A CRYPTOGRAPHIC APPROACH FOR SECURITY AND PROTECTION OF IMAGE USING BASIC COLOR SPACE

Shubhangi Pathak[1] and Rohit Miri[2]

[1]Dr C V Raman University, Kagi Road Kota, Bilaspur, Chhattisgarh, India
[2]Dr C V Raman University, Kagi Road Kota, Bilaspur, Chhattisgarh, India

***

Abstract: *C*ryptography scheme is now a day most secure techniques for security and protection, that allow the encryption of image or data by transferring it into the secure and protected share and such a scheme is able to recover the secret image or data without any computation devices. In this digital world where we are full of technologies wants to use, transmit and receive our secret image or data in a safe manner. Many number of Cryptography scheme allow encoding the original message to hide its meaning and decode it to reveal the original message.

Also encoding of information in the number of shares and distributed to number of participants, which decrypt information without any cryptographic knowledge. The shares are sent through different communication channels from sender to receiver so that the probability of getting sufficient shares by the intruder minimized. But the shares may arise suspicion to the hacker's mind that passed information is secret. We can encrypt original image using a key to provide more security to this scheme. This make visual cryptography scheme a completely secure scheme. Visual cryptography scheme is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes, and picture) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. There are various measures on which performance of visual cryptography scheme depends, such as pixel expansion, contrast, security, accuracy, computational complexity, share generated is meaningful or meaningless, type of secret images(either binary or color) and number of secret images(either single or multiple) encrypted by the scheme.

Keywords:VisualCryptography,Encryption,Decryption,Shares,Extended Visual Cryptography

1. Introduction

Today, more and more digital documents are transmitted and exchanged on internet. It has created an environment that the digital information is easy to distribute, duplicate and modify. Image security becomes a very important issue for image transmission over the internet or wireless network. Cryptography includes a set of techniques to achieve confidentiality when transmitting or storing data. Cryptography can be categorized into three different scheme s: symmetric cryptography, asymmetric cryptography and secret sharing. Visual Cryptography has made the security of information easier. The traditional symmetric and asymmetric cryptography transform a given message to a random looking string of characters with the aid of a secret or public key. . In contrast to symmetric and asymmetric cryptography, secret sharing is based on the distribution of the secret information over several parties. Only if the required subset of parties put their information together the secret is revealed. The resulting cipher text is supposed to reveal no information on plain text. The decryption of transforming the cipher text back to plain text is employed using the same or different secret key The disadvantage of traditional symmetric and asymmetric cryptographic schemes is that they require complex operational steps for the encryption as well as for decryption of information. For average and inexperienced users, these schemes are rarely convenient to employ . In 1994 MoniNaor and Adi Shamir [1] combined the two mechanisms : secret sharing and traditional cryptography. They introduced a new concept named Visual Cryptography for the encryption and decryption of printed materials such as images or text. The new scheme requires no complex mathematical operations but only the human visual system for the deciphering of a given printed material. The concept relies on transparencies which exhibit a white noise when each transparency is considered separately. The transparencies consist of randomly located white and black pixels. When stacking these transparencies together, the secret image is revealed. The decryption is executed by the human visual system and only the ownership of all transparencies can reveal the secret. The shares generated by the above method are meaningless and look like random dots. With such appearance, they make easy for the attackers to look into shares; whether or not the secrets can be easily cracked open, the looks of the meaningless shares are already revealing the existence of secrets to attackers. When the shares produced are meaningful images, then the attackers cannot find the secret image. A visual cryptography that reveals the target image by stacking meaningful images is Extended Visual Cryptography (EVC)[2] .

