IMAGE ENCRYPTION FOR SECURE NETWORK TRANSFER

[1] S Kumar Reddy Mallidi, [2] A Kusuma, [3] A Geethika, [4] P Vaheed, [5] S V V Varun
[1]Assistant Professor, [2,3,4,5] UG Student,
Department of CSE,
Godavari Institute of Engineering and Technology, Rajahmundry, India,

Abstract: Now-a-days, most of our data is travelled over internet so the security of that data is most important. Cryptography and Steganography are two important branches of information security. Cryptography provides encryption techniques for a secure communication. Many cryptographic algorithms are available and almost all are suitable for text encryption. Communicating only through text is not possible now-a–days and hence images, audios and videos are used for communication. Steganography involves hiding information in images. Apart from steganography, visual cryptography is widely used for securing transfer of images or visual secrets. One of the efficient methods for visual cryptography is Colour share generation in which the image is divided into shares and in decryption process all shares are stacked together to reveal the secret image. But implementing only Colour share generation will not be that much secured. Still there are some patterns in the Colour shares generated using many of the existing methods. This work proposes a new scheme for visual cryptography using both AES and Colour share generation. In this scheme R, G and B component is extracted from Colour image then apply Visual-AES algorithm on all components and generate an encrypted image. The encrypted image is then divided into Colour shares. At decryption side all shares are combined using Colour share combination and is passed as input to the Visual-AES decryption module to reveal the secret image.

Index Terms **- Colour share generation, Cryptography, Visual AES.**

I. INTRODUCTION

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes the job of the person to decrypt via sight reading. visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. There are several generalizations of the basic scheme including k-out-of-n visual cryptography. Visual cryptography can be used to protect biometric templates in which decryption does not require any complex computations.

II. EXISTING SYSTEMS

Previous efforts in visual cryptography were restricted to binary images which is insufficient in real time applications. Chang- ChouLin, Wen-HsiangTsai [1] proposed visual cryptography for grey level images by dithering techniques. In (k,n) Basic model any ‘k’ shares will decode the secret image which reduces security level. To overcome this issue the basic model is extended to general access structures by G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson [2], where an access structure is a specification of all qualified and forbidden subsets of ‘n’ shares. Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo [3] proposed halftone visual cryptography which increases the quality of the meaningful shares. In halftone visual cryptography a secret binary pixel ‘P’ is encoded into an array of Q1 x Q2 (‘m’ in basic model) subpixels, referred to as halftone cell, in each of the ‘n’ shares. Recursive threshold visual cryptography proposed by Abhishek Parakh and SubhasKak [4] eliminates this problem by hiding of smaller secrets in shares of larger secrets with secret sizes doubling at every step. When Recursive threshold visual cryptography is used in network application, network load is reduced. The researches in visual cryptography leads to the degradation in the quality of the decoded binary images, which makes it unsuitable for protection of Color image, F.Liu, C.K. Wu X.J. Lin proposed a new approach on visual cryptography for Coloured images. They proposed three approaches as follows:

i. The first approach to realize Colour VCS is to print the Colours in the secret image on the shares directly similar to basic model. It uses larger pixel expansion which reduces the quality of the decoded Colour image.

ii. The second approach converts a Colour image into black and white images on the three-Colour channels (red, green, blue or equivalently cyan, magenta, yellow), respectively, and then apply the black and white VCS to each of the Colour channels. This results in decrease of pixel expansion but reduces the quality of the image due to halftone process.

iii. The third approach utilizes the binary representation of the Colour of a pixel and encrypts the secret image at the bit-level. This results in better quality but requires devices for decryption.

Steganography is the practice of concealing a file, message, image, or video. The word steganography combines the Greek words steganos meaning "covered, concealed, or protected", and graphein meaning "writing".

Visual cryptography plays a very crucial role for security of image-based secret. Colour Share generation using visual cryptography [5][7] encrypts the image in to shares and in decryption process all shares are stacked together to reveal the secret image. The study [8] identified the following gaps in visual cryptography:

i. The need of multi-level key security with random key generation is arises so that the data security will become more robust.

ii. Data partitioning is needed based on subset and super set approach so that level wise security can be applied to make the hacker unreachable.

iii. The length of the key should be maximized up to 256 to 512 bytes.

iv. RGB Entropy should be randomized to change the pixel positions.

v. The combination of cryptography with steganography is a stronger way to enhance the security.

