

Research Article

Visual Cryptography

Aryan Alam Shaikh^a, Dr. Chandrashekhar Mahajan^b

^aB.Tech (Computer Engineering), Vishwakarma Institute of Technology, Pune, India

^bHOD, DESH, Vishwakarma Institute of Technology, Pune, India

Email: ^aaryan.shaikh18@vit.edu, ^bchandrashekhar.mahajan@vit.edu

Abstract

As the use of the web over the world has enlarged to a high level, the safe transmission of the information has become tougher. the protection of the information and data is incredibly necessary for each individual. this is often the explanation why researchers are perpetually concerned in developing new technologies for safe transmission of the information over the web. Several cryptography techniques are discovered and therefore the add this field is sort of unending. one of the best techniques is Visual cryptography. it's a crypto logic technique within which the human sensory system is accountable for the decoding of the visual data, be it an image, text, etc. Visual Cryptography could be an immense space of analysis and is employed in I information activity, color imaging securing I pictures, and different such fields. Here, we tend to aim to look towards a complicated version of cryptography named Visual Cryptography. I Visual I Cryptography came up as a singular secret writing method for data security. It uses pictures rather than texts. An awfully special feature of this method is that the decoding of the encrypted image is finished via the human vision only if I the I right key of image is used. The secret image is reworked into many I share pictures during this procedure. These I shared pictures are I meaningful however distorted. the original image I may be recovered by the union of those shared pictures.

Keywords: *Visual Cryptography*

Introduction

As delineated above, Visual Cryptography could be a special crypto logic technique that eliminates the need for a computer because the method of decoding becomes automatic. This theme is employed to share the key image by an awfully completely different technique. It divides the image into n distorted, secure, meaningful shares, out of that k shares are combined together to get back the key. If you're given, any variety of shares less than 'k', the decoding won't be potential and hence secret image won't be recovered. Most significantly the simplest part of the crypto logic technique is that it doesn't need complicated mathematical computation because it is predicated on HVS or Human Visual system.

Moving towards the history of visual cryptography, it absolutely was invented in 1994 by Naor and Shamir. They fabricated I a straightforward however a safe technique that permits the secret sharing of pictures with no crypto logic complicated computation. The concept was - "An image is nothing however a group of black & white pixels which are treated I independently".

In the visual crypto logic model delineated in [1], the key image ought to be sent to n completely different people. The key image is split into n shares. So, if m shares are placed along, the image can be recovered. If the obtainable shares are not m then the image is invisible. This makes positive that the key image is looked upon as a group of black and white pixels. The specialty of this technique was that any n-1 shares don't seem to be capable of recover I the key image. Once all n shares were combined, the initial image might be visible.

Let us take an associate example, in figure 1, a secret image is first split into 2 shares. Once these shares are stacked along the image is recovered.

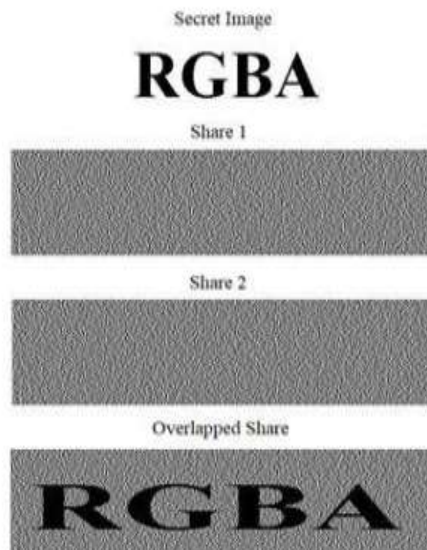


















Fig1: An example of Visual Cryptography

Visual Cryptography is applicable to Binary Pictures, Grayscale Images and Colored Images. The strategy given by Naor and Shamir, for transmission of a secret binary picture was by using their cryptography table. All through the technique, the binary picture is part into two shares, for the white part inside the key picture, one from the upper two columns of table I is picked to make share 1 and share 2. Pixel extension is the primary element, during which each pixel of the key picture is reached out to four pixels. Along these lines, the recovered picture winds up four times the underlying secretpicture since the pixels were reached out to four pixels. By superposition of all shares along a fourfold, bigger picture than the underlying secret image was created. In any case, the standard of the goals was degraded in the reconstructed image than the original secret picture because of the deterioration of each white pixel.