Cryptography is a method of protecting confidential information. It encrypts the content of information using some mathematical computation and then the decryption is done to revert back onto the original image and it requires

the use of a secret key. Although we can also use the traditional methods of cryptography to encrypt the images but it is prohibited because of two main reasons:
1. As image size is much greater than that of text, the traditional cryptosystems requires a lot of time to directly encrypt the image data.
2. Also, the decrypted text must be equal to the original text, but due to the characteristics of human perception the decrypted image should not necessarily be equal to the original image as small distortion in image is acceptable as far as human is able to perceive that distortion.
Even with remarkable advances in computer technology, using a computer to decrypt secret image is infeasible in some situations. In these situations, the human visual system is one of the most convenient and reliable technique to do secret recovery. Visual Cryptography was pioneered by MoniNaor and Adi Shamir in 1994. They come up with a visual secret sharing scheme, where an image is divided or broken up into n shares so that only someone with all n shares could decrypt the image, while someone with any n-1 shares can reveal no information about the original image. Each share is printed on a separate transparency (which serve the purpose of secret key) and decryption is performed by overlaying the shares when all n shares are overlaid, the original image gets appeared. Visual Cryptographic is one of the new technique which provides information security and uses the simple algorithm unlike the complex one used in other traditional cryptography. This allows visual information like pictures to be encrypted in such a way that their decryption can be performed by human visual system without any complex computation or algorithms. This is known as (k,n) VCS model where k represents minimum no of shares needed to decrypt the secret image and n is the total number of shares generated by the visual cryptographic scheme.
Hence, the whole Visual cryptographic process can be summarized as.

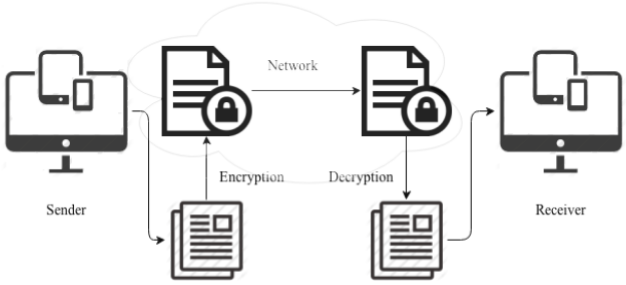


Figure 1. Encryption decryption technique

2.Page Size and Layout

Pixel	Probability	Shares		Superposition of two parts
		№1	№2	
□	$p = 0.5$	◨	◨	◨ White pixel
	$p = 0.5$	◧	◧	◧
■	$p = 0.5$	◨	◧	■ Black pixel
	$p = 0.5$	◧	◨	■

Figure 2. Basic division of Pixel into shares.

3.Title, Authors, Body Paragraphs, Sections Headings and References

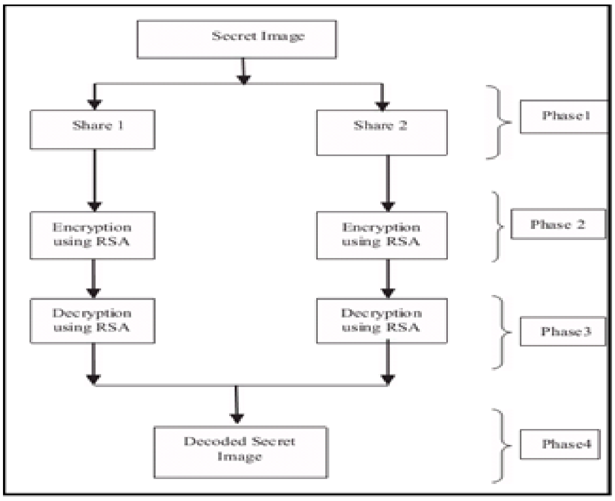


Figure 3. Proposed layout of algorithm

4.OBJECTIVES -

Objective of this project is to hide the original image information from an intruder or an unwanted user. For this the original image converted into the shares and shares will be transmitted to the authenticate receiver over the communication network, the receiver recalculate the secret image by the help of those shares when only they receive all the shares and this is called the decryption process.

The main objective of this project is to provide a security of a message when they are transmitting over the communication network and enhanced the quality of decrypted image.

Objective-

1.To hide original image.

2. To enhance the picture quality.

3. To reduce noise.

4. For security of image.

Different types of losses occurs like:

- Color loss
- Contrast loss
- Noisy image
- Pixel expansion

It is not good to have distortion in color after reconstruction of image. Until now the quality of image being increased in terms of decreasing the pixel expansion, loss less recovery of the image, also making the contrast nearly equivalent to the original image. But the color of the image is not yet preserved while reconstruction.