The uses of steganography methods with the help of image encryption enhance the retrieval complexity.

III. PROPOSED SYSTEM

In the existing Colour share generation method, R, G and B components are extracted from Colour image then apply grey share generation algorithm on R component and make n number of R grey shares then all shares are combined with B and G component to make Colour shares. At decryption side B and G component is extracted from all shares and then combine all r grey share to make r component and after that all R, G and B is combined to revealed the secret image. Decrypted secret image has same size as original secret image. In this method, grey share generation algorithm is applied only on the R component and hence it may not generate a complete scrambled image share. There may be the visibility of the original image and hence it is less efficient.

There are many encryption techniques. DES is a rather old way of encrypting data so that the information could not be read by other people who might be intercepting traffic. DES is rather quite old and has since been replaced by a newer and better AES. The replacement was done due to the inherent weaknesses in DES that allowed the encryption to be broken using certain methods of attack. Common applications of AES, as of the moment, are still impervious to any type of cracking techniques, which makes it a good choice even for top secret information. There are many studies on AES to further improve the efficiency of it. 3D-AES [6] block cipher symmetric cryptography algorithm for SMS transfer securing. From the experiment, the 3D-AES has low encryption time when message size is more than 256 bits.

This work proposes an image securing algorithm that is a combination of both Visual-AES (a modified version of AES) and Colour share generation.

Here visual cryptography is done using two techniques namely, Advanced Encryption Standard (AES) algorithm and Colour share generation technique. The input to the system is a Colour image of any dimensions. The input Colour image is initially encrypted using Advanced Encryption Standard algorithm. By apply V-AES algorithm, an encrypted image is generated in which the original image is not visible. Later Colour share generation is applied in which the encrypted image is divided into two shares.

At the decryption side, the two-Colour shares are fed as input to the Colour share combination flow in which the two-Colour shares are combined and key generation is applied on R, G and B components. Later the V-AES decryption is applied on the encrypted image and the original Colour image is generated as output.

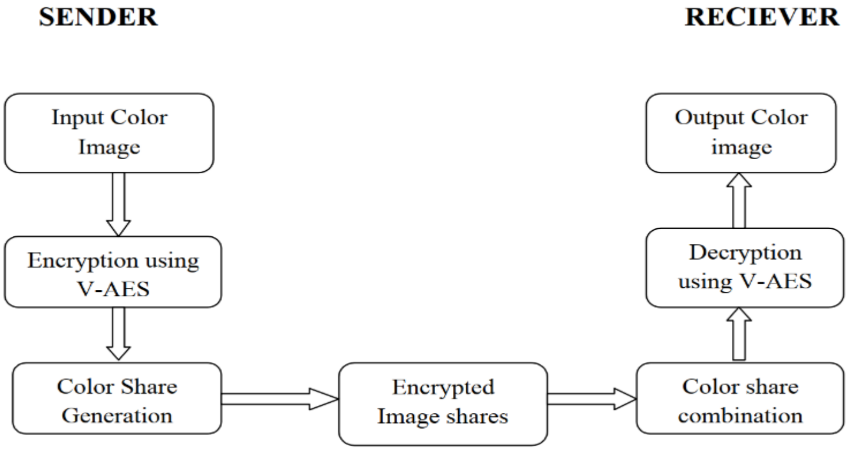

Figure 1: Overall architecture of Proposed Method

Encryption process

AES is a block cipher intended to replace DES for commercial applications. AES algorithm is of three types i.e. AES-128, AES-192 and AES-256. This classification is done on the bases of the key used in the algorithm for encryption and decryption process. The numbers represent the size of key in bits. This key size determines the security level as the size of key increases the level of security increases. The AES algorithm uses a round function that is composed of four different byte-oriented transformations.