Table I Combination of share 1 and share 2

Original image	Pixel value	Share1	Share2	Share1 + Share2
	0			
	0			
	1			
	1			

The review of various works done in this area has been covered in section II of this paper. The next section is all about the comparison of various schemes studied so far. Section IV summaries the paper and derives a conclusion. And finally section V contains the references used.

RelatedWork

In 1994, the visual cryptography subject was anticipated by Naor and Shamir [1]. This proved to be a significant subject of visual cryptography in which the first picture is part into two shares. When these shares are stacked on, it delivers the essential secret image. This subject is only for Black & White images. Naor, M, and Shamir were the father of Visual Cryptography. They built up a fresh out of the box new hypothesis that presented the methodology of cryptography that structures the base of visual cryptography. The main form of hypothesis expect that the secret could be a blend of dark pixels and bright pixels, and furthermore the message is dispersed among n members. After that, message is cut up into n partakes in such a manner, on the off chance that, k scope of transparencies is characterized, at that point the message ends up noticeable through HVS. Be that as it may, such a subject experiences pixel broadening for example size of the recuperated secret message isn't steady as of the first. The first coloured visual cryptography theme [3] was planned by Verheul & Tilborg. The shares generated by this theme were senseless. They planned a coloured visual secret sharing theme for restricted colour pictures. Assume the number of colours is (M) at that point each image component inside the secret picture is divided in m areas; each segment is part into m sub pixels and also generates n shares I to m sections. At the point when I the I shares I are I consolidated, the m -color secret picture is found. In the event that m is enormous, at that point the pixel expansion will turn out to be high. Unfortunately, this plan will in general produce numerous squares with huge quantities of dark sub pixels, the visual nature of the recuperated picture is frail and I the I shares I are I trivial. In [4], the coloured secret pictures are spoiled to the following three I channels: cyan, magenta and yellow. And then, halftone strategy is applied to move each channel to the halftone picture as showed up in Figure 3. When decayed, each picture is faltered, so every image has 2 concealing levels (either 0 or 1), quickly explaining the presence of corresponding colour or absence of the same.

Hsien-Chu Shanghai, Hao-Cheng Wang, and Rui-Wen Yu, in 2008, anticipated a subject [7] that focused at making the shares significant and furthermore the size of the recovered picture is twofold of the key image. The algorithmic program has four stages. Right off the bat, from the I given I secret I picture a secret colour halftone I picture I is made. Furthermore, from the coloured I half tone I image the pixels are extracted as essential data to downsize I the I pixels of the key picture I for I encrypting. In the event that elements of the initial secret

image are $N \times N$, at that point, once extricating the odd or even rows that are contemplated as essential qualities, the new dimensions would be $I \times N \times N/2$. The encryption strategy goes in close vicinity to the third step, wherever the shares are created. Where each I share I will I be $I \times 2(N \times N)$. At long last, when these 2 offers are stacked along, key picture would be generated with twofold I the I pixels of the initial picture.

Key fundamentally based method puts on the idea of the general public and private key [12]. On the off chance that someone needs to impart a hundred pictures to someone, he should get 100 shares, one for each image, that is hard to oversee. Along these lines this subject understands this drawback while not the prerequisite of complex calculation, wherein that individual keeps only one shared picture and decodes every single distinctive picture with this share. This share is thought of as "UNIVERSAL SHARE". Figure 5 delineates the idea.

In 2014, a theme [14] was acquainted whose objective was to accomplish key security and secure picture sharing. Complex scientific calculations were familiar which produced an image, going about as a secret picture. This key is produced from the secret picture and a couple of picked verifying pictures (p).

Afterward, in the year 2016 [9], the equipment practical visual cryptography topic was anticipated. It advanced time for picture transmission. The modification of Shamir's equation was done in order to reduce the time.

