Colour Visual Cryptography (3,3) Scheme

Mandru Manisha[1] ,Dr.G.Siva Nageswara Rao[2]

[1]M. Tech Student, Department of CSE (Cyber Security and Digital Forensics),), KoneruLakshmaiah Education Foundation, VaddeswaramA.P, India, manishamandru@gmail.com
[2]Professor, Department of Computer Science and Engineering, KoneruLakshmaiah Education Foundation, Vaddeswaram, A.P, India, sivanags@kluniversity.in

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract: Visual Cryptography is an encryption technique which performs only encryption in cryptography, and it is used to encrypt every visual data. And this cryptography is different and unique in all cryptographic techniques, because of not performing decryption process mechanically, and that is done mechanically. In normal visual cryptography only black and white images are encrypted. In this paper we propose a different type of visual cryptography scheme for colour imagesin CMY format. And it protects the secret of the original image and no other techniques does not decrypt it except our decryption technique.

Key words: Visual Cryptography, colour images, CMY format, Cryptography.

1. Introduction to cryptography

Cryptography is a technique which is just like an ocean it looks like simple and easy concept to define of to give example just like this “Cryptography protectscontent which is readable by humans by transforming it into unreadable format for human.

And it name explains the definition and work it does is in the word cryptography and it is actually two parts one is "crypt" means hidden and another one is "graphy" means writing. It secures data with the help of different types of codes and different algorithms.

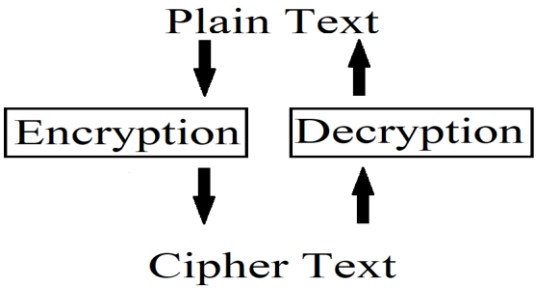

Fig-1: General Procedure of Cryptography

And those different codes and algorithms has the ability to perform both the encryption and decryption operation in their respective ways, to protect the data from unauthorized data access[1].

In cryptography technique security is in four objectives they are Confidentiality, Integrity, Non-reputation, Authentication. In those four objectives confidentiality means the information cannot be accessed by anyone except for authorized people.

Integrity means the information cannot be edited or removed in storage or in transit between both the sending person and receiving person and does not allows any altering to perform on it.

Non-repudiation means the sending personsends the information which cannot be denied at a later stage sender’s intention while sending information.

Finally, Authenticationmeans both the sender and the receiver has to authorize their identity along with the starting point and the ending of the transmission data.

All the cryptographic techniques are classified into three phases and those are Symmetric Key Cryptography, Asymmetric Cryptography, and Hash Functions[2].

In Symmetric key cryptography type both the sending person and receiving person uses same single key to perform both the encryptionand the decryption operations on the sending data.

And in asymmetric key cryptography type both the sending person and receiving person use two different keys one for encryption and another for decryption on the secret data.

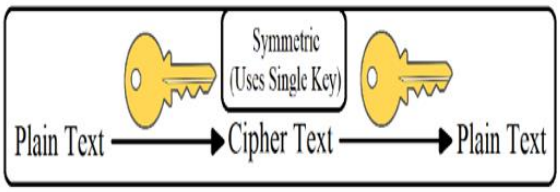

Fig-2: Symmetric Cryptography

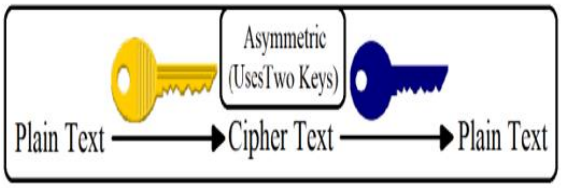

Fig-3:Asymmetric Cryptography

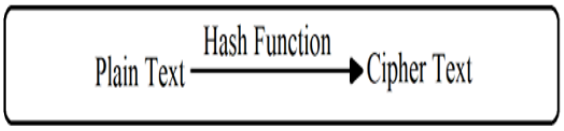

Fig-4:Hash Function

And the remaining last typeis hash functions, here in this type the operation uses hash values instead of keys.