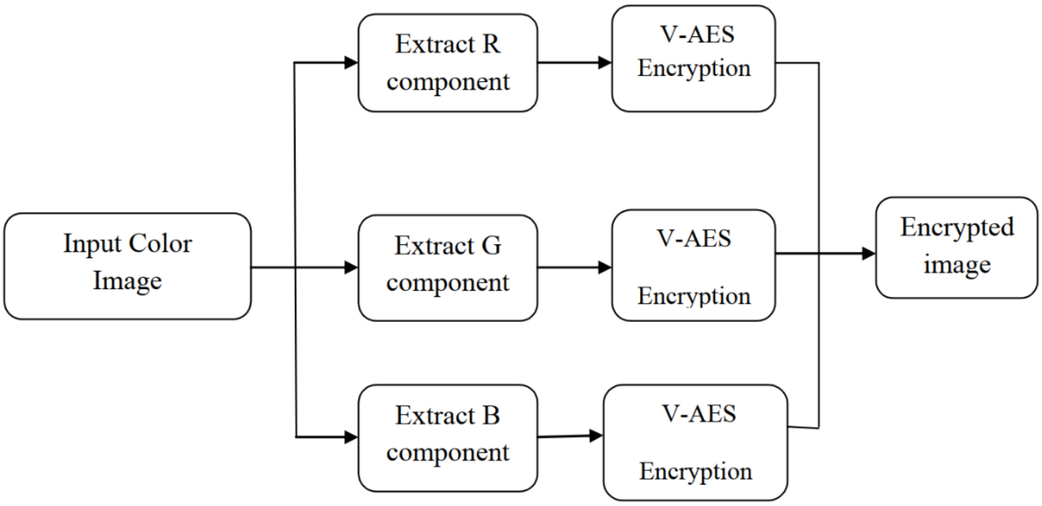

Figure 2: Image Encryption Process

In AES, all operations are performed on 8-bit bytes. In particular, the arithmetic operations of addition, multiplication, and division are performed over the finite field GF (2^8). For encryption purpose four rounds consist of:

- Substitute byte
- Shift row
- Mix columns
- Add round key

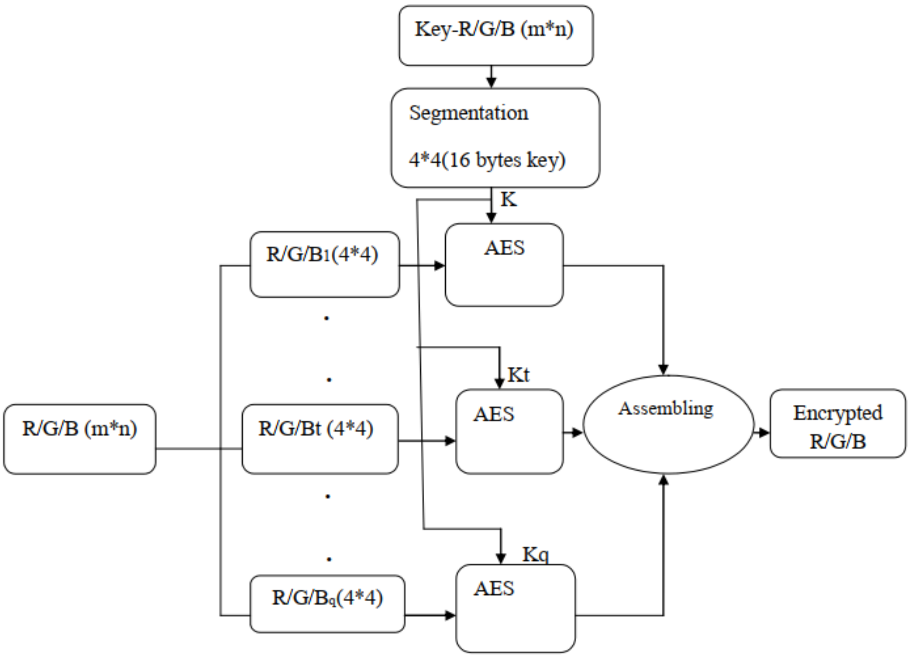

Figure 3: V-AES Block Diagram

The cipher consists of 10 rounds since this is a 16-byte key. The first 9 rounds consist of four distinct transformation functions: Sub bytes, Shift rows, mix columns and Add round key. The final round contains only three transformations, and there is an initial single transformation (add round key) before the first round. Each transformation takes one or more 4*4 matrices as input and produces a 4*4 matrix as output.