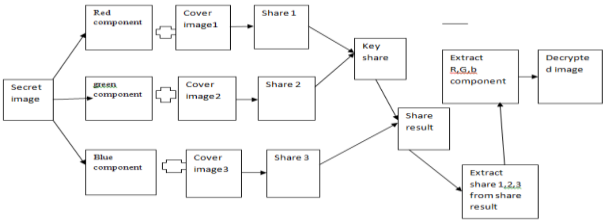


Figure 5. RGB Process

5.Proposed Methodology

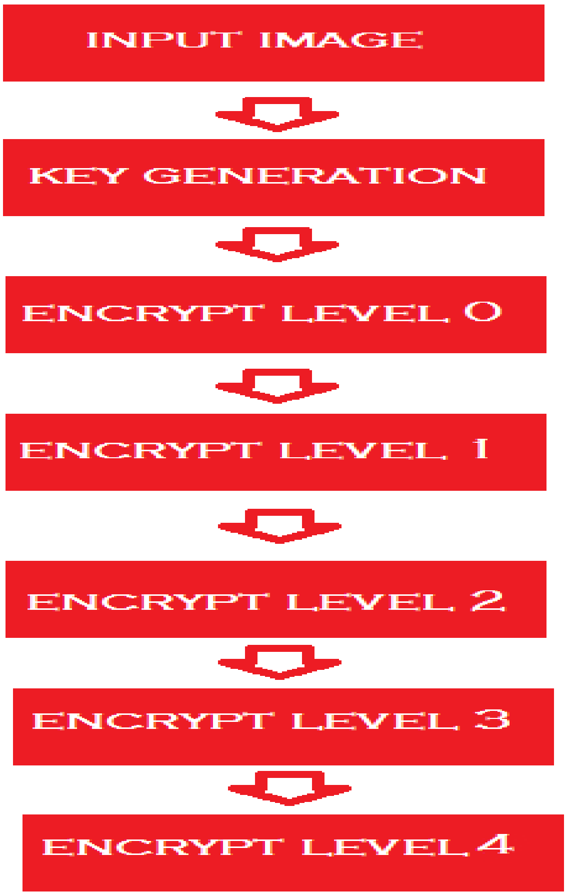
At the very first step we need to select an image for encryption after the selection of image the randomly key pattern is generated from the available keys. The shares are divided into three different parts i.e. Red shares, Green shares and Blue shares. The image intensity, average ration, and generated are individual statistics mean of images. This are shows all three different Red, Green and Blue shares of stand alone properties. The all existing particles from the Red share and the particles of red share will be accumulated as read particles. Two other particles will be also same. Encryption of Green share and Blue share for process term as the 0 level.

The next level is red share is divided into the 8 different red shares in this shares provides high complexity. And other is Green share it is also divided into 8 shares of green and blue share is divided into the same 8 shares.

Other level of encryption is Red, Green and Blue individually colors are combined and processed in to the all present 8 shares and this is processed for all three color i.e. Red, Green and Blue. So we get all 3 shares per individual color Red, Green and Blue are generated into the total of nine numbers of shares.

The next 3rd level process of encryption are available 3 shares i.e. Red, Green and Blue first combined and processed into the single of Red share and the next share is green color are combined into the single share are Green share after that blue share they are followed for the same share of green share and they are combined into the blue color.

The final 4th level of encryption they received the 3 shares of RGB from the previous stages. All RGB which held and combined together and from single share of image.



The staring point to generates the key and then after match with the encryption key and the same time earlier generated the key of encryption.