The hash value is a fixed value to any file which has data, by using that value user can find that it is real or edited file.

These are the techniques which are used toperform encryption and decryption operations works only in text formats and other text formats and it does not encrypt the images, signatures etc.

To encrypt the images, pictures, signatures etc there is another technique, and it is called Visual Cryptography.

2. Introduction to Visual Cryptography\

Visual Cryptography is the only technique which is used to protect all types of visual data and it is the most secure technique and it performs encryption only and for decryptionalgorithm is not designed.

But the decryption can be done only in one way just with the help of using human visual system(HVS) after overlapping all the sharesmechanically.

This was created by Moni Naor and Adi Shamir at Eurocrypt'94conference in the year 1994.It is so powerful technique for powerful encryption when we compared with other Technique[3].

Visual Cryptography can be performed on Black&White images, GreyColor images, and Colour images. It helps to encrypt images,signatures,barcode etc.

In this encryption the original image will be converted into unidentified images which are generally called as shadow images.

But in this visual encryption they are called as shares. In image each pixel is broken into given number of equal parts. But in type of colour visual cryptography image is broken into two type either CMY or RGB.

Decryption can be done by combining all shares mechanically which are formed in the encryption process. If all shares are not overlapped properly and equally then original image does not reveal properly and clearly[4]

And to reveal complete and clear image only by using all the encrypted shares of the original image. Just as we can see in Fig 1 how pixel will be broken in colour visual cryptography scheme.

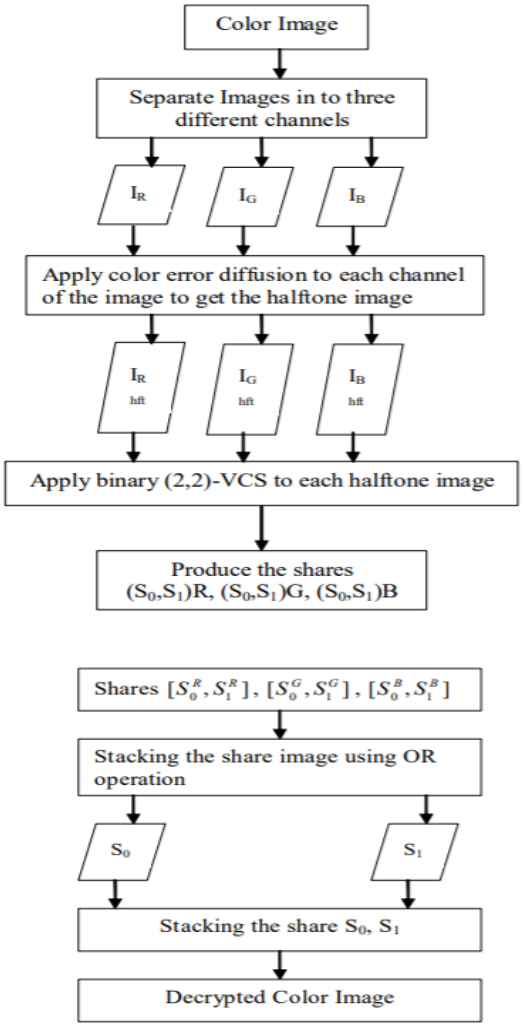

Fig-5:Block Diagram algorithm used in Colour Image Encryption

Mask	Revealed color (C,M,Y)	Share1(C)	Share2(M)	Share3(Y)	Stacked image	Revealed color quantity (C,M,Y)
	(0, 0, 0)					(1/2, 1/2, 1/2)
	(1, 0, 0)					(1, 1/2, 1/2)
	(0, 1, 0)					(1/2, 1, 1/2)
	(0, 0, 1)					(1/2, 1/2, 1)
	(1, 1, 0)					(1, 1, 1/2)
	(0, 1, 1)					(1/2, 1, 1)
	(1, 0, 1)					(1, 1/2, 1)
	(1, 1, 1)					(1, 1, 1)

Fig-6:Pixel Sharing division in colour image

We can see how pixel are divided into 3 shares named as share1,share2 and share 3.Here 0 represent one pattern and 1 represent inverse one pattern. Based upon them the colour will be revealed[5].

