Cheating prevention in visual Cryptography

Himashekar K S[1]
MTech (CSE),2nd sem,
[1]himashekarks @gmail.com
SJB Institute of Technology, Bangalore-60

Chetan Shetty[2]
2-Asst. Prof.
[2]chetanshetty1986@gmail.com
Dept of Computer Science & Engineering
SJB Institute of Technology, Bangalore-60

ABSTRACT: ***Today, the world is on the anvil of being shrunk into a global net. All the systems around the world are to be used in the epoch of a nanosecond even when installed across continents and oceans. This is possible only through networks. It is in this context that networks become crucial to the viability of science and engineering research. It is in this context that Visual Cryptography has gained importance for communications between disparate networks. Visual cryptography is a scheme where a image is encrypted which independently disclose no information about the original image. Due to security threats original image may be modified by attacker. To deal this issue visual cryptography schemes can be applied to secure the original image.***

I. INTRODUCTION

In 1994, Naor and Shamir proposed a variant of secret sharing called visual cryptography (VC) . In a visual secret-sharing scheme, the shares given to participants are xeroxed onto transparencies. If is an authorized subset of participants, then the participants in can visually recover the secret image by stacking their transparencies to- gether without performing any computation. Visual cryptography (VC) is a method of encrypting a secret image using AES algorithm that reveals the different image during transmission. If intruder hacks the image while transmission they not able to visualize the original secret image. This provides a high security to maintain secret images. At the receiver end encrypted image should be decrypted using AES algorithm to get the original secret image. AES algorithm is used to get entirely different image form original secret image so that the intruder cannot even predict what kind of image it is. Since many visual cryptography schemes exists we proposed a new way sending from one system to another system. The original secret image is encrypted using AES algorithm and the encrypted pixel values are stored in a file with width and height of image. The file having encrypted pixel values send to receiver with private key. When receiver receives the file having encrypted pixel values can decrypt the pixel values to get theoriginal pixel values then gets the original secret image. Even if intruder hacks the file he cannot able to get the original secret image from the encrypted pixel values.

II. PRELIMINARIES

A.VC

A visual secret sharing scheme is a special variant of a secret-sharing scheme, where the shares given to participants are xeroxed onto transparencies. Therefore, a share is also called a transparency. If is a qualified subset of participants, then the participants in can visually recover the secret image by stacking their transparencies without performing any cryptographic computation. Usually, the secret is an image. To create the transparencies, each pixel, either black or white, of the secret image is separately handled. It appears as a collection of black and white sub pixels in each of the transparencies. It says that these sub pixels together form a block. This block is referred to as a black (resp. white) block if the pixel to be shared is black (resp. white). Therefore, a pixel of the secret image corresponds to sub pixels.

B. Cheating in VC

The issue of cheating is well studied and understood in secret-sharing schemes. Since VC is a variant of secret sharing, it is natural to also consider this issue. Most cheating attacks in VC are known plaintext attacks where the cheaters know the secret image and are able to infer the blocks of victim's transparency based on the base matrices. Let us take a two-out-of-three visual secret-sharing scheme as an ex- ample. A secret image is encoded into three distinct transparencies, de- noted . Then, the three transparencies are delivered to Alice, Bob, and Carol, respectively. Without lose of generality, Alice and Bob are assumed to be collusive cheaters, and Carol is the victim. For example, Alice and Bob may want to fool Carol such as kidding. During the cheating activity, Alice and Bob use and to create forged transparency such that superimposing will visually recover the cheating image. Assuming the following collections of 3 3 matrices, which are used to generate transparencies , Alice and Bob can predict the actual structure of Carol’s transparency so as to create :

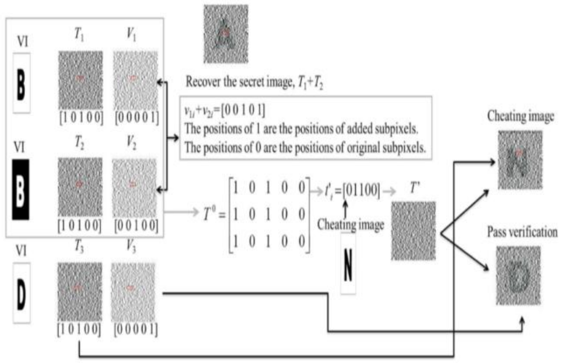

VI
T_1
V_1
B
[1 0 1 0 0]
[0 0 0 0 1]
VI
T_2
V_2
B
[1 0 1 0 0]
[0 0 1 0 0]
VI
T_3
V_3
D
[1 0 1 0 0]
[0 0 0 0 1]
Recover the secret image, T_1+T_2
$v_{1i}+v_{2i}$=[0 0 1 0 1]
The positions of 1 are the positions of added subpixels.
The positions of 0 are the positions of original subpixels.
$T^0 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{bmatrix}$
t'_i=[01100]
T'
Cheating image
N
Cheating image
Pass verification

Fig.1Transparency of image.

