced applications and the ideas of cryptography, steganography, advanced watermarking, share sharing, and visual cryptography is well known. A thorough survey of material on visual cryptography and research works done by different scientists in this subject has additionally been finished. This postulation concentrated on the issues of visual cryptography, for example, improvement of complexity, security, and uses of visual cryptography plans. Visual cryptography plans dependent on recursion and mixture method for the upgrade of security and dependability were additionally given point by point test results.

B. Future Directions

There are various problems left unsolved. Some of them like the following, maybe the core issues for future work

- The quality of the recovered secret images is not perfect. In the future, the improvement of the image quality without any additional computation can be considered.
- The design of new access structures for VCS with enhanced contrast.
- Using XOR operation instead of OR will provide the perfect reconstruction of the secret image. Therefore, the implementation of XOR like OR operation in VCS is another issue that can be explored.
- Instead of using adjacent pixels as polynomial coefficients, the image is first divided into k parts.
- Visual cryptography scheme with recursion can be extended to different VCS.
- Design basis matrices for the IP model.
- Quantum Cryptography Will behold as future of advanced cryptography in future.
- Visual cryptography scheme can be applied to different digital applications for tamperproof and reliable transmission of information with low computational capable devices like mobilephone, digital camera, etc.
- Algorithms such as the Advanced Encryption Standard (AES) and the Keyed-Hash Message Authentication Code (HMAC)can be used for the establishment of key between the participating entities.A key-establishment scheme can be characterized as either a key-agreement scheme or a key-transport scheme. The NIST in its recommendation has specifies key-establishment schemes based on the discrete logarithm problem over finite fields and elliptic curves, including several variations of Diffie-Hellman and Menezes-Qu-Vanstone (MQV) key establishment schemes [3] with Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography.

ACKNOWLEDGMENT

I have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organizations. I would like to extend my sincere thanks to all of them. This work would not have been possible without the encouragement and guidance of **Dr. Shivendra Shivani**,Department Computer Science & Engineering, Thapar Institute Of Engineering And Technology,Paiala. Dr. Shivendra Shivani′s enthusiasm and optimism made my experience both rewarding and enjoyable. Most of the novel ideas and solutions in this work are the result of our numerous stimulating discussions.

I am indebted to sir for providing me the facilities in the department for the completion of my work. I would like to thank to all the faculty members and employees of Thapar Institute Of Engineering And Technology for their support and guidance during my Graduation years. Last but not least, I would like to thank Almight God for all good deeds.

UTKARSH SURYAMAN

REFERENCES

[1] Shamir, “How to Share a Secret”Association for Computing Machinery, vol.22, pp.612, 1979.

[2] M.Naor and A.Shamir, Visual Cryptography, Advances in Cryptology-Eurocrypt94, 1995, pp.1–12.

[3] Barker Elaine and Chen Lily and Roginsky Allen and Smid Miles, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography,” doi:10.6028 NIST.SP.800-56Ar2,2018

[4] R .Ito and H. Kuwakado, and . Tanaka, “Image size invariant visual cryptograhy,” IEICE Transactions on Fundamentals Vol 82 , pp-2172.

[5] S. Haykin, “Digital Communications,” John Wiley and Sons, Vol 2, 1998.

[6] J. Weir and W.Yan,“”Visual Cryptography and its applications”” Jonathan weir and WeiQi Yan and Ventus Publications,2012

[7] https://doi.org/10.6028/NIST.IR.8240,2019 / 2018

[8] Https:// www.wikepeadia.com

[9] C .E. Sahnnon,Communication theory of secrecy systems,Bell System Technical Journal,vol 7,pp 656,1948,

[10] Https:// www.google.com

[11] N. Anusha, P.subba Rao,Visual Cryptography Schemes For Secret Image, International journal of Engineering and technology,ISSN, vol 1,2012,

[12] Gorjan Alagic and Jacob Alperin-Sheriff and Daniel Apon and David Cooper and Quynh Dang and Carl Miller and Dustin Moody and Rene Peralta and Ray Perlner and Angela Robinson and Daniel Smith-Tone,“”Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process””,NISTJan2019,https://doi.org/10.6028/NIST.IR.8240,2019,