Secret Sharing Using Visual Cryptography

[1]Shweta Maurya, [2]Nidhi Chauhan, , [3]Rajat Singhal, [4]Himanshu Pandey, [5] Prof. G.V. Bhole

[1]Student, [2]Student, [3]Student, [4]Student, [5]Professor

Department of Information Technology

Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune , India

Abstract : For securing visual content like text and images, a new form of cryptography methodology is introduced which requires less computation and is difficult to modify or hack by any intruder. Visual Cryptography provides high security with very low computation. The proposed system takes any image with the key in text form. With the help of key the image is encrypted. The same key will be required to decrypt the unreadable image to the original image at the receiver's side, thus providing additional level of security to the system. In the proposed system, we have implemented the visual cryptography using k-n sharing method and is made more secure using AES(Advanced Encryption Standards) algorithm. The implementation of the proposed system is done with the help of MATLAB tool. MATLAB provides various inbuilt functions and interactive environment for technical computations, graphic, user interface etc.

IndexTerms **- Visual cryptography, k-n sharing, AES algorithm, Image Encryption.**

I. INTRODUCTION

Today, the whole world is dependent on the Internet and hence, millions of files are shared over Internet per day. Among them some are the one which are private and needed to be securely transferred without any intervention or shared without being hacked. Here, then comes the term visual cryptography into picture. Visual Cryptography is the new technique to securely share visual contents like images and text. During encryption, it splits an image into various shares and then those shares are transmitted to the the receiver. Each share is in unreadable form and no one can depict any information by going through any one share. During decryption, those splitted shares are then stacked up to form an informational content. A methodology of k-n sharing was introduced to implement the visual cryptography which encrypts the black and white image. Then many new schemes were introduced which implemented sharing of Colored and Gray images using Visual Cryptography. Image Encryption has many implementation in banking sector, Medical Image processing, etc.

K-N sharing is a technique in which we divide an image into n shares, and among those n shares minimum k shares are required to recover the original image at the receiver's end. It was first introduced by Naor Shamir where the encrypted image can be decoded directly by human individual system[1]. Shares are generated in the form of random noises.

There are many approaches to make the system secure like DES and Chaotic theory. DES uses 64 bit data to generates the secured data. In encryption side the original data is converted to cypher data. In decryption side, the cipher data is converted to the original data. We have used AES over those due to its strength as it has many key size options and its longer block size. AES is chosen over DES because the later one becomes vulnerable to Brute Fore Attack. Chaotic Algorithm was also dropped because it requires hardware to implement encryption process[2].

II. LITERATURE SURVEY

This paper explains the review of literature from various authors. Naor, Moni, and Adi Shamir introduced the encryption of data in secured way and can be easily decoded by human system, they proposed k out of n secret sharing system to transfer imaged securely with their asymptotic construction proved optimal for specific classes of construction.

Nadeem, Aamer, and M. Younus Javed[2] compared the cost of implementation of various encryption algorithms. According to him the encryption algorithm would not be in much use if it is secure but the computation speed is slow.He compared the performance DES, 3DES, AES and Blow-fish encryption algorithms.

E.Verheul and H.V Tilborg[3] proposed the scheme to share the colored images using k out of n secret sharing algorithm and proving definition of k out of n color secret sharing scheme. They also presented various theatrical result on visual secret sharing schemes and specified some applications of colored secret sharing.

Knudsen, Ross Anderson1 Eli Biham2 Lars[4] introduced block cipher as a new candidated for AES which allows efficient implementation. With 128 and 256 bit key it is fast than DES and proved to be more secure than triple DES encryption algorithms.

Vignesh M, Raihana. P. A, Shahadha Hakkim, Sukanya. S[5] proposed a Visual Cryptography system which takes an image to be secretly shared and the encryption is done with the help of a key input by the user. With the help of K-N sharing scheme the shares are produced. The same key is needed to decrypt to the original image.

Venkata Krishna Pavan Kalubandi, et al. [6] proposed a secure encryption algorithm that uses AES and Visual cryptography to secure an image. Further, the crypto-analysis of algorithm was performed and proved to be secure.