Decryption process

The AES decryption process is the reverse process that of the encryption process. The figure 4 shows flow of the AES decryption algorithm. In case of decryption the inverse substitute byte, inverse shift rows and the inverse mix columns are to be implemented. While the add round key remains the same.

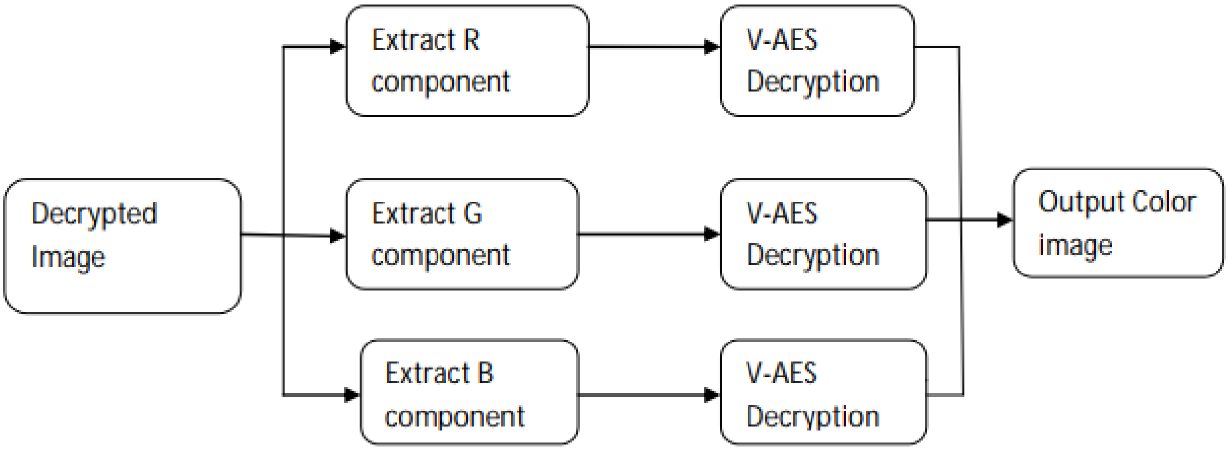

Figure 4: Image Decryption Process

Colour Share Generation

The encrypted image obtained by using Advanced Encryption Standard algorithm is given as input to the Colour share generation algorithm. The entire process of Colour share generation is shown in the figure 5.
The encrypted image is taken as input and R, G and B components are extracted from it.
Each component is divided into two shares.

R component is divided in the ratio of 1:3 as follows

$$R1=1/4(R)$$
$$R2=3/4(R)$$

G component is divided in the ratio of 1:1as follows

$$G1=1/2(G)$$
$$G2=1/2(G)$$

B component is divided in the ratio of 3:1 as follows

$$B1=3/4(B)$$
$$B2=1/4(B)$$

Thus, the three components are divided into two shares each. A key matrix is generated by using a key of size 64 bits. Each share is XOR-ed with the key matrix. By performing these operations, the pixels of the original image are changed. Now combine the first shares of the three components and generate a Colour shared image. In the similar manner combine the second shares of the R, G and B components and generate a second Colour shared image.

By using the Colour share generation, we are able to provide additional security for the secret sharing of images. In cryptography, it is always preferable to provide multiple levels of security. So that it is very difficult to identify the original information.