The proposal of this scheme authors are Liu F, Wu C.K, Lin X.J proposed three new approaches in this scheme. The new approaches are as follows:

In first method, Shares are printed directly with colour. This works just like the normal visual cryptography, and it leads to some limitations like decoded image quality is reducing and it need large pixel expansion

In second method, there are three colours Red, Green, Blue are used as channels for additive operation and another three colours Cyan, Magenta, Yellow used as channels for subtractive operation.

After this general procedure of visual cryptography which was applied on black & white images is applied to each and every colour channel. This overcome the limitation of pixel expansion by reducing the expansion of pixels, but the image quality is reduced due to the process of halftoning.

In third method, colour to pixels is represented in binary and image is encrypted at bit-level. This method overcomes the other limitation of image quality, and it gives the resultant image in a better quality[6].

3. Existing System

In normal visual cryptography image is broken into equal parts for example lets choose shares count to three[7].

The selected image has to be in black and white for existing system this why I selected an image which contain a password of an account and that is as shown in the following image

Fig-7: Selected Black & White Image

And the above is broken into three equal share which means each and every pixel in the given image will be broken into three equal parts.

The images which will form after breaking the image into three equal parts are called as shadow images and to see the original image user need every encrypted share of the original image.

Even with any two of the shadow images does not generate the original image. By using the duplicate of any one of the two shares as a third share, then also image does not reveal.

And the encrypted images of the selected black and white images are as follows and they are named as share1, share2, share3. In the fig8, fig9, fig10.

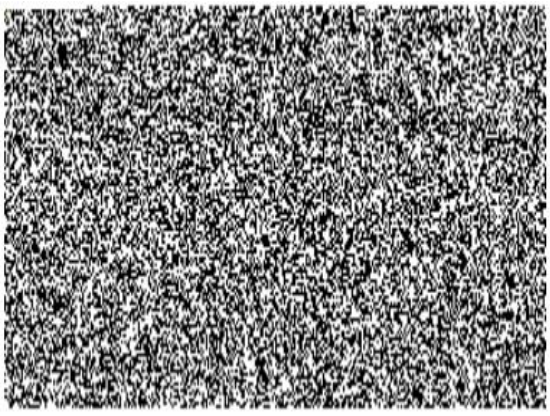

Fig-8:Share1

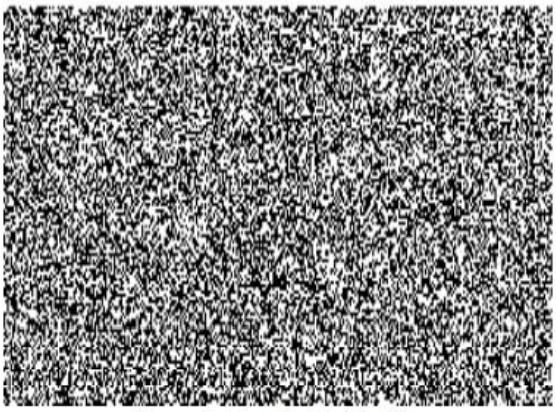

Fig-9:Share2

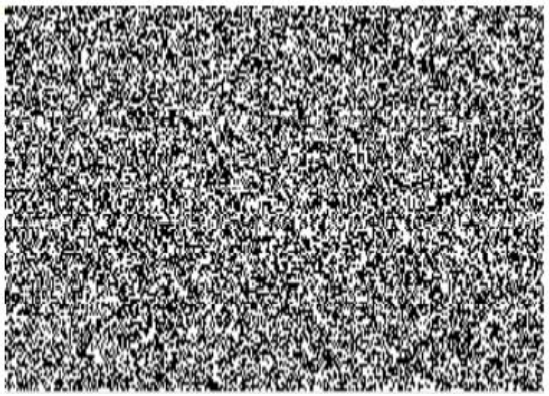

Fig-10:Share3

As I explained previously, we need all the above three shares to reveal the selected image. These shadow image reveal the original image only when they are together placed one by one clearly otherwise not[8].