Visual cryptography scheme (VCS) is a kind of secret sharing scheme which allows the encoding of a secret image into shares distributed to participants. The beauty of such a scheme is that a set of qualified participants is able to recover the secret image without any cryptographic knowledge and computation devices. An extended visual cryptography scheme (EVCS) is a kind of VCS which consists of meaningful shares (compared to the random shares of traditional VCS).

Visual cryptography scheme (VCS) is scheme where image is encrypted using some algorithm using key or generating key image and the encrypted image will be send tointended person with key. Receiver will decrypt the encrypted image using same key to get the original image.The existing system does not provide a friendly environment to encrypt or decrypt the data. And vulnerable to different attacks. If intruder gets the encrypted image and key while transmitting he can get the original image.

III. SYSTEM ARCHITECTURE

Architectural design depicts the functionalities of the modules of the system and the interaction between the individual modules of the system. It shows the flow of the information or execution process in the system.

A major task of the design is to spell out in detail, the input, output and functionality of each module of the system. The design document is the developer’s blueprint. It provides precise directions to software programmers about how basic control and data structures will be organized. The design document is usually written before the programming starts. It describes how the software will be structured, and what functionality will be included. The architectural design is shown below.

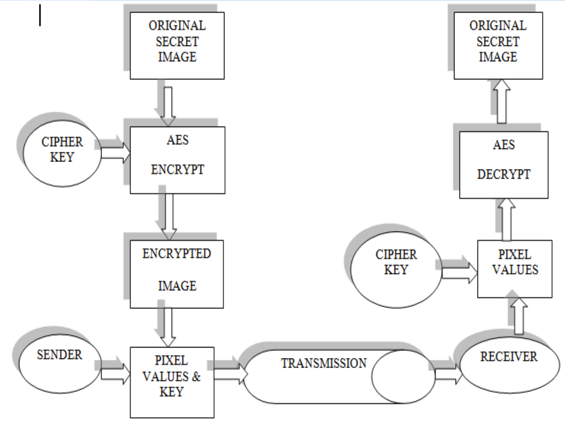


Fig.2Architectural design

Our application uses AES algorithm to encrypt the original secret image using 16 byte key.Here instead of sending encrypted image, the encrypted pixel values are stored in a file and send to intended person with key. Receiver decrypts the pixel values to get original image. This application uses key generation during addroundkey step while producing encrypted pixel values, which provides high security to the encrypted pixel values.Proposed system **Visual cryptography** provides a friendly environment to deal with text. Generally cryptography tools supports only one kind of image formats. Our application supports (portable network graphics) text and our application has been developed using swing and applet technologies, hence provides a friendly environment to users.

This application uses AES algorithm to encrypt the original secret image using 16 byte key.Here instead of sending encrypted image, the encrypted pixel values are stored in a file and send to intended person with key. Receiver decrypts the pixel values to get original image.This application uses key generation during addroundkey step while producing encrypted pixel values, which provides high security to the encrypted pixel values.Proposed system **Visual cryptography** provides a friendly environment to deal with text. Generally cryptography tools supports only one kind of image formats. This application supports (portable network graphics) text and This application can be developed using swing and applet technologies, hence provides a friendly environment to users.Inuse-case models each possible interaction is named in an ellipse and the external entity involved in the interaction is represented by a stick figure.