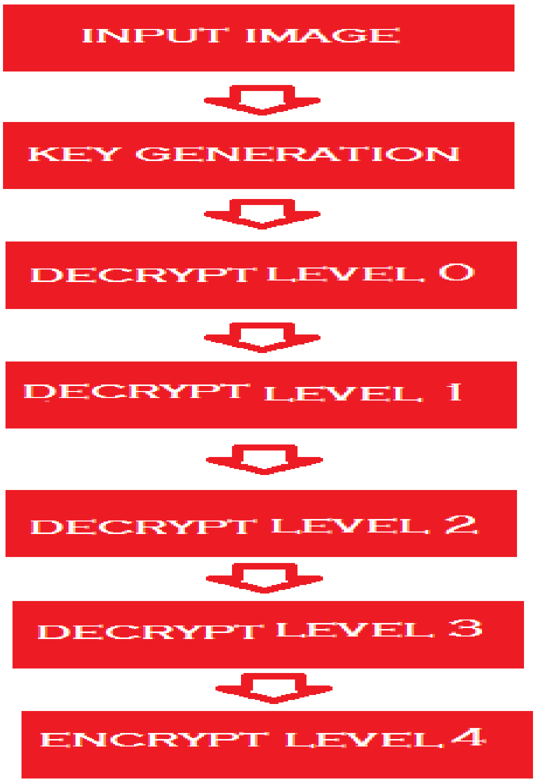
The next level of description which is level 0 they are generated to the key of decryption processing hence after getting the decryption key then we are getting image input and we will continuous follow the same process so we have done level 4 encryption successfully.

there are divide into three different input shares of Red share, Green share and Blue share which is called RGB shares this share provide to input image.

And the next level will be divide into the individual RGB share they are process at the single share. The red share at the present level but it is single and they are further divided in to the three Red, Green and Blue shares individually.. The Green and Blue shares also followed for the same process so each RGB divided in three individual share i.e. RGB shares.

At the level 3 are present individual shares further processed and expanded in the shares per color share from the present 3 share condition there are three share i.e. Red, Green and Blue are expanded individual and red share they are expanded 8 shares and other two shares followed same as Red share.

So the next 4th level is single share they are decomposed and converted into single share per color of all 3 RGB shares are individual shares. the single share are converted into 8 shares of red share which is inherent RGB share, remaining Green and Blue share also followed same as previous Red share. Hence decrypted the input image shows stastics of image as mean of image received.



6. Literature Review

In the year 2014,Ya-Lin Lee and Wen -Hsiang Tsai [28] "A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations" In this paper authors have creating an algorithm where mosaic image are coming out from the result of conversion from secret images using secure image transmission. A key for using mosaic image without any loss the image by secret key. This method is extended by Lai and Tsai , this type of new innovative concept is called secret-fragment-visible mosaic image. The preselected database stored mosaic image through key and output of rearranged secret image in cover of another image is called target image

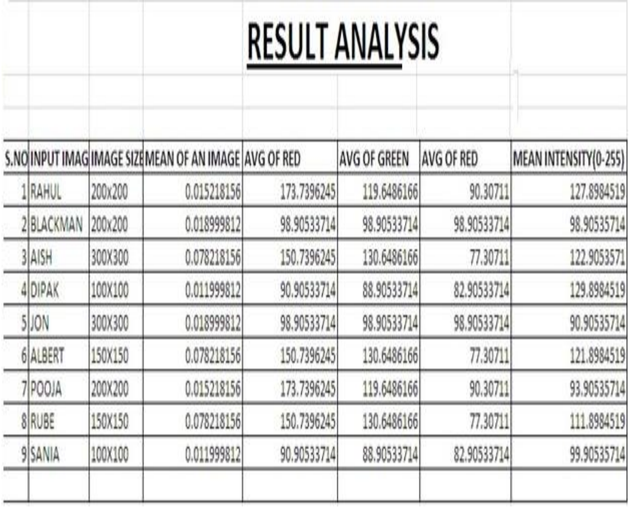
In the year 2014, Bharanivendhan N et al.[29]

Visual Cryptography Schemes for Secret Image Sharing using GAS Algorithm
Image encryption method is called visual cryptography schemes (VCS) that method to hide the secret image secret information encrypted to traditional VCS. There are n number of participants randomly and divided into n number of shares. Using share images are recovered without any problems pixel expansion and Noise problem are involved in previous so there are proposed system involve two phases one is sender side. Using first phase apply GAS algorithm and shares top input secret images are generated. Then after jump to the second phase and share are used in stamping algorithm and distributed algorithm that cover images are done in second phase after starting on the second phase that is receiver side they are extracted the cover image to the share and secret image and align them in particular order. It is also password protected to make this secure, reliable, and increases the number of share to make it more effective that is the problem of pixel expansion will be deducted.