Chang, Chin-Chen, Chwei-Shyong Tsai, and Tung-Shou Chen[7] proposed an effective and generalized color image hiding scheme which goes through color index table to recover and hide a secret picture. A camouflage technique was used to encrypt and decrypt the image.

Zeghid, Medien, et al.[8] analyzes the AES and added key streamed generator to AES which improved the encryption performance and detailed results for the security and implementations were given in their paper.

Heidarinejad, Mohsen, Amirhossein Alamdar Yazdi, and Konstantinos N. Plataniotis[9], in their paper introduced cost effective visual cryptography scheme appropriate for color image transmission on top of bandwidth constraint channel.

Lukac, R., and K. N. Plataniotis. [10] proposed scheme to encrypt color image, the required color shares are generated by operating at bit level during encryption.

Yu, Bin, Zhengxin Fu, and Liguo Fang[11] proposed a modified visual cryptography scheme(k,l,n) which analyzes the relation between pixel expansion and range of participants. A much accurate definition of multi secret sharing visual cryptography was introduced.

III. BACKGROUND

Visual Cryptography:

Visual Cryptography is a technique in which the encryption process is done on an image and the result of decryption is also in the image form. It requires relatively less computation for encryption and decryption of the images. One of its best scheme was developed by Moni Naor and Adi Shamir, who developed it in 1994[1]. There are varieties of formats accepted by visual cryptography such as black and white, Gray scale and colored images. Here, we have presented the implementation of visual cryptography for colored images.

For simpler approach, each pixel is subdivided into 4 pixels and according to the color, whether the original pixel is black or white, the subpixels are divided into different shares. For black pixels, the pixel formed by overlapping the 2 layers should be wholly black and for white pixel, the result of overlapping shares must be gray.

One of the simplest implementation is 2 out of 2 sharing scheme, where an image is encrypted divided into 2 shares and both the shares are needed to decrypt the image and get the original sent image. This scheme is further extended to k-n sharing where out of n shares of an image, minimum k shares are needed for the encryption.

Then, a scheme was introduced for colored image sharing by E.Verheul and H.V Tilborg[3]. In colored image sharing an image is represented as an array of pixel k_0, k_1…..k_{c-1}, where 0,1…c-1 are c colour and k_i is the i^{th} color.

AES Algorithm:

Advanced Encryption Standards(AES) is a symmetric block cypher developed by Joan Daemen and Vincet Rijmen in the year 2001. The features of AES are:

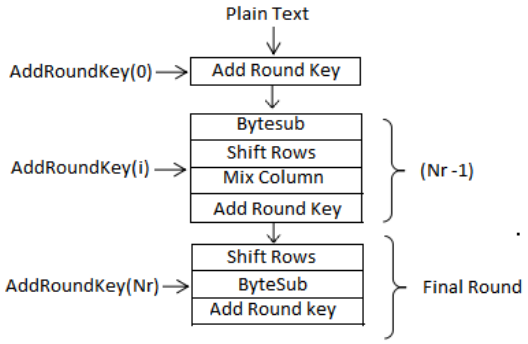
Block size - 128 bit

Key size - 128, 192,256 bit

Rounds - 10(128 bit key size)

12(192 bit key size)

14(256 bit key size)



It performs substitute, Shift rows and Mix columns and Add Round Key operations in each round except the last round where Mix column operation is skipped[4]. AES can be easily implemented in software as well in hardware for cryptography.

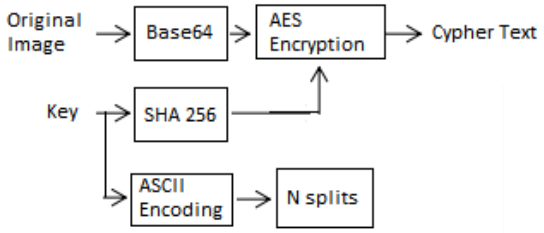
IV. PROPOSED SYSTEM

The AES and Visual Cryptography, individually are prone to various attacks and hence not at all secure for cryptography. But, when used together they form an another level of security and hence become ideal method for cryptography.

RGB values of pixels from the original image is stored in a 4x4 matrix R_M where M is the value of the pixel color M=0,1,….., 255. The image is then divided into n shares and it can be recovered if k shares are bring together k<=n.

