Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 167 (2020) 323–333

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Computational Intelligence and Data Science (ICCIDS 2019)

Enhanced Visual Cryptography: An Augmented Model for Image Security

Jyoti Tripathi[a], Anu Saini [a*] , Kishan [a], Nikhil [a], Shazad [a]

[a]*G. B. Pant Government Engineering College, New Delhi 110020, India*

Abstract

Security of data has become a necessity in today's world. Data as all know is the raw form and information can be extracted from it. Thus, data needs to be secured. This concern becomes even more significant when share information and it mostly constitute of images. As already know that a picture speaks a thousand words, there is no reason not to believe that picture carry the most information. Furthermore, they can be easily manipulated. This paper presents two schemes to secure such information in the form of images. Under the concept of (k, n) - Visual Cryptography, authors present these two schemes to secretly share images, that can be practically used to secure the information sent. The (3, 3) - enhanced visual cryptographic scheme, enhances security of the currently existing (3, 3) - visual cryptographic scheme by utilizing the concept of keys to secure information. Authors also introduce a new scheme, (2, 3) - visual cryptographic scheme. The (2, 3) - visual cryptographic scheme also utilizes the concepts of keys but reduces the bandwidth requirement or increases reliability. This provides us two modes of operation that are more practical than existing scheme. The paper shall discuss the scheme with a schematic analysis and an analysis of its implementation both subjectively and objectively. Using several parameters of security, this paper presents our findings as our results. The schemes discussed are found to be more secure than existing visual cryptographic scheme and are more reliable and imperceptible.

Keywords: Visual Cryptography; Secret key; transformed pixel; (3,3) – EVS;(2,3)- VCS

1. Introduction

Visual Cryptography is a secret sharing scheme that is used to share the secret image by dividing it into n noise-like secure shares which are meaningful, out of which any k shares are stacked together to recover the secret. Given,

Corresponding Author: dranusaini@gbpec.edu.in

10.1016/j.procs.2020.03.232

any number of shares less than k will not be able to reveal the secret. The best part of this cryptographic technique is that it is based on Human Visual System (HVS) and does not requires complex mathematical computation.
In [1], authors devised a simple yet secure method which allows secret sharing without any cryptographic computation. The primary idea was "A secret image consists of a collection of black and white pixels where each pixel is treated independently". The secret image was divided into 2(n) Shares out of which 2(k) were required to recover the secret and this scheme is known as (2, 2)-Visual Cryptographic scheme (VCS). But, this idea was only confined to black and white images. At present however, emphasis is on color images. Fig 1 shows an example of (2, 2)-VCS.

Fig 1. Example of Visual Cryptography

The definition of color visual cryptography is given in paper [2]. The paper mentions three approaches to realizecolor visual cryptography. Our paper focuses on the third approach, which is the most suitable method to implement color visual cryptography. With no pixel expansion involved, our approach stacks pixels of composing color channels to reveal the secret image. At this point, we would like to clarify that color channels refer to the comprising channels in a color model. Two of the color models worth mentioning is RGB (Red, Green and Blue) – color model and CMY (Cyan, Magenta and Yellow) – color model, each comprising of primary colors that make the other composite colors by mixing them in their models respectively. Utilizing these color models, a scheme called (3, 3)-VCS was defined. In this scheme, authors divide the color at each pixel into its comprising primary colors and store them into their respective channels (R, G and B). Three shares are formed each carrying a channel's information. On the receiving end, the individual stacks the channels to regenerate the secret image. This method, however, has the disadvantage that it does not provide any security to the shares. Thus, any person having all three shares can reveal the secret image. Other approaches have been suggested but provide even less security than this scheme.

This paper presents a (3, 3)-EVCS, which enhances the security of the (3, 3)-VCS by transforming the pixel values using a reversible operation with a key. A detailed description is provided in section n. Here also present a scheme a new scheme called (2, 3) – VCS. This scheme is discussed in detail in section n'. Through this scheme, authors hope to provide more reliability during transmission. In addition, the scheme requires only 2(k) shares; this reduces the transmitted data. Therefore reducing bandwidth requirement in a network. Although the scheme provides two advantages, it is required to secure data in this scheme with the help of a key. Both the schemes have an added advantage of eliminating the need of a cover image. By modifying the pixel values in such a way that the data becomes not understandable, simply send the modified image. This reduces the overhead of processing the cover image to extract data, which can be computationally complex.

