Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.39 – 46

RESEARCH ARTICLE

XOR-Base Secret Sharing Scheme for Image Database Security

MISS. BHAGYASHREE A. DHAMANDE
Master of Engineering Scholar, Computer Science & Engg, Department
G. H. Raisoni College of Engg and Management, Amravati, India
bdshree28@gmail.com

PROF. SWATI S. DESHMUKH
Guide, Information Technology, Department
G. H. Raisoni College of Engg and Management, Amravati, India
deshmukh.swati05@gmail.com

Abstract- ***This paper emphasize on, how to encrypt image by using XOR Visual cryptography Technique. Here we propose model, which highlights a novel approach of XOR-Base Secrete Sharing Scheme for Image Database Security. It Divide the image in RGB shares and then encrypt each shares. The overall effort of the proposed scheme is the achievement of encrypting and decrypting targeted images. Our objective is to improve security, reliability and efficiency of targeted image using XOR-Base visual cryptography Technique. XOR-Based visual cryptography is capable to overcome the drawbacks of the visual cryptography scheme (VCS).***

Keywords- Visual cryptography, random key generator, XOR-encryption

I. INTRODUCTION

Visual cryptography could be a cryptographic technique that permits visual information to be encrypted in such some way that cryptography becomes a mechanical operation that doesn't need a computer. One among the known techniques has been develop by Moni Naor and Adi Shamir; United Nations agency developed it in 1994. They incontestable a visible secret sharing scheme, wherever a image was divided into n shares in order that solely somebody with all n shares might decode the image, whereas any n − 1 shares unconcealed no information regarding the initial image. Every share was printed on a separate transparency, and cryptography was performed by overlaying the all shares. Once all n shares were overlaid, the initial image would seem. There square measure many generalizations of the fundamental theme as well as k-out-of-n visual cryptography.

Various confidential information like military maps and business identifications square measure transmitted over the web. Whereas victimization secret pictures, security problems ought to be taken into thought as a result of hackers might utilize weak link over communication network to steal information that they need .To deal with the protection issues of secret pictures, numerous image secret sharing schemes are developed.

Secret sharing permits sharing secret information among a group of participants such coding is feasible only if all the participants' square measure gift with their shares. Secret are often divided into any range shares. A locality of secret info is termed a share. Whereas coding the knowledge, it's needed to require all the shares on transparency and so place them in correct order. There square measure numerous secret sharing schemes. Among all on the available, the author targeting two out of two

secret sharing schemes. Two out of two secret sharing schemes separate secret information into precisely two shares. Once these 2 shares square measure ascertained one by one, nobody will reveal the key information. Among 2 shares, one acts as a cipher text and different acts as secret key. However, by rigorously positioning the transparencies, the initial secret message is reproduced. Whereas generating shares, every pixel in original is delineate as a group of pixel in shares.

The word cryptography derived from two Greek words that mean "secret writing". Cryptography is that the method of scrambling the initial text by rearranging and substituting the initial text, transcription it in an exceedingly on the face of it unclear format for others. Cryptography is efficient thanks to defend the data that's transmittal through the network communication path. Cryptography is that the science that deals regarding cryptography and scientific discipline. Cryptography is that the approach of causation the message on the quality technique and firmly to the destination.

Scientific discipline is that the methodology of getting the embedded messages into original texts. In general, cryptography is transferring information from supply to destination by neutering it through a code. The cryptosystems uses a plaintext as Associate in plaintext as input and generate a cipher text mistreatment coding algorithmic program taking secret key as input. Cryptography could be a technique for securing the key information. Sender encrypts the message secrete the key then sends it to the receiver. The receiver decrypts the message to get the key information.

A (k; n) visual cryptography (VC) scheme is a type of secret sharing scheme with the special property that a secret

image can be recovered visually by the human eye and does not require any calculation on a computer. However, the recovered secret image has poor quality. In this case, some developer attempts to consider other different approaches to improve the quality (contrast) of the recovered image. Lee et al. Presented a VC scheme using an XOR method to share a binary image.

II. LITERATURE SURVEY

Following are the papers associated with visual cryptography, used for encrypting the data.

2014: Ching-Nung principle projected [1] to see the relation between OVCS and XVCS. Our main contribution is to on paper prove that the premise matrices of (k, n)-OVCS will be Utilized in (k, n)-XVCS. Meantime, the distinction is increased 2(k−1) times.

2013: Shyong Jian Shyu planned [2] academic degree introduced two novel and effective VCRG-GAS algorithms to resolve the matter of visual secret sharing for binary and color footage. Throughout this paper the algorithms do not want any longer pixel growth. The approach of VCRG relieves the priority of pixel growth, yet its reconstruction ability is not excellent as VCS.

2012: J. United Nations agency Christy and Dr. V. Seenivasagam projected [3] Extended Visual branch of knowledge theme mistreatment Back Propagation Network. There are a unit four main steps among the projected technique.