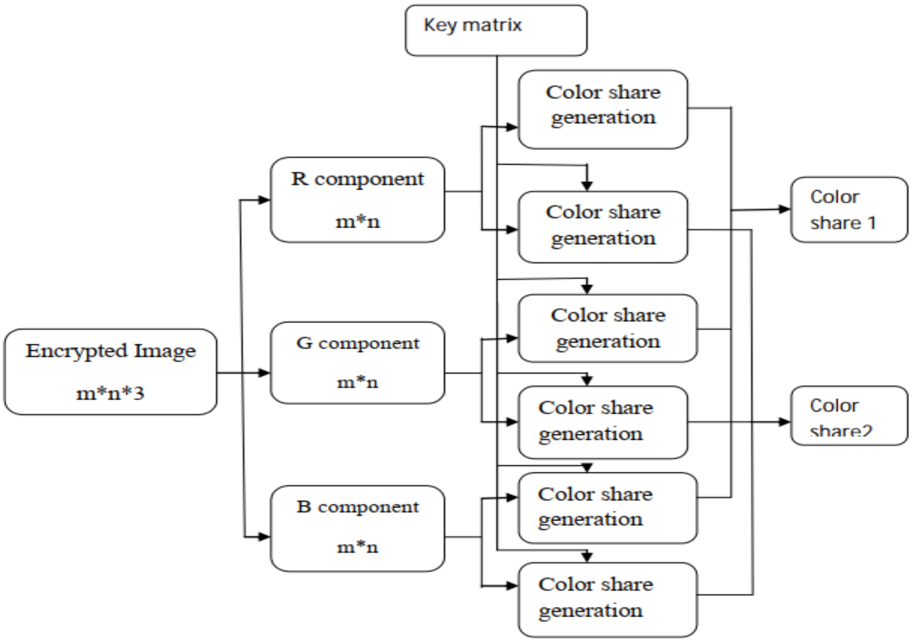

Figure 5: Colour Share Generation

Colour Share Combining

R, G and B components are extracted from the Colour shares. These are fed as inputs to the Colour share generation algorithm in which R components, G components and B components of both shares are combined. Thus, the two-Colour shares are combined to form a single decrypted image. The decrypted image is fed as input to the V-AES decryption algorithm and the original Colour image is generated as the output.