As a single image they look like an unidentified image which does not have errored pictures.And to perform the decryption in existing system the images has to be place one by one just like the following image fig11.

In the following image encrypted images are placed in order in a super imposed way and then they reveal the image just like the following image.

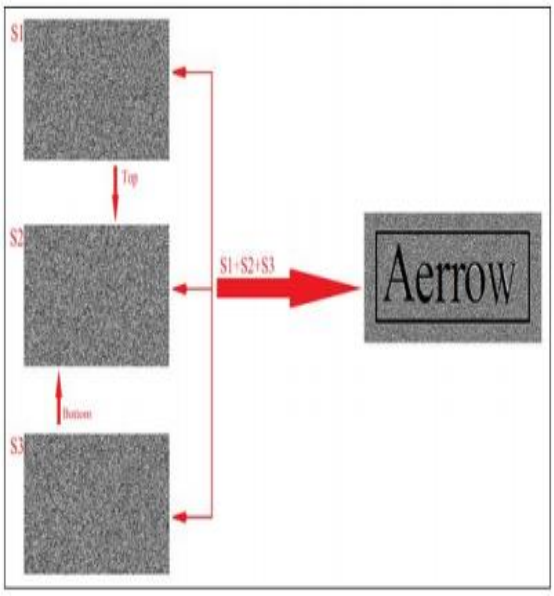

Fig-11: Decryption of Existing System

The problem with the existing system is, it works only on the black and white images even if we gave any colour image it converts that image into black and white.

Then it breaks into black and white shares and in the time of sharing the shadow images able make a little bit data noise and the people who is aware of this concept can identify the shadow image.

But in the concept we proposing that will work on both the colour and black & white images and shadow image of the proposed scheme looks like as a single colour paper and no hacker or the people who is aware of this concept can never be able to detect the data inside it[9].

Not only that it helps by reducing risks of identification of the secret data while transmitting.

3. Proposed System

Generally in this concept of visual cryptography we has many scheme and one of them is color visual cryptogrpahy and it is done in two ways based on computer format colors which we called RGB format and CMY format.

Colour VC allows us to use colour images which has natural colours on them, only to make a good secured framework to provide security to information.

And it reduces the risk of the information will be revealed which was stored in it which was hidden.

In our scheme we used CMY format to perform the secret sharing with visual cryptography and it works in two ways and better not only better than RGB color visual cryptography scheme, it works far better than the remaining visual cryptography schemes.

Because of the unique ness of our work, in our concept we created a decryption code along with encryption process in this color visual cryptography.

And with the help of our work user can share the secret in two different ways like sending in person and able to sent the secret shares in digitally without of getting into attackers hands.

Let us explain properly our proposed sytem to perform the color visual cryptography in three level and we explained them one by one.

As we explained previously visual cryptography performs encryption only but our scheme performs decryption and the decreyption doesn't work on every color scheme, it works only on this scheme.

To start the procedure we need to choose a color photo whether it is a jpg jpeg any other format.

Then we has to paste the image in a directory where code is store because if the image in another directory work will be late and gets complicated while execute. And the selected picture is as follows with the name fig12.

Fig-12: Selected Colour Image

After that we has to divide the selected image into CMY color format with the help of 1stlevelof the scheme is just executing the process of image breaking by giving the selected image to the command.

As a result it breaks the given color image into three parts in three different colors and are as follows shown in the fig13, fig14, and fig15.

Fig-13: Decomposition of Share 1

Fig-14:Decomposition of Share 2

Fig-15:Decomposition of Share 3

After getting the broken images just like the above image for the given image, the images must be halftoned that is the 2nd level of the concept. Halftone means here images are highlighted in quality which helps the user to identify after decrypting the image.

To perform halftone, we has to execute the second part of the project where images will be halftoned and to perform that we just need to execute that part only and doesn't need to add the names of the broken images.