2. Related Work

For better performance in any cryptographic algorithm, the importance of security aspect is undeniable. In [1] conceived a new theory that lays as the groundwork for Visual Cryptography. The simplest version of this theory assumes that the message is a combination of 2 facets: Black pixels and White pixels, that message is distributed among n participants. The message is sliced up into n transparencies in such a way if k number of transparencies are stacked together, then the message becomes visible through HVS. But, such a scheme is applicable on black and white images only and it also suffers from pixel expansion i.e. size of the recovered secret message is not same as of the original one. Some research has been done in the past that serves visual cryptography scheme for color images. In this section, look into several hypotheses instantiated over the years. In [2] proposed several (k, n) - visual

cryptography schemes for colored as well as black and white images, with less pixel expansion. The results were quite promising, even without the use of concept of keys to enhance security. The construction produced good resolution, contrast and color properties. The construction also did not require Halftone representation or any assistance of any computational devices. The construction was so good that it could be generalized to (k, n) threshold access structure. These points made the research in the paper a significant addition to the (k, n) - VCS, but the pixel expansion is still more as compared to our scheme. Also, the schemes suffered certain disadvantages such as few visible parts of the original image shares were still visible and assumed an extremely difficult to obtain value as given.

In [3] discussed the visual cryptography scheme in which every single pixel of secret image is splitted into subpixels which can still be perceived as single pixel by HVS. Authors have used an input 24-bit bitmap color image which each 3-byte sequence in the bitmap array represents the relative intensities of red, green and blue respectively for image size 256x256 RGB pixel. Transparencies are generated by mixing the R, G and B component of an image with 3/4th pixel component of cover image through OR operation. So, there are 2 major issue related with this scheme. Firstly, an overhead is associated with this methodology which needs to be excluded to improve the overall efficiency. Secondly, the whole reliability of the secret image depends upon the transparencies. If any trespasser has all the 3 shares, then he could easily recover the secret bye stacking up the transparencies. In [4] proposed an extended visual cryptography scheme for using half toned images for creating transparencies. Size of transparencies and resultant image is same as of the original secret image. Andsah and Utama in [5] proposed a system that uses RC4 algorithm which is used to encrypt R, G and B component of secret image each with a different pseudo-random key which is different for each channel. After the encryption each layer must be combine again to produce the visualization.

A more practical and secure cyclic steganographic algorithm for colored images using the concept of randomization with better imperceptibility. But this method is exposed to several vulnerable image processing and statistical attacks such as image cropping, scaling and noise attacks [6].

In [7] suggested a cryptography scheme to encrypt secret image by using the concept of RSA asymmetric key ciphering algorithm. The key generated will consist information about the number of shares and the information about the envelope images. Error diffusion using XOR technique is used for half toning. The quality of the original image depends on the quality of the channel images. The key has to be sent over the network in a secure manner so that it will not be accessible to the intruder.

Authors [8] proposed a similar key scheme as [5] to encrypt halftone color images by generating two shares, random shares and key shares which are of same size as of the original secret image. Shares generated are totally based on private key. The secret color image is revealed by stacking the two shares and exploiting the human vision system.

3. Proposed Work

This section provides the details of the proposed schemes. The section is further divided into two sections describing the (3, 3) - EVCS scheme and the (2, 3) - VCS for colored images. For both the schemes, a significant change of not embedding data in a cover image and in the process save the computation of extracting data from the so formed image. The paper [3] describes the various techniques of embedding data into a cover image and a method to introduce randomization in the data. The techniques although are written in reference to steganography, are also applicable in the case of visual cryptography. Provide us a general idea of introducing randomization in data. However, the technique has the disadvantage of introducing unnecessary computation at transmission and reception. Our method saves this effort. In addition, introducing a cover image leads to an extra overhead. Our studies of previous work has led us to believe that introducing a cover image not only involves an overhead, it also enables the intruder to apply heuristics and simple operations to extract data like cropping of the image, extracting the LSB, etc. Another disadvantage of using a cover image is that it provides less capacity for payload (data transmission). This leads to transmission of more unnecessary data and provides less security. Our schemes overcome the various disadvantages involved with cover images by avoiding their use. Also, our scheme saves the extra computation in introduction of randomization of data in reference to paper [3], by using a controlled and systematic randomization with the help of key.