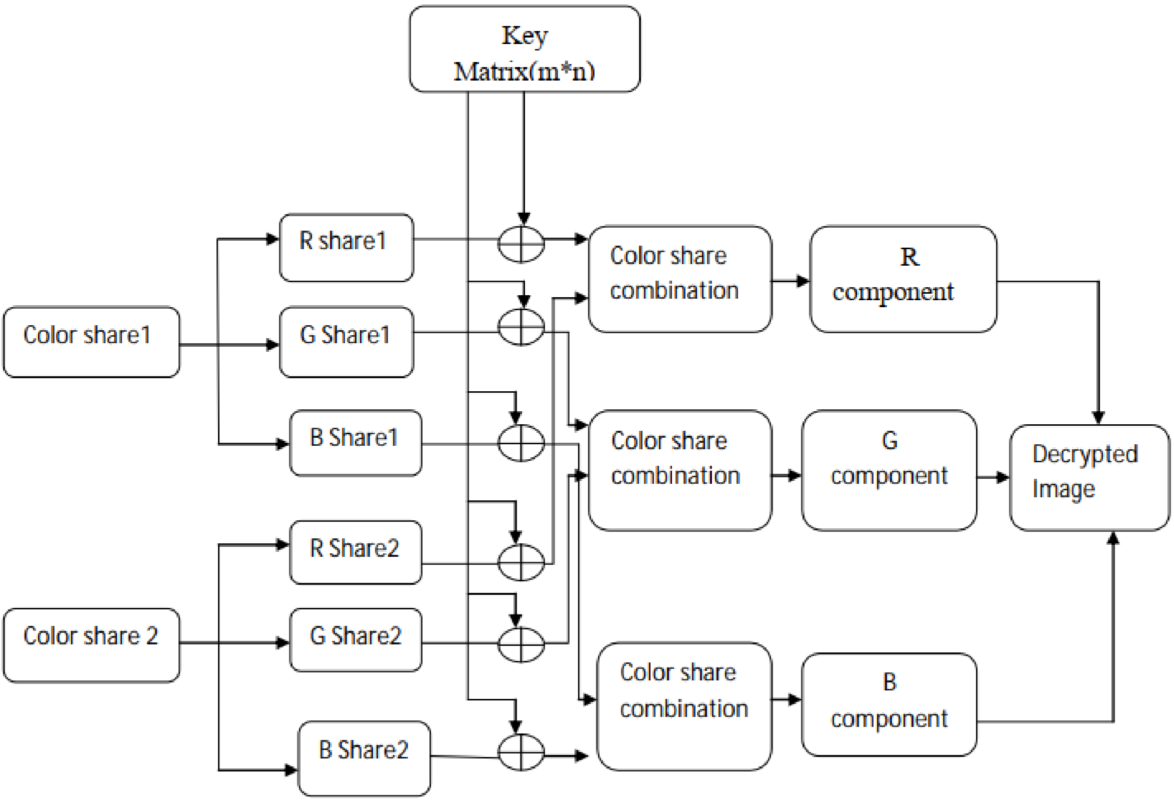

Figure 6: Colour Share Combining

IV. Implementation and Result Analysis

The complete proposed system was implemented using MATLAB. The original input image given to the algorithm is of JPG format. The unreadable image is the encrypted image and by applying the decryption algorithm the original image is obtained in JPG format. In this paper, For Encryption and the decryption the same key is used.

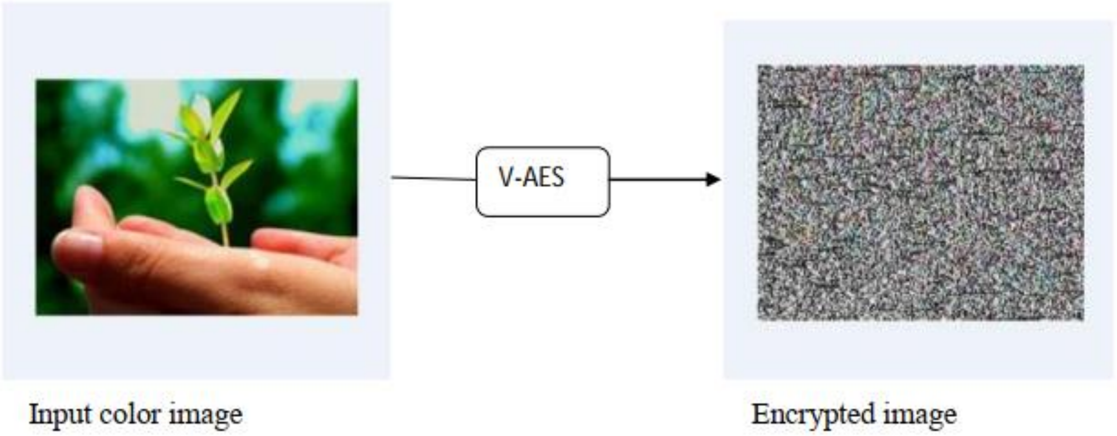

Figure 7: Image Encryption Using V-AES

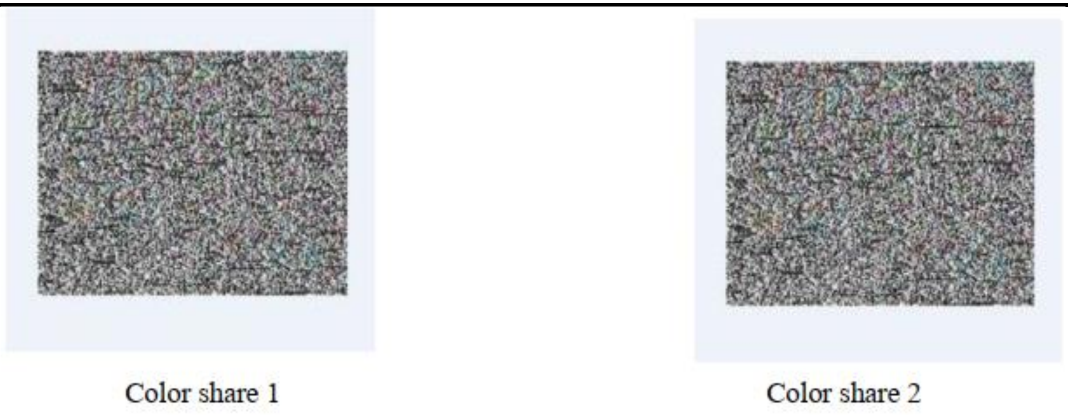

Figure 8: Colour Shares Generated

Here all Colour shares must have to participate to reveal the original Colour image. From the experimental result we can see that the attacker does not get any idea about which component's share is generated.