•In the first step, the three footage unit resized to 0.5 their size. Then the three footage unit transformed to color halftone footage.
•In the second step some useful pixels unit extracted.
•The third step is writing where the key image is encoded among the two shares.
•The last step is that the secret writing procedure where the key image are going to be obtained by overlapping the two shares.

2012: Kulvinder Kaur and Vineeta Khemchandani projected [4] theme generates the VC shares victimization basic Visual Cryptography model so write in code each shares victimization RSA formula of Public Key Cryptography that the key shares square measure unit} on the brink of be safer and shares unit of measurement secure from the malicious adversaries World Health Organization might alter the bit sequences to make the fake shares. Throughout the writing 0.5, secret shares unit of measure extracted by RSA writing formula & stacked to reveal the key image. It consists of generation of shares from secret image victimization VC (2, 2) scheme. Encrypting the generated Shares by the RSA formula. Decrypting the Shares victimization RSA formula.

2012: Meera Kamath, Arpita Parab planned [5] Extended Visual Cryptography for Color footage exploitation committal to writing Tables. There are three steps throughout this algorithm:

• Color Halftone Transformation: each input image is rotten into 3 constituent planes red, inexperienced and blue. Then the halftone technique is applied to each of these planes. By combining these 3 halftone planes, a color halftone image is generated
• Coding and Generation of Shares: A Key Table and 2 forms of committal to writing Tables—Cover Table (CT) and Secret Table (ST) ar used to encrypt the key image into the quilt footage. These encoded cowl footage a pregnant shares and could be transmitted firmly.
• Decryption: within the cryptography technique, we've a bent to stack 2 or further shares in conjunction with the Key Image to reconstruct the key image.

2012: Chun-Yuan Hsiao, Hao-Ji Wang planned [6] use the color model of Ateniese et al. to spice up the image quality of the reconstructed image of Chiu's image secret sharing theme. The aim behind is that a color pixell is employed either as a white or black one, so finding the matter that the share footage do not manufacture (when stacked) enough black pixels for the

reconstructed image. The technical downside of this work is but and where to inject the color pixels therefore every the shares and conjointly the reconstructed footage have top of the range.
2011: Himanshu Sharma, Neeraj Kumar projected [7] Visual Cryptography system victimization cowl Image share embedded security formula. Three phases of projected algorithm:
•First half Image converted into the halftone image by victimization any Half toning technique
•Second half is marked by the generation of embedded footage with the help of compliment footage of the quilt image.
•Third half results of upper than two half is that the new image having some data extract from cowl image and many hidden data extract from secret image.
2009: Zhengxin Fu, Bin Yu projected [8] Schema supported correlative matrices set and random permutation, a different construction of rotation visual cryptography theme (RVCS) has been given. It will be accustomed write four secret footage into two shares. For extending this theme for color image, exploiting color decomposition with high distinction is needed.
2009: Du-Shiau Tsai, Gwoboa Horng, Tzung-Her genus, Yao-TeHuang planned [9] secret image sharing theme for true-color secret footage. among the planned theme through Combination of neural networks and variant visual secret sharing, the quality of the reconstructed secret image and camouflage footage are visually the same as a result of the corresponding original footage.
2008: F. Liu, C.K. Wu, X.J. carver planned [10] color visual cryptography theme beneath the visual cryptography model of Naor and Shamir with no pixel growth. throughout this theme the increase among the vary of colours of recovered secret image does not increase pixel growth.
2006: S. J. Shyu planned [11] more economical colored visual secret sharing theme with part enlargement of [log2c*m] wherever m is that the part enlargement of the exploited binary theme for reducing part enlargement in color visual cryptography theme.
2006: R.Youmaran, A. Adler, A. Abor planned [12] academic degree improved visual cryptography theme for concealing coloured image into multiple colored cowl footage. This theme provides improvement among the signal to noise relation of the camouflage footage by producing footage with similar quality to the originals.
2002: Chin-Chen stream, Tai-Xing Yu planned [13] once additional colors area unit there within the key image the larger the scale of shares can become. To beat this limitation developed a secret color image sharing theme supported changed visual cryptography. This theme provides additional economical because of hide a grey image in several shares. throughout this theme size of the shares is fixed; it doesn't vary once the amount of colors showing within the key image differs. Theme doesn't wish any predefined Color Index Table.
2000: C. Chang, C. Tsai, and T. genus planned [14] color visual cryptography theme for a secret color image a try of important color footage are selected as cowl footage that ar an equivalent size as a results of the key color image. Then per a predefined Color Index Table, the key color footage unit has hidden into a try of camouflage footage. For sharing a secret color image and along to return make a copy with the pregnant share to transmit secret color image.