In paper [2], the authors have proposed a similar enhancement by a XOR operation. But their model is for black and white images and does not utilize the concept of a key. This provides evidence in support to enhancement by randomizing pixel values. However, utilizing a key can provide a systematic randomization and security. Furthermore, our method works on colored images.

Section n'.n' presents our (3, 3) - EVCS scheme where authors make three shares and require at least three shares to regenerate the secret image, with an added requirement of a key to transform the pixel values back to their original ones. In this scheme, a simple way to extract the pixel values for different channels such that the channels are completely distinguishable and regeneration of the image after extraction just involves stacking of different channels. Followed by this section, our other scheme (2, 3) - VCS scheme, where generate three shares and require at least two of the shares to regenerate the secret image, with an added requirement of a key to transform the pixel values. This scheme provides scope for less data transmission and improves reliability in cases where data reception is to be ensured and data transmission is not an issue. Each section describes the scheme in detail, describing the algorithm, working and an example to show how it works.

3.1. (3, 3) - EVCS Scheme for colored secret images

The (3, 3) - EVCS for colored images, uses the concept of stacking pixel values of different channels, in a color model, and performing an operation using the key to obtain the original pixel values. The entire procedure is presented in algorithm M. A significant change in comparison to other algorithms is using a key to transform and regenerate pixel values. In order to perform such an operation using the key, it must be noted that the operation is completely reversible, that is, the domain of the function (operation) and the range of the inverse of the function is equivalent. The operation will fail if such a condition is not satisfied. Besides this condition, the three conditions for a (k, n) - visual cryptography scheme also applies and are necessary. The three conditions are explained with the algorithm to prove its correctness. Also, the way of ensuring the third condition is modified to utilize the concept of key.

Before presenting the algorithm, a general idea of the working and certain prerequisites required to understand the algorithm. Firstly, explain representation and model for colored scheme, this paper used the RGB color model to represent our colored images. The channels present in the images are Red, Green and Blue, in that order respectively. Thus, each pixel value is represented as a stacked view of pixel values of Red, Green and Blue channel. Each channel is distinct and is never fused with other channels during the process. Here, the color darkening effect by stacking same pixel values of the same channel, for practical purpose. This is similar in comparison to paper [2] where this effect is explained. The key is also kept alphanumeric and is converted to numeric representation of range 0-255, for performing the operation. The key is converted into the specified range by a procedure explained as procedure P. The operation considered here is XOR operation, as it is a reversible function and provides a parameter for comparison to previous work. It must be noted that, the operation for the sole purpose of comparison, as the performance of algorithms could only be compared on common parameters. Other operations can also be considered like XNOR, complementation, etc.. Our scheme is a mathematical model and do not involve using cover images. That is why, use certain constant values to multiply with the transformed channels which serve the purpose of distinguishing the channels from each other, during recovery. In order to fulfil this purpose, the constant value must be multiplied with all transformed values of the channel, so that able to distinguish the operation (multiplication with a constant) from noise. Thus, do not require values bigger than what can be represented in 8-bits. This also simplifies computation as the only purpose is for distinguishing. Finally, the conditions for (k, n) - visual cryptography schemes hold, which will demonstrate in the explanation of the algorithm.

Now, present a procedure to convert the provided alphanumeric key into m x n values, corresponding to the size of a secret image of m x n. The set of values returned transform their corresponding pixel values by performing a XOR operation on them. The procedure KeyGen() takes an alphanumeric key in the form of a string and the size of the image; and gives as an output a set of m x n numeric values. Authors also use the ASCII character coding to convert the character

Procedure P:

Input: a string of alphanumeric values in the form of a key; size of the image

Output: a set of m x n numeric values
Procedure: KeyGen(key, size)

1. Convert string to an array (multi-set) of individual characters.
2. Represent each value as their ASCII equivalent and store it in the same array or a different one.
3. Create a new set of size 'size'.
4. For each value i in the array from step 3
    a) Store value of remainder of the division of the index of value i by the length of string, in a temporary variable temp.
    b) Store the value i as a function of temp, index and character value.
5. Return the set of values, created in step 3.