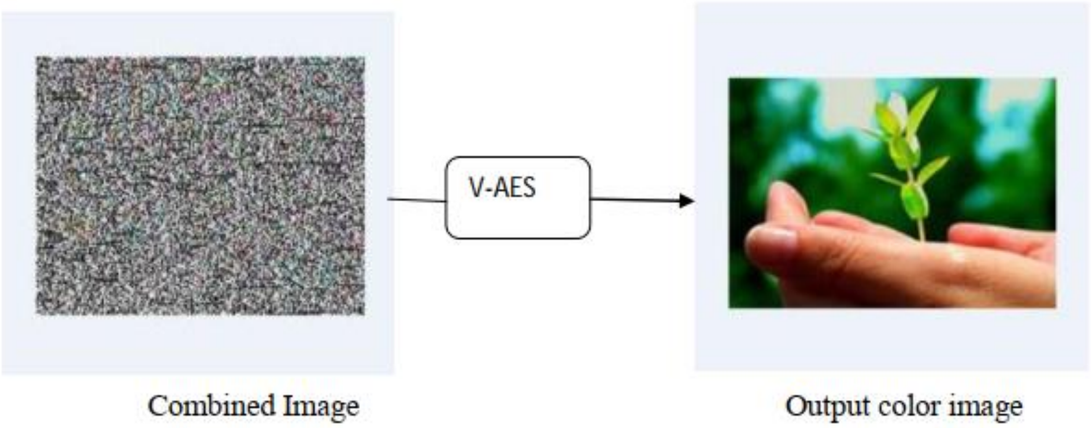

Figure 9: Image Decryption Using V-AES

V. Conclusion

Undoubtedly, Visual Cryptography provides one of the secure ways to transfer images on the Internet. Unlike most studies of visual cryptography, which concentrate on black-and-white images, this paper exploits the techniques of V-AES and Colour share generation. Based on the theory of Colour decomposition, every Colour on a Colour image can be decomposed into three primary Colours: R, G, and B. This paper proposed a new Colour share generation scheme using visual cryptography. In this scheme Colour image is encrypted in two shares. The revealed secret image has same sizes original image and visual quality is also maintained.

In this work, Image Encryption and Decryption using V-AES algorithm is implemented to secure the image data from an unauthorized access. A Successful implementation of symmetric key AES algorithm is one of the best encryptions and decryption standard available in market. With the help of MATLAB coding implementation of V-AES algorithm is synthesized and simulated for Image Encryption and Decryption. The original images can also be completely reconstructed without any distortion. It has shown that the algorithms have extremely large security key space and can withstand most common attacks such as the brute force attack, cipher attacks and plaintext attacks.

VI. References

[1] Chin chen Chang, Min Shian Hwang and Tung Shou Chen, “A new image encryption algorithm for image cryptosystems”, the journal of system and software 58(2001).

[2] Chin chen Chang, Min Shian Hwang and Tung Shou Chen, “A new image encryption algorithm for image cryptosystems”, the journal of system and software 58(2001).

[3] Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo, “Halftone Visual Cryptography”, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 15, NO. 8, AUGUST 2006.

[4] Abhishek Parakh, Subhash Kak, “A Recursive Threshold Visual Cryptography Scheme”, arxiv.org/abs/0902.2487.

[5] Trupti Patel, Rohit Srivastava, “A New Technique for Colour Share Generation using Visual Cryptography”, 2016.

[6] Suriyani Ariffin, Ramlan Mahmod, Ratini Rahmat, Nuzul Annisa Idris, “SMS Encryption using 3D-AES Block Cipher on Android Message Application”, Encryption,2013.

[7] Archana B. Dhole*, Prof. Nitin J. Janwe “An Implementation of Algorithms in Visual Cryptography in Images”, visual Cryptography, 2013.

[8] Apoorva Shrivastava and Lokesh Singh, “A new hybrid encryption and steganography technique”, steganography, 2014.

ACKNOWLEDGEMENT

We have great pleasure in expressing our gratitude to Sri K.V.V.Satyanarayana Raju, Founder & Chairman, Chaitanya Group of Institutions, Sri K. Sasi Kiran Varma, Vice Chairman, GIET Group of Institutions, Smt. Lakshmi Raju Executive Director, GIET, for their kind support in providing us an opportunity to do research in this college.