III. Proposed Methodology

The proposed work is basically a framework design with two modules:

1. Image Encryption.
2. Image Decryption.

3.1. Proposed Image Encryption Method

Algorithm: Image Encryption.

Input: RGB Image.

Output: Encrypted Image.

Step 1: An input image will be selected. It must be RGB Image.

Step 2: Red, Green and blue channels are separated from an input image.

Step 3: Encrypt each channel using XOR based encryption method using 8 bit random key generated by random key generator.

Step 4: Fuse all Red, green and Blue channels to create final encrypted RGB image.

Step 6: End.

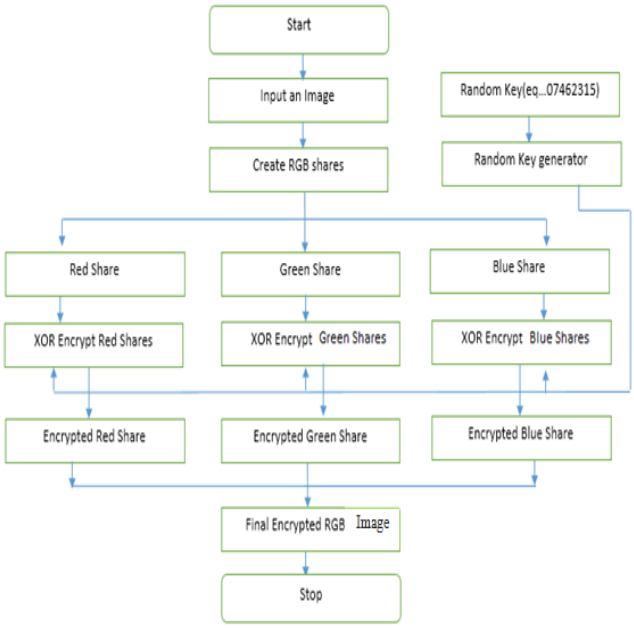


Fig-1 Image Encryption Method

3.2: Proposed Image Decryption Method

Algorithm: Image Decryption.

Input: Final Encrypted Image.

Output: Decrypted Image.

Step 1: Select an encrypted image.
Step 2: Separate Red, Green and Blue channels from an encrypted Image.

Step 3: Decrypt Red, Green and Blue using XOR based decryption method with random key generated by random key generator in image encryption method.

Step 4: Fuse all decrypted image shares to create final resultant decrypted image.

Step 5: End.

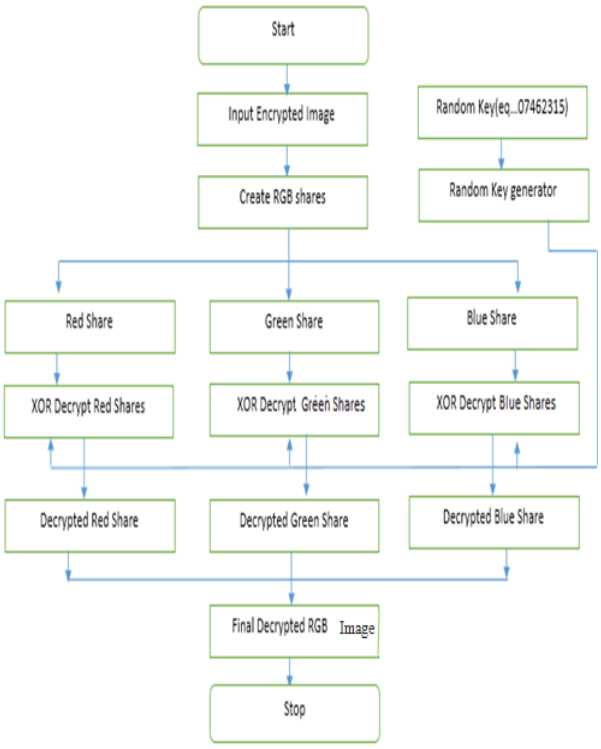


Fig-2 Image Decryption Method

IV. EXPERIMENTAL RESULTS

The implemented method is evaluated on images of different human faces, animals, paintings, Graphical and wave images. To test the image for find loss of pixel between the original image and resultant image.

	Before Encryption		After Encryption	
Input Image	Entropy	Mean Intensity	Entropy	Mean Intensity
Dennis.jpg	17.668	0.38039	17.995	0.4804
Lena.jpg	17.5477	0.43137	17.8538	0.76552
Paint.bmp	17.7892	0.40392	17.9842	0.05588
Image.png	15.2215	0.63137	15.6919	0.498
Sine.gif	14.004	0.1882	14.734	0.49412

Table 1: Entropy and Mean Intensity

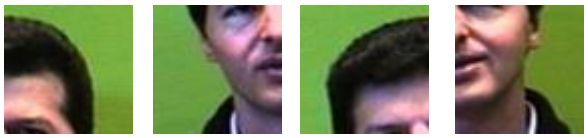
Above table shows that the values of entropy, mean intensity of the images before the encryption are closely similar to the values after the encryption. We have considered the Dennis image as an example in figure 1. We first apply splitting techniques then we apply XOR method on the splitted image using key and then join together to get an encrypted image. Then, it will be decrypted by the same key and XOR method for getting the decrypted image.