The above-mentioned procedure converts the given alphanumeric key into a set of m x n values, to be XORed with corresponding values of each channel. The procedure given above basically converts ASCII character coding values into a range of 0-255. Though the ASCII values for alphanumeric do not exceed value 122, starting from 48, perform the procedure to uniformly distribute the generated values by the function mentioned in the step 4.b in the above procedure. Besides, the domain can also be expanded to include special characters that are mostly inclusive of values upto 32 in ASCII character coding.

Next present our main algorithm corresponding to the scheme (3, 3) - EVCS forcolored images. The algorithm M is presented in two parts. The first set of steps describe the way to transform the image using the key, under the scheme. The second describes the steps to regenerate the secret image from the transformed image. Algorithm M.aEncrypt: takes the colored image and the key as an input and produces a 3(n)shares as an output. While, algorithm M.bDecrypt: takes the set of shares and the key as an input and produces the regenerated image as an output.

Algorithm M

A. **Encrypt** (image, key)
Input: secret image; alphanumeric key
Output: 3(n) shares

1. Call procedure KeyGen with the actual parameter as key and size of the image. Store the result in a set called Keys.
2. Perform the operation on pixel values with corresponding key values and store the results in an image.
3. Separate the image into channels as Red, Green and Blue.
4. Change pixel values by multiplying pixel values with corresponding channel constant.
5. Return the channels as a set of shares.

B. **Decrypt** (set of shares, key)
Input: set of shares; alphanumeric key
Output: recovered secret image

1. Call procedure KeyGen with the actual parameter as key and size of the image. Store the result in a set called Keys.
2. Recover transformed pixel values by dividing pixel value by corresponding channel constant and store the distinguished channels as Red, Green and Blue, respectively.
3. Stack the channels in the sequence of Blue, Green and Red, with the Red channel as the top.
4. Perform the reverse operation on pixel values with corresponding key values and store the results into their corresponding channel pixel values.
5. Return the recovered secret image.

The algorithm M.a describes the steps to create 3(n) shares using the (3, 3) - EVCS for colored images. The working of the algorithm is described in the following sentences. The algorithm first calls the procedure KeyGen to generate the set of keys using the key entered by the user and the size of the image and store them in a set. In step 2, transform the pixel values corresponding to the values of the Keys stored in the set, returned in step 1. The

transformation is applied on each pixel value of each channel. Then extract the channels from the image and apply an individual multiplication on pixel values by a constant for the respective channel. This second transformation is only applied for the ease of differentiating the channels apart, it does not serve any other purpose. In order to regenerate the image completely at receiver's end, must be able to distinguish between the different channels. That is why, the necessity of this step is emphasized. It acts as an alternative to using cover images to distinguish between channels. The last step is simply to return these modified channels as separate shares. The figure shown below describes the flow chart for the algorithm M.a.

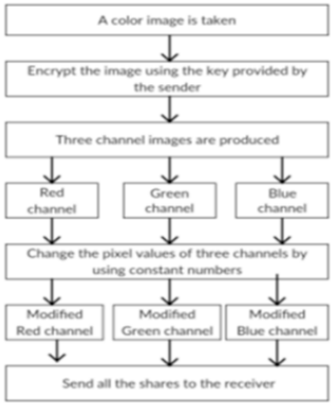

Fig 2: Flow chart for the algorithm M.a

The algorithm M.b describes the steps to recover the secret image using the (3, 3) - EVCS for colored images. The working of the algorithm is described in the following sentences. The algorithm first calls the procedure KeyGen to generate the set of keys using the key entered by the user and the size of the image and store them in a set. In step 2, recover the transformed pixel values corresponding to the values of the operation on the original pixel values, by dividing by the corresponding channel constants. In step 3, stack the channels in the specified order of Red, Green and Blue, with red channel being the closest to the Human Visual System. Then apply the reverse operation on each channel's individual pixel value, in the next step. This second transformation applied performs the actual operation to recover the original values. The last step is simply to return the stacked image as the recovered image. The figure shown below describes the flow chart for the algorithm M.b.