After some time, it gives the halftoned images which looks like as follows just like the images show in the fig16, fig17 and fig18.

Fig-16:Halftoned share1

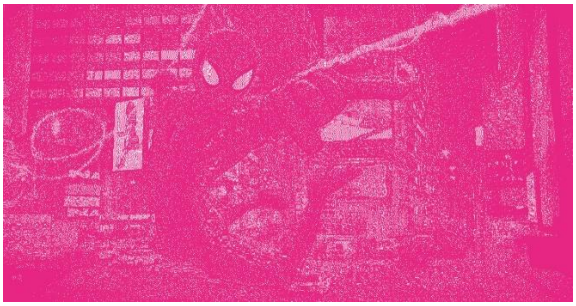

Fig-17:Halftone Share 2

Fig-18:Halftone Share3

After performing the halftoning process the images looks like the above image for the given image and they are ready for 3rd level which is the final process of share creation.

In that process also we have to just like we did previously on the process of halftoning. Which means here also we does not need to give the image name of halftoned images names.

The shares will be generated after performing the final process of the scheme and it will take a little bit of time and the shares which forms after the share creation process and looks like colour images and are as shown in fig19, fig20 and fig 21.

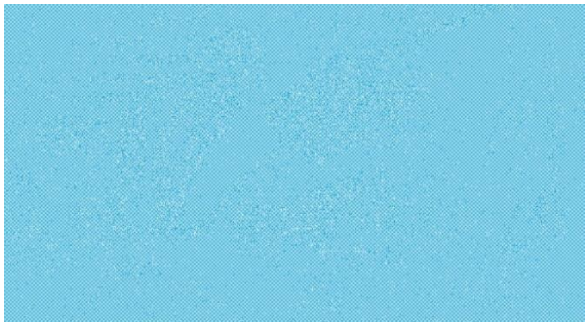

Fig-19:Encrypted share1

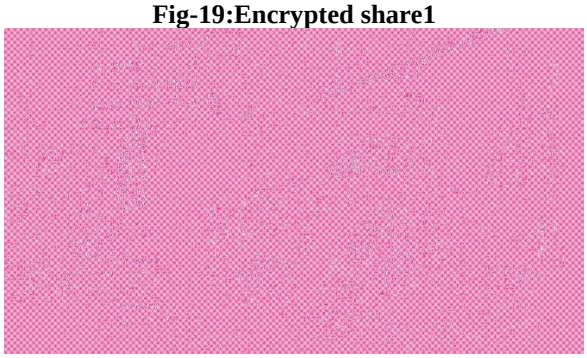

Fig-20:Encrypted share 2

Fig-21:Encrypted share 3

And the share of the colour visual cryptography will be generated just like the above and to decrypt the image which is encrypted user has to take the print out of them in colour and has to overlap one by one constantly and clearly then the image will be decrypted.

That is the only and unique way for the entire visual cryptography to decrypt the image whether it is a colour image or a black and white image[10].

But we also created a decryption code to perform the decryption of the original image by using these sharesand it only work on this scheme only. And it does not work until the user or the known person or the creator of the code gives the command to it.

And in the decryption, it selects only final shares of the scheme and then overlaps in background and generated the final decrypted image of the given original image and it looks likes as follows.

Fig-22:Decrypted Colour Image

The above image is the decrypted image of the original image and this is the image will form by placing all the shares are overlapped.

4. Conclusion

Visual Cryptography is the best way to transfer the files securely in internet. Because most of the data transmission create data noise while transferring and attackers able to identify and see the transferring data easily. And Data transferring with this concept is already working in some areas but all of those areas work only on the black and white images. But our concept will help to transfer the color images also and able to hide the data from the eyes of attackers. Here in our concept we used C,M,Y format decomposition. This concept can replace and secure many of the application works basing on this visual cryptography concept. By the help of this concept, people are aware of this will able to generate many powerful and secured applications like authentication system, identifications, secret sharing, etc.