The use case diagram describes the proposed system interaction between the sender and receiver while encrypting and decrypting of the image by generating a secrete key and the encrypted image

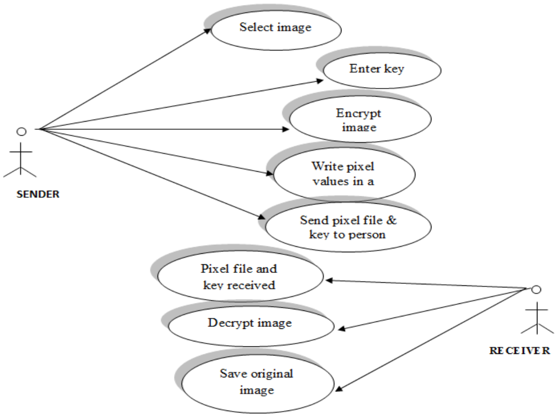


Fig.3 Use case diagram.

This picture shows the image before encryption and the encrypted image and the image produced after encryption by usibg the proposed system of cryptography method

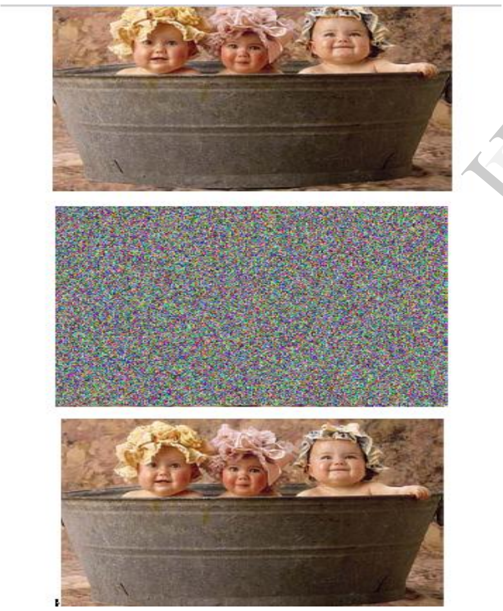


Fig.4 Image before and after encryption.

The below mentioned architecture shows how the encryption procedure is taken place from selecting of image and encrypting it which leads to the two file namely encrypted image file and the generated key file and they are send to the inted receiver and the receiver is decrypring it by making use of the key file and the encrypted image file containaining hexa decimal value in the file

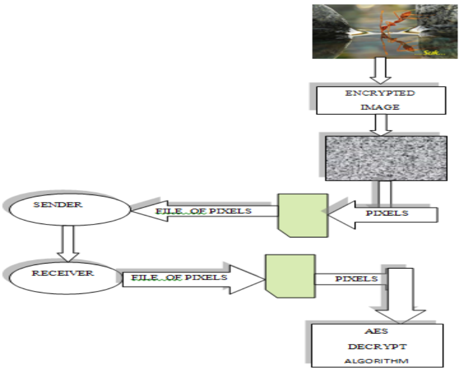
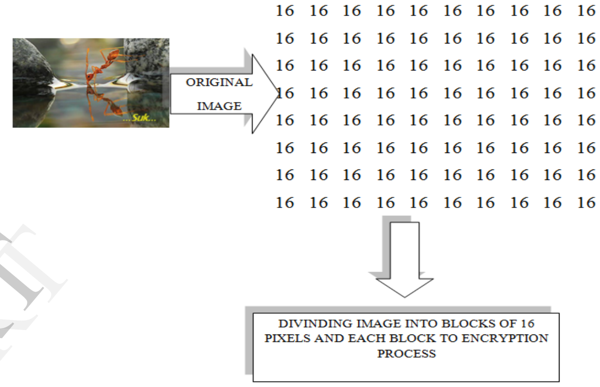


Fig.5 Encrypting and sending of image

Image that is breaking into block of sixteen pixels for the encryption following the algorithm


ORIGINAL IMAGE
DIVINDING IMAGE INTO BLOCKS OF 16 PIXELS AND EACH BLOCK TO ENCRYPTION PROCESS

16	16	16	16	16	16	16	16	16	16
16	16	16	16	16	16	16	16	16	16
16	16	16	16	16	16	16	16	16	16
16	16	16	16	16	16	16	16	16	16
16	16	16	16	16	16	16	16	16	16
16	16	16	16	16	16	16	16	16	16
16	16	16	16	16	16	16	16	16	16
16	16	16	16	16	16	16	16	16	16