Figure 1**:** Input image

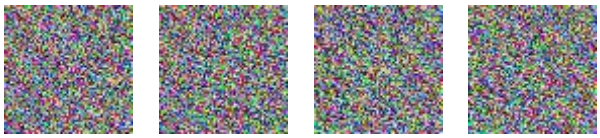
I/p Image	Entropy	Mean Intensity
Dennis	17.668	0.38039

Table 2: Input image

Splitting Input Image into Four Parts shows in below



Encrypt each four parts using proposed method shows in below



Join all encrypted part for generating the final encrypted image

Figure 2: Encrypted input image

Encrypted Image	Entropy	Mean Intensity
Dennis	17.995	0.4804

Table 3: Encrypted Image

Table 2 shows the entropy and mean intensity of the input image and table 3 shows entropy and mean intensity of the encrypted image.

Figure 3: Decrypted image

Decrypted Image	Entropy	Mean Intensity
Dennis	17.668	0.38039

Table 4: Decrypted Image

Mean Intensity = Avg (Red+Green+Blue)/3

In our system, we are calculating mean intensity by taking the average of all R, G and B pixels using above formula.

V. CONCLUSION

Visual Cryptography provides one among the secure ways to encrypt the image. Our Experimental results shows that the values of entropy and mean intensity of the image before encryption are closely similar to the values after encryption. Since the image parameters have not changed much, the method offers a good concealment of image. The proposed method has been employed for applications that require high-security against certain statistical attack. If an image is encrypted with XOR based secrete sharing Visual Cryptography scheme, it provides more security and low computational time. And the method satisfies the requirements of robustness which are intended for visual cryptography. It is simple to implement.

REFERENCES

1. Ching-Nung Yang, "Property Analysis of XOR-Based Visual Cryptography" IEEE Transactions On Circuits And Systems For Video Technology, Vol. 24, No. 2, February 2014.

2. Shyong Jian Shyu,"Visual Cryptograms of Random Grids for General Access Structures" IEEE Transactions on Circuits and Systems for Video Technology, Volume: 23 , Issue: 3 pp: 414 – 424, 2013.

3. 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©2012 IEEE.

4. Kulvinder Kaur and Vineeta Khemchandani "Securing Visual Cryptographic Shares using Public Key Encryption", 978-1-4673-4529-3/12/$31.00c 2012 IEEE.

5. 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.

6. Chun-Yuan Hsiao, Hao-Ji Wang, "Enhancing Image Quality in Visual Cryptography with Colors", 2012 IEEE, International Conference on Information Security and Intelligence Control (ISIC), Page(s): 103 – 106, 2012.

7. 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.
8. Zhengxin Fu, Bin Yu "Research on Rotation Visual Cryptography Scheme" International Symposium on Information Engineering and Electronic Commerce, 2009.

9. Du-Shiau Tsai, Gwoboa Horng, Tzung-Her Chen, Yao-TeHuang, "ANovel Secret Image Sharing Scheme For True-Color Images With Size Constraint", Information Sciences 179 3247–3254 Elsevier, 2009.

10. F. Liu, C.K. Wu, X.J. Lin,"Color Visual Cryptography Schemes" 2008

11. S.J. Shyu, "Efficient Visual Secret Sharing Scheme For Color Images", Pattern Recognition 39 (5) ,pp. 866– 880, 2006.

12. R.Youmaran, A. Adler, A. Miri , "An Improved Visual Cryptography Scheme For Secret Hiding", 23rd Biennial Symposium on Communications, pp. 340-343,2006.

13. Chin-Chen Chang , Tai-Xing Yu , "Sharing A Secret Gray Image In Multiple Images", Proceedings of the First International Symposium on Cyber Worlds (CW.02), 2002.

14. C. Chang, C. Tsai, and T. Chen. "A New Scheme For Sharing Secret Color Images In Computer Network", Proceedings of International Conference on Parallel and Distributed Systems, pp. 21–27, July 2000.

Author Profile

Bhagyashree A.Dhamande received the Bachelors degree in CSE from SIPNA College of Engineering and Technology, Amravati in 2013. She currently pursuing Masters degree in Computer science and Engineering from G. H. Raisoni College of Engineering and management, Amravati.

Swati S. Deshmukh received the Bachelors degree in IT from Sipna College of Engineering and Technology, Amravati in 2010. Her main area of interest includes Image processing and database management system. She received Masters degree in information technology from SIPNA College of Engineering, Amravat in 2013.