Proposed Work

Now, we present our answer of the previously mentioned issue. The segment is additionally separated into two segments portraying the (3, 3) - EVCS conspire and the (2, 3) - VCS for shaded pictures. The paper [3] portrays the different procedures of implanting information into a spread picture and a strategy to present randomization in the information. The strategies although are written regarding steganography, are likewise relevant on account of visual cryptography. Give us a general thought of presenting randomization in the information. Notwithstanding, the strategy has the hindrance of presenting pointless calculation at transmission and gathering. Our technique spares this exertion. Also, acquainting a spread picture leads with additional overhead. Our investigations of past work have persuaded that presenting a spread picture not just includes an overhead; it additionally empowers the interloper to apply heuristics and straightforward tasks to remove information like trimming of the picture, extricating the LSB, and so on. Another detriment of utilizing a spread picture is that it gives less ability to the payload (information transmission). This prompts the transmission of increasingly pointless information and gives less security. Our plans beat the different drawbacks associated with spread pictures by keeping away from their utilization. Additionally, our plan spares the additional calculation in the presentation of randomization of information regarding paper [3], by utilizing controlled and methodical randomization with the assistance of key.

In paper [2], the creators have proposed a comparable improvement by an XOR activity. Yet, their model is for high contrast pictures and doesn't use the idea of a key. This gives proof in help to improve by randomizing pixel esteems. In any case, using a key can give methodical randomization and security. Moreover, our technique chips away at shaded pictures.

Our (3, 3) - EVCS plot where creators make three offers and require in any event three offers to recover the mystery picture, with an additional necessity of a key to change the pixel

esteems back to their unique ones. In this plan, a straightforward method to extricate the pixel esteems for various channels with the end goal that the channels are discernable and recovery of the picture after extraction just includes the stacking of various channels. Followed by this segment, our other plan (2, 3) - VCS conspire, were to create three shares and require at any rate two of the offers to recover the mystery picture, with an additional necessity of a key to change the pixel esteems. This plan gives extension to less information transmission and improves unwavering quality in situations where information gathering is to be guaranteed and information transmission isn't an issue. Each area depicts the plan in detail, portraying the calculation, working and a guide to show how it functions.

(3, 3) - EVCS Scheme

The (3, 3) - EVCS for shaded pictures, utilizes the idea of stacking pixel estimations of various channels, in a shading model, and playing out an activity utilizing the way to get the first pixel esteems. The whole strategy is introduced in calculation M. A noteworthy change in contrast with different calculations is utilizing a key to change and recover pixel esteems. To perform such an activity utilizing the key, it must be noticed that the activity is reversible, that is, the area of the capacity (activity), and the scope of the converse of the capacity is comparable. The activity will come up short if such a condition isn't fulfilled. Other than this condition, the three conditions for a (k, n) - visual cryptography conspire likewise apply and are essential. The three conditions are disclosed with the calculation to demonstrate its accuracy. Additionally, the method of guaranteeing the third condition is changed to use the idea of a key.

Before introducing the calculation, a general thought of the working and certain essentials required to comprehend the calculation. Right off the bat, clarify portrayal and model for hued conspire, this paper utilized the RGB shading model to speak to our hued pictures. The diverts present in the pictures are Red, Green, and Blue, in a specific order individually. In this way, every pixel esteem is spoken to as a stacked perspective on pixel estimations of Red, Green, and Blue channel. Each channel is particular and is never combined with different channels during the procedure. Here, the shading obscuring impact by stacking the same pixel estimations of a similar channel, for a useful reason. This is comparative in contrast with paper [2] where this impact is clarified. The key is additionally kept alphanumeric and is changed over to numeric portrayal of range 0-255, for playing out the activity. The key is changed over into the predetermined range by a strategy clarified as method P. The activity considered here is XOR activity, as it is a reversible capacity and gives a parameter to correlation with past work. It must be noticed that the activity for the sole motivation behind examination, as the exhibition of calculations must be looked at on basic parameters. Different activities can likewise be viewed as like XNOR, complementation, and so forth... Our plan is a numerical model and doesn't include utilizing spread pictures. That is the reason; utilize certain consistent qualities to increase with the changed channels which effectively distinguish the channels from one another, during recuperation. To satisfy this reason, the consistent worth must be duplicated with every changed estimation of the channel, so ready to recognize the activity (increase with a steady) from the clamor. Hence, don't require values greater than what can be spoken to in 8-bits. This additionally disentangles calculation as the main reason for existing is for recognizing.