In the year 2015, Prof. Sujit Ahirrao1 , Tusharkumar Sakariya2, Abhijeet Bhokare3, VISUAL CRYPTOGRAPHY SCHEME FOR COLOR IMAGE USING K-N SECRET SHARING ALGORITHM [30]

A powerful tool for encryption technique named visual cryptography is used to secure nad protect personal data by using HVS. This technique shows how and image divides into parts and that part is known as shares. And the n encryption as well as decryption techniques is applied on that shares. In older work decryption technique process is done using HVS which is not very reliable as compare to newer one. Many parts or share are divided from main image. In this paper watermarking is also applied to make this algorithm more secure and more protected.

7.RESULT ANALYSIS CHART



RESULT ANALYSIS

S.NO	INPUT IMAG	IMAGE SIZE	MEAN OF AN IMAGE	AVG OF RED	AVG OF GREEN	AVG OF RED	MEAN INTENSITY(0-255)
1	RAHUL	200x200	0.015218156	173.7396245	119.6486166	90.30711	127.8984519
2	BLACKMAN	200x200	0.018999812	98.90533714	98.90533714	98.90533714	98.90535714
3	AISH	300X300	0.078218156	150.7396245	130.6486166	77.30711	122.9053571
4	DIPAK	100X100	0.011999812	90.90533714	88.90533714	82.90533714	129.8984519
5	JON	300X300	0.018999812	98.90533714	98.90533714	98.90533714	90.90535714
6	ALBERT	150X150	0.078218156	150.7396245	130.6486166	77.30711	121.8984519
7	POOJA	200X200	0.015218156	173.7396245	119.6486166	90.30711	93.90535714
8	RUBE	150X150	0.078218156	150.7396245	130.6486166	77.30711	111.8984519
9	SANIA	100X100	0.011999812	90.90533714	88.90533714	82.90533714	99.90535714

8. Conclusion and Future Work

The previous techniques for final receiving of image transmission image has some drawbacks in degradation. Image transmitted technique there are some problem related in pixel value, less impact of the brightness, contract and sharpness of image they are all picture qualities of image transmission. Using RGB color space has given the solution to these degradations are used in secret sharing based visual cryptography schemes for color preservation with the use of this drawback state previous can be avoided transmitted picture can be quality wise better image are generated. the visual cryptography is lots of scope for exciting research area. Cryptography system are used in there are various scpe of enhancement. Our future work to develop algorithm for quality, reliability, contrast and clarity of final decoded image to quantitative analysis directly decrypted by using visual system by human without using any type of algorithms, so this technique is very fast computing and save more money and time very compatible with color image they are only possible through visual cryptography.

9. References

[1] M. Naor and A. Shamir, "Visual cryptography," Advances in Cry ptology - EUROCRYPT'94, pp. 1-12, 1995.

[2] J. Ida Christy and Dr. V. Seenivasagam, "Construction of Color Extended Visual Cryptographic Scheme Using Back Propagation Network for Color Images", 20 12 International Conference on Computing, Electronics and Electrical Technologies [IC CEET] 978- 1-4673 -02 1 0-41 1 2©20 12 IEEE.

[3] Himanshu Sharma , Neeraj Kumar, Govind Kumar Jha," Enhancement of security in Visual Cryptography system using Cover Image share embedded security algorithm (CISEA)", 978-1-4577-1386-611©2011 IEEE

[4] Zhongmin Wang and Gonzalo R. Arce, "Halftone visual cryptography through error diffusion", ISBN 1-4244-0481-9/06 © 2006 IEEE, pp.109-112.

[5] Digital Image Processing Laboratory: Image Halftoning" April 30, 2006. Purdue University.

[6] J. K. Mandal and Subhankar Ghatak, "Constant Aspect Ratio based (2, 2) Visual Cryptography through Meaningful Shares (CARVCMS)".

[7] Meera Kamath, Arpita Parab, "Extended Visual Cryptography for Color Images Using Coding Tables", 2012 International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-20, Mumbai, India 978-1-4577-2078-9/12 ©2011 IEEE.

[8] Bin Yu, Xiaohui Xu, Liguo Fang, "Multi-secret sharing threshed visual cryptography," CIS Workshops 2007, Harbin, 2007: 815-818.