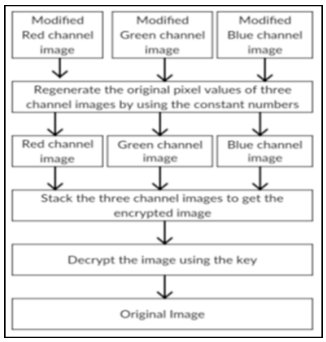

Fig 3: Flow chart for the algorithm M.b

The (3, 3) - EVCS forcolored images securely transmits data by randomizing the pixel value in a controlled manner using a key. The sender can send the image by encrypting it with a key and the key can be securely transmitted over secure channels. The user may also utilize ways of exchanging key over an unsecure channel using secure methods. The key is the only parameter that keeps the data safe and hence, must be securely sent. The following figure depicts the results of applying algorithm M.a and algorithm M.b to a secret image.

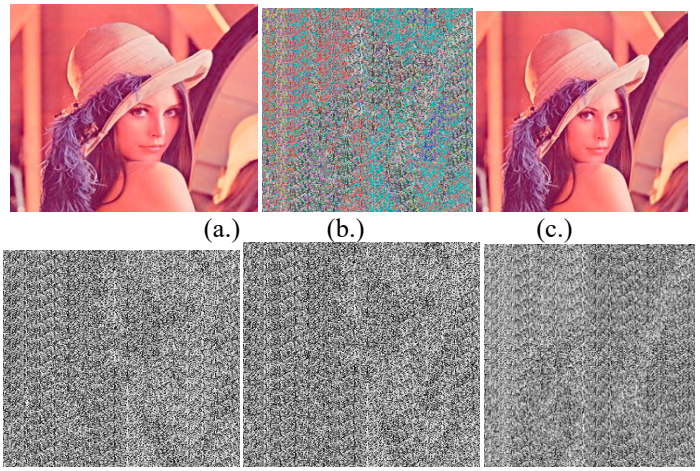

Fig 4: Example of application of (3, 3) - EVCS.

a) Original Image
b) Image after performing operation with the key
c) Decrypted Image
d) Encrypted shares

3.2. (2, 3) - VCS Scheme for colored secret images

The (2, 3) - VCS for colored images generates three channel images (i.e. Red, Green and Blue) in similar way to that of (3,3) – EVCS scheme, but these channel images are not transmitted to the receiver directly. These channel images are stacked on each other to form Red-Green channel image (RG share), Green-Blue channel image (GB share) and Red-Blue channel image (RB share). Out of these 3(n) shares, only 2(k) shares need to be transmitted to the receiver. The entire procedure is presented in algorithm N. Also, (2,3) – VCS scheme uses the same procedure KeyGen() to convert the provided alphanumeric key into m x n values.

Now present our main algorithm corresponding to the scheme (2, 3) - VCS forcolored images. The algorithm N is presented in two parts. The first set of steps describe the way to transform the image using the key, under the scheme. The second describes the steps to regenerate the secret image from the transformed image. Algorithm N.aEncrypt: takes the colored image and the key as an input and produces a 3(n) shares as an output. Out of these 3(n) shares, only 2(k) are transmitted to the receiver end. While, algorithm N.bDecrypt: takes the set of shares and the key as an input and produces the regenerated image as an output.

Algorithm N

A. **Encrypt** (image, key)
Input: secret image; alphanumeric key
Output: 3(n) shares

1. Call procedure KeyGen with the actual parameter as key and size of the image. Store the result in a set called Keys.
2. Perform the operation on pixel values with corresponding key values and store the results in an image.
3. Separate the image into channels as Red, Green and Blue.
4. Use channel images produced in Step 3, to generate RG share, GB share and BR share.
5. Return the combined channels as a set of shares.