At long last, the conditions for (k, n) - visual cryptography plans hold, which will exhibit in the clarification of the calculation.

Presently, present a technique to change over the given alphanumeric key into $m \times n$ esteems, comparing to the size of a mystery picture of $m \times n$. The arrangement of qualities returned change their relating pixel esteems by playing out an XOR procedure on them. The technique KeyGen() takes an alphanumeric key as a string and the size of the picture and gives as a yield a lot of $m \times n$ numeric qualities. Creators likewise utilize the ASCII character coding to change over the character.

The previously mentioned system changes over the given alphanumeric key into a lot of $m \times n$ esteem, to be XORed with relating estimations of each channel. The technique above fundamentally changes over ASCII character coding esteems into a scope of 0-255. Even though the ASCII values for alphanumeric don't surpass 122, beginning from 48, play out the technique to consistently circulate the created qualities by the capacity referenced in the progression 4.b in the above system. Also, space can likewise be extended to incorporate exceptional characters that are for the most part comprehensive of qualities up to 32 in ASCII character coding.

Next to present our primary calculation relating to the plan $(3, 3)$ - EVCS for colored pictures. Algorithm A is introduced into two sections. The primary arrangement of steps portrays the best approach to change the picture utilizing the key, under the plan. The second portrays the means to recover the mystery picture from the changed picture. Calculation M. Encrypt: takes the hued picture and the key as information and produces a $3(n)$ shares as a yield. While A.b Decrypt: takes the arrangement of parts or shares and the key as data and produces the recovered picture as a product.

Algorithm A

a. Encrypt (picture, key)

Product: $3(n)$ shares

1. Call KeyGen with the parameter as key and size of the picture. Store the outcome in a set called Keys.
2. Play out the procedure on pixel shares by comparing key qualities and store the outcomes in a picture.
3. Separate the picture into channels as Red, Green, and Blue.
4. Change pixel esteems by increasing pixel esteems with relating channel steady.
5. Return the channels as a lot of offers.

b. Decode (shares, key)

Product: recouped mystery picture

1. Call KeyGen with the parameter as key and size of the picture. Store the outcome in a set called Keys.
2. Recoup changed pixel esteems by separating pixel esteem by relating channel steady and store the recognized channels as Red, Green, and Blue, separately.
3. Stack the directs in the grouping of Blue, Green, and Red, with the Red channel as the top.
4. Play out the converse procedure on pixel esteems with comparing key qualities and store the outcomes into their relating channel pixel esteems.
5. Return the recuperated picture.

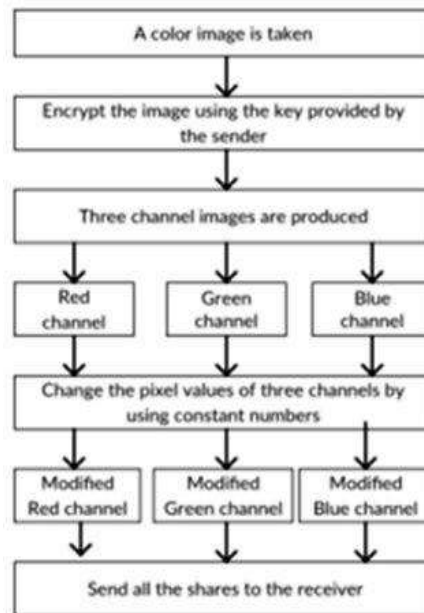


Fig 2: Flowchart for EVCS encoding

A.a depicts the means to make $3(n)$ shares utilizing the $(3, 3)$ - EVCS for hued pictures. The working of the calculation is portrayed in the accompanying sentences. The calculation first calls the method KeyGen to create the arrangement of keys utilizing the key entered by the client and the size of the picture and store them in a set. In sync 2, change the pixel esteems comparing to the estimations of the Keys put away in the set, returned in sync 1. The change is applied to every pixel estimation of each channel. At that point extricate the channels from the picture and apply an individual augmentation on pixel esteems by a steady for the particular channel. This subsequent change is just applied for the simplicity of separating the channels separated, it doesn't fill some other need. To recover the picture totally at the beneficiary's end, must have the option to recognize the various channels. That is the reason, the need of this progression is accentuated. It goes about as an option in contrast to utilizing spread pictures to recognize channels. The last advance is basically to restore these adjusted channels as discrete offers. The figure appeared beneath portrays the stream graph for the calculation M.a.