References

1. Visual cryptography for color images Young-Chang Hou∗ Department of Information Management, National Central University, Jung Li, Taiwan 320, ROC Received 6 June 2002; accepted 26 August 2002
2. International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA Secret
3. Sharing Based Visual Cryptography Scheme Using CMY Color Space Ankush V. Dahata , Pallavi V. Chavan

4. https://en.wikipedia.org/wiki/Visual_cryptography
5. https://geekuniversity.com/uncategorized/confidentiality-integrity-and-availability-cia-triad
6. Encryption and Decryption of Color Images using Visual Cryptography M.Karolin Volume 118 No. 8 2018, 277-281
7. J.Tamilarasi, V. Vanitha, T. Renuka, "Improving Image Quality In Extended Visual Cryptography For Halftone Images With No Pixel Expansion", in International Journal of Scientific & Technology Research, Volume 3, Issue 4, April 2014, pp:126-131
8. Naor, Moni; Shamir, Adi (1995). "Visual cryptography". Advances in Cryptology — EUROCRYPT'94. Lecture Notes in Computer Science.
9. Jiao, Shuming; Feng, Jun; Gao, Yang; Lei, Ting; Yuan, Xiaocong (2019-11-12). "Visual cryptography in single-pixel imaging"
10. Verheul, Eric R.; Van Tilborg, Henk C. A. (1997). "Constructions and Properties of k out of n Visual Secret Sharing Schemes". Designs, Codes and Cryptography
11. Gnanaguruparan, Meenakshi; Kak, Subhash (2002). "Recursive Hiding of Secrets in Visual Cryptography"
12. Kafri, O.; Keren, E. (1987). "Encryption of pictures and shapes by random grids". Optics Letters.
13. G.Siva NageswaraRao, "A logical analysis perspective of Ios devices" in Journal of Advanced Research in Dynamical and Control Systems (ISSN 1943-023X) volume 16, Issue 06, pp 369-386, May 2020.
14. G.Siva NageswaraRao,"An IOT based automatic Accident Detection and tracking system for emergency services" in Journal of Advanced Research in Dynamical and Control Systems (ISSN 1943-023X) volume 12, Issue 02, pp 111-117, March 2020.
15. G.Siva NageswaraRao ,"Design and Implementation of Biomedical device for Monitoring fetal ECG" in journal of Advances in Intelligent systems and computing (ISSN 2194-5357) volume 1108, issue 01, pp 727-734, January 2020.
16. G.Siva NageswaraRao,"Smart Health Care System" in International Journal Innovative Technologies of Exploring Engineering (ISSN 2278-3075) volume 8, Issue 12, pp 4184-4188, October 2019.
17. G.Siva NageswaraRao, "Food Waste Protein sequence analysis using clustering and classification techniques "in International Journal of Advanced tends in computer science and Engineering (ISSN 2278-3091) volume 8, Issue 5, pp 2289-2298, October 2019.
18. G.Siva NageswaraRao,"Modern Vehicle Tracking and Monitoring System using Embedded Technology "in International Journal of Recent Technology and Engineering (IJRTE) (ISSN 2277-3878) volume 8, Issue 1, pp 1849-1851, May 2019.
19. G.Siva NageswaraRao, "A Model for Smart Agriculture using IOT "in International Journal Innovative Technologies of Exploring Engineering (ISSN 2278-3075) volume 8, Issue 6, pp 1656-1659, April 2019.
20. G.Siva NageswaraRao, "Efficient PIMRR Algorithm for Improving scheduling Criteria's in Real Time Systems "in International Journal of Engineering and Technology (ISSN 2227-524X) volume 7, No. 2.32,Special Issue 32, pp 275-278, July. 2018.
21. G.Siva NageswaraRao, "Iot Based Garbage Management System "in Journal of Advanced Research in Dynamical and Control Systems (ISSN 1943-023X) volume 10, Special Issue 04, pp 31-36, April. 2018.
22. G.Siva NageswaraRao, "Airport Language Tracking System using RFID and GSM "in Journal of Advanced Research in Dynamical and Control Systems (ISSN 1943-023X) volume 9, Special Issue 18, pp 748-757, Dec. 2017.