B. **Decrypt** (set of shares, key)
Input: set of shares; alphanumeric key
Output: recovered secret image

1. Call procedure KeyGen with the actual parameter as key and size of the image. Store the result in a set called Keys.
2. Generate channel images (Red, Green and Blue) from the two shares received.
3. Stack the channels in the sequence of Blue, Green and Red, with the Red channel as the top.
4. Perform the reverse operation on pixel values with corresponding key values and store the results into their corresponding channel pixel values.
5. Return the recovered secret image.

The algorithm N.a describes the steps to create 3(n) shares using the (2, 3) - VCS forcolored images. The working of the algorithm is described in the following sentences. The algorithm first calls the procedure KeyGen to generate the set of keys using the key entered by the user and the size of the image and store them in a set. In step 2, transform the pixel values corresponding to the values of the Keys stored in the set, returned in step 1. The transformation is applied on each pixel value of each channel. Then extract the channels from the image and use these channel images to produce RG share, GB share and RB share by stacking any two channel images. The last step is simply to return these combined channels as separate shares. The figure shown below describes the flow chart for the algorithm N.a.

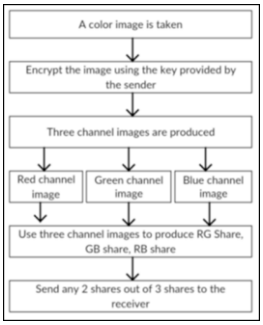

Fig 5: Flow chart for the algorithm N.a

The algorithm N.b describes the steps to recover the secret image using the (2, 3) - VCS forcolored images. The working of the algorithm is described in the following sentences. The algorithm first calls the procedure KeyGen to generate the set of keys using the key entered by the user and the size of the image and store them in a set. In step 2, generate the channel images (Red, Green and Blue) by using the 2(k) shares received at the receiver end. In step 3, stack the channels in the specified order of Red, Green and Blue, with red channel being the closest to the Human Visual System. Then apply the reverse operation on each channel's individual pixel value, in the next step. This second transformation applied performs the actual operation to recover the original values. The last step is simply to return the stacked image as the recovered image. The figure shown below describes the flow chart for the algorithm N.b.

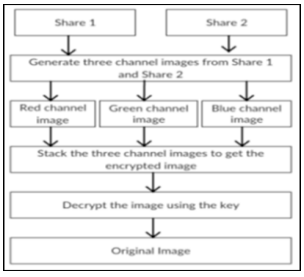

Fig 6: Flow chart for the algorithm N.b

The (2, 3) - VCS forcolored images securely transmits data by randomizing the pixel value in a controlled manner using a key. The sender can send the image by encrypting it with a key and the key can be securely transmitted over secure channels. The user may also utilize ways of exchanging key over an unsecure channel using secure methods. The key is the only parameter that keeps the data safe and hence, must be securely sent. This scheme provides scope for less data transmission and improves reliability in cases where data reception is to be ensured and data transmission is not an issue. The following figure depicts the results of applying algorithm N.a and algorithm N.b to a secret image.

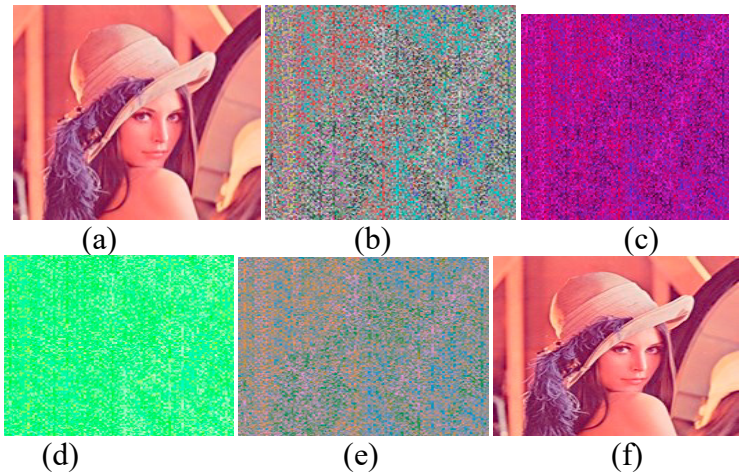

Fig 7: Example of application of (2, 3) - VCS.