A.b depicts the means to recuperate the mystery picture utilizing the $(3, 3)$ - EVCS for hued pictures. The working of the calculation is portrayed in the accompanying sentences. The calculation first calls the strategy KeyGen to create the arrangement of keys utilizing the key entered by the client and the size of the picture and store them in a set. In sync 2, recuperate the changed pixel esteems relating to the estimations of the procedure on the first pixel esteems, by separating by the comparing channel constants. In sync 3, stack the diverts in the predetermined request of Red, Green, and Blue, with a red channel being the nearest to the Human Visual System. At that point apply the converse procedure on each channel's pixel part, in the subsequent stage. This subsequent change applied plays out the genuine activity to recuperate the first qualities. The last advance is basically to restore the stacked picture as the recouped picture. The figure appeared underneath depicts the stream outline for the calculation A.b.

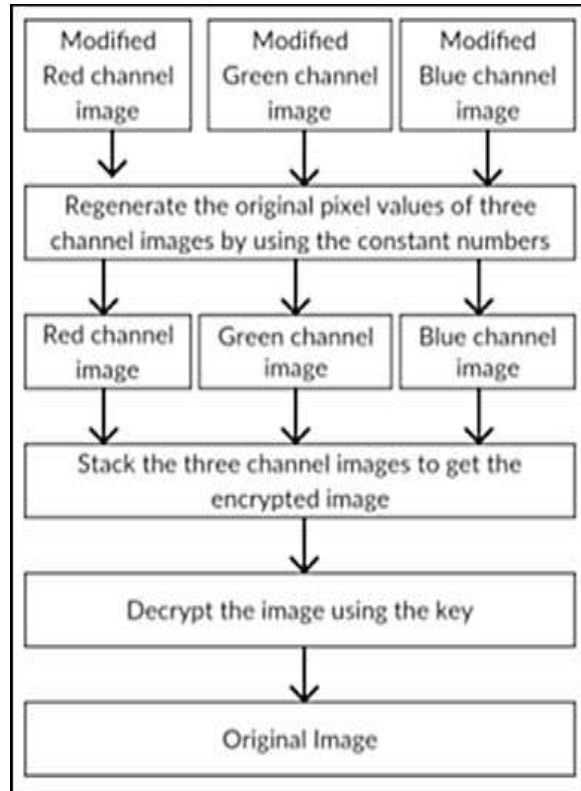


Fig 3: Flowchart for EVCS Decryption

The (3, 3) - EVCS for shaded pictures safely transmits information by randomizing the pixel esteem in a controlled way utilizing a key. The sender can send the picture by scrambling it with a key and the key can be safely transmitted over secure channels. The client may likewise use methods of exchanging key over an unbound channel utilizing secure strategies. The key is the main parameter that keeps the information safe and subsequently, must be safely sent.

1. (2, 3) - VCS Scheme for hued mystery pictures
2. The (2, 3) - VCS for hued pictures creates three channel pictures (for example Red, Green and Blue) in comparable route to that of (3,3) – EVCS plot, however these channel pictures are not transmitted to the recipient straightforwardly. These channel pictures are stacked on one another to shape Red-Green channel picture (RG share), Green-Blue channel picture (GB offer) and Red-Blue channel picture (RB share). Out of these 3(n) shares, just 2(k) shares should be transmitted to the collector. The whole method is introduced in calculation N. Additionally, (2,3) – VCS plot utilizes a similar method KeyGen() to change over the gave alphanumeric key into $m \times n$ esteems.
3. Presently present our primary calculation comparing to the plan (2, 3) - VCS for colored pictures. The calculation N is introduced in two sections. The primary arrangement of steps depict the best approach to change the picture utilizing the key, under the plan. The second depicts the means to recover the mystery picture from the changed picture. Calculation N.aEncrypt: takes the hued picture and the key as an info and produces a 3(n) shares as a yield. Out of these 3(n) shares, just 2(k) are transmitted to the collector end. While, calculation N.bDecrypt: takes the arrangement of offers and the key as an info and produces the recovered picture as an output.