Encryption:

The input key is converted to the secret key(SK) using 256 Hashing algorithm where the key of any length is converted to 256 bit string and as it is a one way function, we cannot get the original key from the converted string. Then, with the help of Base64 encoding, the input image is encrypted to BI. The output SK and BI together are fed into AES 256 encryption algorithm and a cypher text is generated[5]. The third step is to split the image to n shares with the help of ASCII encoding[6]. The whole process can be summarized into the following diagram.



1. Read the input image and encode it using Base 256.

2. Read the key and initiate 256 key file.

3. Encrypt the image using base 64 encoded text and hash generated from step 1 and 2.

4. Create a new image C of size (w,h) where,

   w: character support for key file

   h: number of characters in key file.

   p: data pixels to be filled.

5. Repeat for each row i in image

   Let j be the ASCII of i^{th} character in the key.

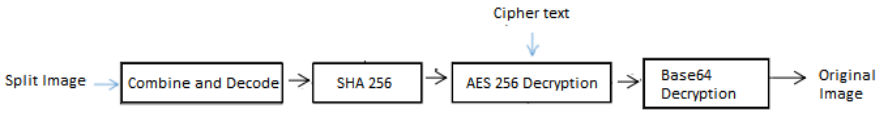
Fill first j pixels in the i^{th} row with black color.

Create N images of the same size(w,h) such that for first image the data is generated randomly and for rest of the images the data is as follows

R[i][j]=C[i][j] xor P[i][j]

Decryption:

Here, two inputs are required. First one is cypher text to be decrypted and the second one is the shares to be combined. The Cypher Text produced at the end of encryption is inputted to AES 265 Decryption along with the secret key after combining the split images and performing SHA 256. The result image is then passed through Base64 Decryption to produce the original image at the receiver side.



1. Read the key
2. Load the shares s where s>=k
3. Create new image with the available shares

   C[i][j]=S1[i][k] xor S2[i][j]

4. Initialize key as array of characters same as the height of the image(CK).
5. For each row i in image repeat:

   Count = 0

   Increment count by 1 for each pixel j in thr i^{th} row.

   Find the character ki, ki=char(count)

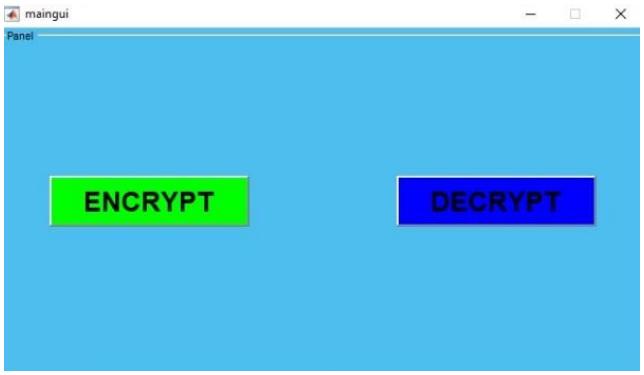
   K[i]=ki

6. Decrypt the cypher text CI and generate I.
7. Output the decrypted image I.

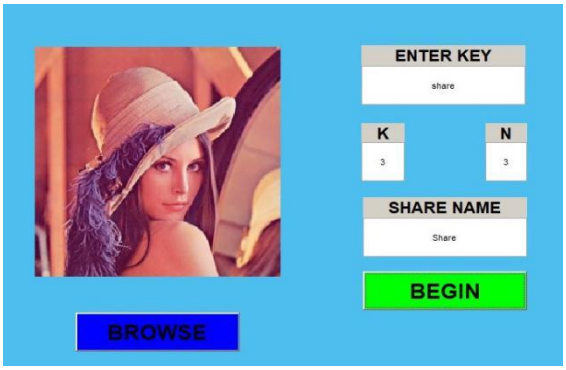
V. USER INTERFACE

For a secret image to be shared, every functionality needed to encrypt and decrypt that image and GUI of the system is implemented in MATLAB. In order to run the GUI, following are the steps:

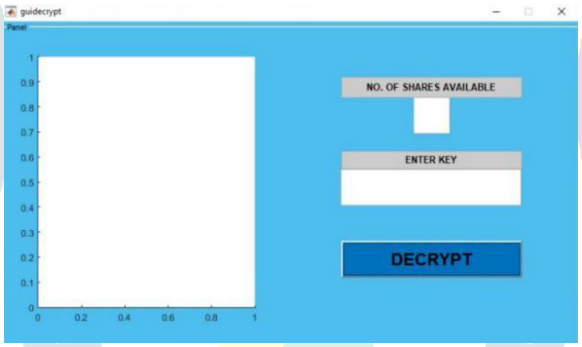
STEP 1: This is the main GUI of our system where the choice to encrypt or decrypt the image is provided.