A. Original Image
B. Image after performing operation with the key
C. RG share
D. GB share
E. BR share
F. Decrypted image by using GB and BR share

4. Results &Analysis

With the advent of shared key concept, the security of the visual cryptography process has enhanced and hence the shares are allowed to be dispatched over the same channel or through different channels. The parameters such as Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) are used to judge the optimality of the proposed scheme.Mean Square Error (MSE): The MSE is defined as the difference between the pixel value of the decrypted image and the original image.

$$MSE = \frac{1}{MN}\sum_{y=1}^{M}\sum_{x=1}^{N}[I(x,y) - I'(x,y)]^2 \qquad (i)$$

Where I(x,y) is the original image, I'(x,y) is the approximated version (which is actually the decompressed image) and M, N are the dimensions of the images. A lower value of MSE means less error.

Table 1: Comparative analysis between the proposed schemes and the one which was implemented 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

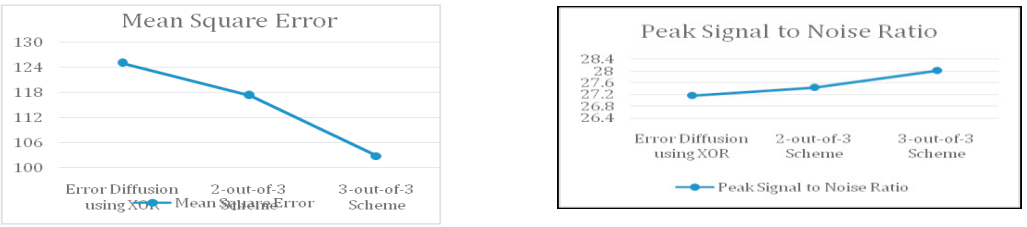

Fig 8: Comparative Analysis of Various Schemes

As PSNR is the inverse function of MSE, thus higher value of PSNR is more preferable because it means that the ration of Signal to Noise is higher. Here, the 'signal' is the original image, and the 'noise' is the error in reconstruction. Thus, a scheme with lower MSE and higher PSNR is more ideal.
Authors have introduced salt and pepper noise with noise intensity 0.005. Noise has to be introduced in shares to judge the performance of scheme over the channel. Figure 7 shows the values of PSNR and MSE for various schemes using line graph.

5. Conclusion

Visual cryptography is an encryption technique that has the advantage of using the human vision to decrypt the encrypted images without any cryptographic computations [8]. But several schemes proposed suffers either from pixel expansion or any other security issue. This paper proposed similar encryption techniques proposed in without pixel expansion and with a shared key concept. Our methods require no overhead and less time for computation during the decryption process. The secret share is encrypted by dividing it two 3 shares depending on scheme imposed. Using 2-out-of-3 scheme for transmission will certainly reduce the time required to decrypt the image for recipient. This idea was never used before perhaps, because the systems did not possess so much processing power. The shares are generated using a key and are recovered using the same key. Our result suggests the fact that security of the scheme critically depends on a shared key and the sum of shares required for regeneration of the secret image.

References

[1] Naor, M. and Shamir, A. (1995) "Visual Cryptography" EUROCRYPT 1994. Lecture Notes in Computer Science, Vol. 950. Springer, Berlin, Heidelberg.

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

[3] Sozan Abdulla, (2010) "New Visual Cryptography Algorithm for Colored Image" JOURNAL OF COMPUTING

[4] Askari, N., Heys, H.M. and Moloney, (2013) "An extended Visual Cryptography Scheme without Pixel Expansion for Halftone Images" 26th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE) : 1-6

[5] Manika Sharma &RekhaSaraswat, (2013) "Secure Visual Cryptography Technique for Color Images Using RSA Algorithm" International Journal of Engineering and Innovative Technology (IJEIT) Volume, 2

[6] K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, R. J. Qureshi (2014) "Secure Cyclic Steganographic Technique for Color Images Using Randomization" arXiv preprint arXiv:1502.07808

[7] AndysahPutera&UtamaSiahaan, (2016) “RC4 Technique in Visual Cryptography RGB Image Encryption” International Journal of Computer Science and Engineering, 3(7): 1-6

[8] 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” Journal of Software Engineering and Applications, 10(01): 1-10