Calculation N

A. Encrypt (image,key)

Info: mystery picture; alphanumeric key

Yield: 3(n) shares

1. Call system KeyGen with the real boundary as key and size of the picture. Store the outcome in a set called Keys.
2. Perform the procedure on pixel esteems with comparing key qualities and store the outcomes in animage.
3. Separate the picture into channels as Red, Green andBlue.
4. Use divert pictures created in Step 3, to produce RG share, GB offer and BRshare.
5. Return the joined channels as a set ofshares.

B. Decrypt (set of shares,key)

Info: set of offers; alphanumeric key

Yield: recouped mystery picture

1. Call methodology KeyGen with the real boundary as key and size of the picture. Store the outcome in a set called Keys.
2. Generate channel pictures (Red, Green and Blue) from the two sharesreceived.
3. Stack the directs in the arrangement of Blue, Green and Red, with the Red channel as thetop.
4. Perform the converse procedure on pixel esteems with comparing key qualities and store the outcomes into their relating channel pixelvalues.
5. Return the recouped secretimage.

The calculation N.a depicts the means to make 3(n) shares utilizing the (2, 3) - VCS forcolored pictures. The working of the calculation is portrayed in the accompanying sentences. The calculation first calls the system KeyGen to create the arrangement of keys utilizing the key entered by the client and the size of the picture and store them in a set. In sync 2, change the pixel esteems comparing to the estimations of the Keys put away in the set, returned in sync 1. The change is applied on every pixel estimation of each channel. At that point extricate the channels from the picture and utilize these channel pictures to deliver RG share, GB offer and RB share by stacking any two channel pictures. The last advance is essentially to restore these joined channels as discrete offers. The figure appeared beneath portrays the stream diagram for the calculation N.a.

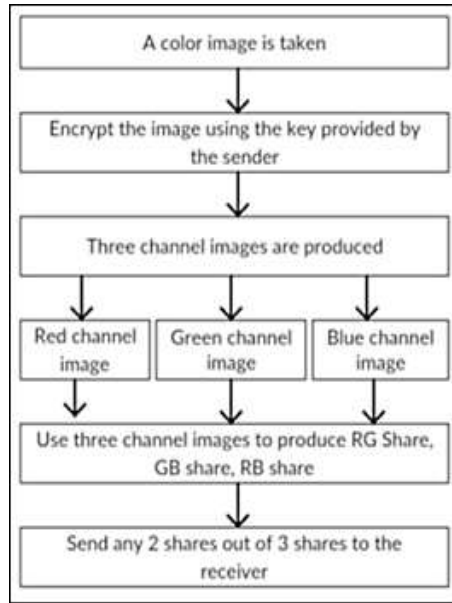


Fig 4: Flow chart for the algorithm N.a

The calculation N.b portrays the means to recuperate the mystery picture utilizing the (2, 3) - VCS forcolored pictures. The working of the calculation is depicted in the accompanying sentences. The calculation first calls the methodology KeyGen to produce the arrangement of keys utilizing the key entered by the client and the size of the picture and store them in a set. In sync 2, create the channel pictures (Red, Green and Blue) by utilizing the 2(k) shares got at the beneficiary end. In sync 3, stack the diverts in the predefined request of Red, Green and Blue, with red channel being the nearest to the Human Visual System. At that point apply the converse procedure on each channel's individual pixel esteem, in the subsequent stage. This subsequent change applied plays out the real activity to recoup the first qualities. The last advance is basically to restore the stacked picture as the recuperated picture. The figure appeared underneath portrays the stream graph for the calculation N.b. N.b.