STEP 2: After clicking the "Encrypt" button below GUI will appear.



STEP 3: To input the image to be encrypted, press the "browse" button to select the image from file selector. Then enter the values of k, n and key. To start the encyption process, press the "begin" button. The shares generated as a result of encryption process will automatically get stored in current MATLAB directory.



STEP 4: In order to decrypt the image at the receiver's end, run the main GUI and press the "decrypt" button which will result in below screen to appear.

STEP 5: Now receiver has to enter the number of shares of encrypted image available at his side along with the same key used to encrypt the original image at the sender's end.To begin the decryption process, press the "Decrypt" button. If the receiver fails to enter the correct key sequence then it will result in another noisy image and the decryption process will be unsuccessful as the original image will not be recovered.

STEP 6: The tracing of the above steps will result in exact duplicate of the original image at the receiver's end and hence, the secret sharing of the image will be done successfully.

VI. CONCLUSION

The cryptography methodology proposed in this paper ensures double layer security. Even if an intruder manages to get the shares, he cannot decipher the image without the availability of cipher. We have experimented various examples on our system by inputting images of various size and qualities, it has been observed that the quality of the decrypted image has not been degraded.

As future work, this scheme can be modified as the quality of the multicolor and gray scale image can be improvised along with the efficiency and speed for generating and combining the the shares.

REFERENCES

[1]. Naor, Moni, and Adi Shamir. "Visual cryptography." *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, Berlin, Heidelberg, 1994..

[2]. Nadeem, Aamer, and M. Younus Javed. "A performance comparison of data encryption algorithms." *2005 international Conference on information and communication technologies*. IEEE, 2005.

[3]. E.Verheul and H.V Tilborg. "Construction and properties of k out of n visual secret sharing schemes" Codes and Cryptography, 1997..

[4]. Knudsen, Ross Anderson1 Eli Biham2 Lars. "Serpent: A proposal for the advanced encryption standard." First Advanced Encryption Standard (AES) Conference, Ventura, CA. 1998.

[5]. Vignesh M, Raihana. P. A, Shahadha Hakkim, Sukanya. S. "An Efficient K-N Secret Sharing Image and AES Image Encryption Algorithm in Visual Cryptography." International Journal Of Advanced Research in Computer and Communication Engineering, Vol. 7, Issue 2, February 2018.

[6]. Venkata Krishna Pavan Kalubandi, et al. "A Novel Image Encryption Algorithm Using AES and Visual Cryptography" 2016 2nd International Conference on Next Generation Computing Technology(NGCT-2016) Dehradun, India, 14-16 October 2016.

[7]. Chang, Chin-Chen, Chwei-Shyong Tsai, and Tung-Shou Chen. "A new scheme for sharing secret color images in computer network." *Proceedings Seventh International Conference on Parallel and Distributed Systems (Cat. No. PR00568)*. IEEE, 2000.

[8]. .Zeghid, Medien, et al. "A modified AES based algorithm for image encryption." *International Journal of Computer Science and Engineering* 1.1 (2007): 70-75.

[9]. Heidarinejad, Mohsen, Amirhossein Alamdar Yazdi, and Konstantinos N. Plataniotis. "Algebraic visual cryptography scheme for color images." *2008 IEEE International Conference on Acoustics, Speech and Signal Processing*. IEEE, 2008.

[10]. Lukac, R., and K. N. Plataniotis. "Colour image secret sharing." *Electronics Letters* 40.9 (2004): 529-531.

[11]. Yu, Bin, Zhengxin Fu, and Liguo Fang. "A modified multi-secret sharing visual cryptography scheme." *2008 International Conference on Computational Intelligence and Security*. Vol. 2. IEEE, 2008.