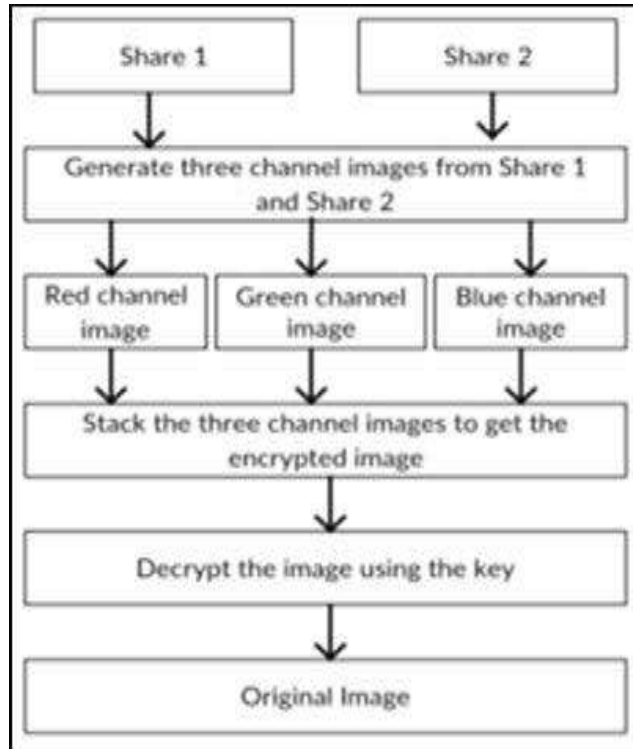


Fig 5: Flow chart for the algorithm N.b

The (2, 3) - VCS for colored pictures safely transmits information by randomizing the pixel esteem in a controlled way utilizing a key. The sender can send the picture by encoding it with a key and the key can be safely transmitted over secure channels. The client may likewise use methods of trading key over an unbound channel utilizing secure techniques. The key is the main boundary that keeps the information safe and thus, must be safely sent. This plan gives degree to less information transmission and improves unwavering quality in situations where information gathering is to be guaranteed and information transmission isn't an issue. The accompanying figure portrays the aftereffects of applying calculation N.a and calculation N.b to a secret image.

Results & Analysis

With the appearance of shared key idea, the security of the visual cryptography process has upgraded and thus the offers are permitted to be dispatched over a similar channel or through various channels. The boundaries, for example, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) are utilized to pass judgment on the optimality of the proposed scheme. Mean Square Error (MSE): The MSE is characterized as the distinction between the pixel estimation of the unscrambled picture and the first picture.

A lower estimation of MSE implies less mistake.

Table 1: Comparative investigation between the proposed plans and the one which was actualized in [5]

Picture Quality Evaluation	Color error diffusion using XOR [5]	3-out-of-3 EVCS	2-out-of-3 EVCS
MSE	125	102.88	117.29

PSNR	27.17	28.0074	27.4379
------	-------	---------	---------

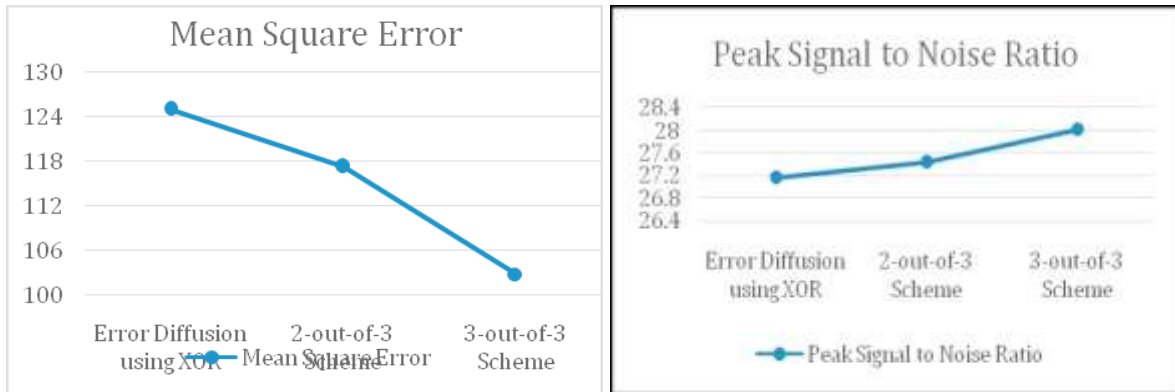


Fig 6: Comparative Analysis of Various Schemes

As PSNR is the opposite capacity of MSE, along these lines higher estimation of PSNR is progressively ideal since it implies that the proportion of Signal to Noise is higher. Here, the 'signal' is the first picture, and the 'clamor' is the mistake in reproduction. Along these lines, a plan with lower MSE and higher PSNR is progressively perfect.

Creators have presented salt and pepper clamor with commotion force 0.005. Clamor needs to beintroduced in offers to pass judgment on the presentation of plan over the channel. Figure 7 shows the estimations of PSNR and MSE for different plans utilizing line diagram.

Conclusion

In regular day to day existence, it is basic to offer security to cutting edge information. Since, Visual Cryptography is one of the frameworks used for mystery sharing of pictures we have concentrated on this method. Visual cryptography is a mystery composing methodology that has the upside of utilizing the human vision to unravel the mixed pictures with no usage of science estimations [10]. In any case, many foreseen plans encounters either pixel widening or the other security issues. The criticalness of coding and translating of the mystery pictures was the point of view behind assessment of visual cryptography procedures during this paper. A couple of components pick which framework or technique to use. An assessment table is given to gather the different choices of each framework evaluated. In this way, by the examination of past work done, we reason that visual cryptography with the help of all inclusive offer is generally unrivaled. It clarifies the matter of finding the opportunity to get a couple of keys to disentangle or recuperate various photographs. Our future work can have viable experience around there; to use an open key to translate different pictures with most outrageous security..

References

[1] Naor, M. and Shamir, A. (1995) Visual Cryptography. In: De Santis, A., Eds., Advances inCryptography—EUROCRYPT'94. EUROCRYPT 1994. Lecture Notes in Computer Science, Vol.950. Springer, Berlin, Heidelberg.

[2] F. Liu, C.K. Wu, X.J. Lin: Color Visual Cryptography schemes, IET Information Security, 2008

- [3] E.R. Verheul and. van Tilborg, Constructions and Properties of k out of n Visual Secret Sharing Schemes, Designs, Codes and Cryptography, Vol. 22(No. 2, pp. 179- 196, 1997.
- [4] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, New Visual Cryptography System on Circular Shadow Image and Fixed Angle Segmentation, Journal of Electronic Imaging 14(3), 033018 (Jul–Sep 2005).
- [5] Askari, N., Heys, H.M. and Moloney, (2013) An extended Visual Cryptography Scheme without Pixel Expansion for Halftone Images.
- [6] Sozan Abdulla, (2010) New Visual Cryptography Algorithm for Colored Image JOURNAL OF COMPUTING
- [7] Hsien- Chu Wu, Hao- Cheng Wang, and Rui-Wen Yu, Color Visual Cryptography Scheme Using Meaningful Shares, achieves a high security level, Proceedings of the Eighth international Conference on Intelligent Systems Design and Applications, pp. 173-178, 2008.
- [8] K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, R. J. Qureshi (2014) Secure Cyclic Steganographic Technique for Color Images Using Randomization
- [9] Shyu, S., Huang, S., Lee, Y., Wang, R. and Chen, K. Sharing multiple secrets in visual cryptography, Pattern Recognition, Vol.40, Issue 12, pp.3633-3651,2007.
- [10] Rola I. Al-Khalid, Randa A. Al-Dallah, Aseel M. Al-Anani, Raghad M. Barham & Salam I. Hajir, (2017) A Secure Visual Cryptography Scheme Using Private Key with Invariant Share Sizes
- [11] <http://www.cs.iit.edu/~agam/cs511/data/images/index.html>.
- [12] Introduction to CRYPTOGRAPHY and NETWORK SECURITY, Behrouz A. Forouzan, McGraw-Hill International Edition
- [13] Hirdesh Kumar , Awadhesh srivastava, A Secret Sharing Scheme for Secure Transmission of Color Images, International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT) 2014