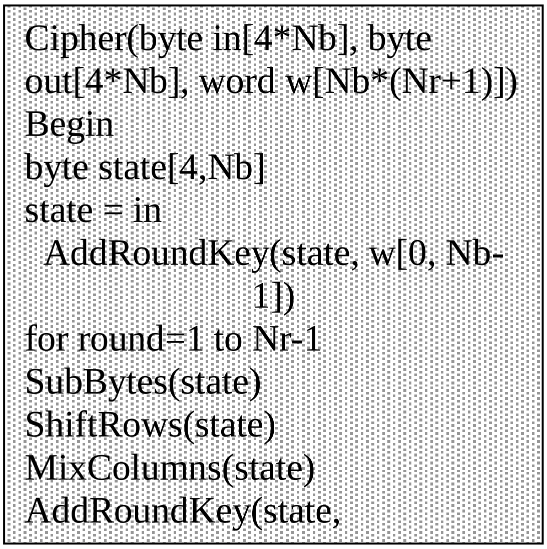
Fig.6 Dividing of image in terms of blocks

IV.ADVANTAGES of proposed system

- Since AES algorithm is used to encrypt the image which provides high protection to encrypted image.
- this application supports various image formats like .jpg, .bmp, .png
- Since encrypting the image and storing the encrypted pixel values in a separate file provides protection to the original image. Intruder cannot predict the image.
- AES algorithm uses key Expansion in which at each round out of 10 rounds different keys are used to encrypt the image.
- Since it sending the file of encrypted pixel values no need to worry about image formats, as it is decrypted which can be saved in format as receiver likes.
- No compression algorithms required since file of encrypted pixel values are sent.

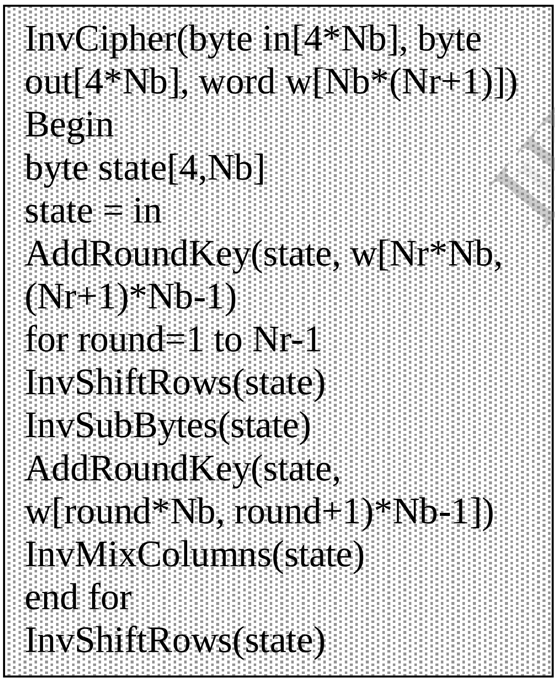
The algorithm follows the steps and rules that are mentioned below in the diagram for both encryption and decryption

A.AES encryption algorithm



```
Cipher(byte in[4*Nb], byte
out[4*Nb], word w[Nb*(Nr+1)])
Begin
byte state[4,Nb]
state = in
  AddRoundKey(state, w[0, Nb-
                    1])
for round=1 to Nr-1
SubBytes(state)
ShiftRows(state)
MixColumns(state)
AddRoundKey(state,
```

B.AES Decryption algorithm



```
InvCipher(byte in[4*Nb], byte
out[4*Nb], word w[Nb*(Nr+1)])
Begin
byte state[4,Nb]
state = in
AddRoundKey(state, w[Nr*Nb,
(Nr+1)*Nb-1)
for round=1 to Nr-1
InvShiftRows(state)
InvSubBytes(state)
AddRoundKey(state,
w[round*Nb, round+1)*Nb-1])
InvMixColumns(state)
end for
InvShiftRows(state)
```

V.CONCLUSION

The main objective of the paper, to provide security to images and to achieve visual Cryptography schemes. This can be used in applications where in a communication between two or more different networks is required.

Linux provides faster system-to-system communication than other operating systems and the network happens to be highly secured from the administrator's point of view. The FTP protocol developed in the course of this paper is highly reliable and deals with connection oriented systems.

Network security, which is the primary concern of today's communication world. Encryption and decryption is successfully implemented using AES algorithm. It provides a safe and secure transmission as it involves various transformations for encryption and decryption.

VI. REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in *Proc. Adv. Cryptol.*,1994, vol. 950, pp. 1–12, LNCS.

[2]"Extended capabilities for visual cryptography," Theoret.Comput. Sci., vol. 250, no. 1–2, pp. 143–161, 2001.

[2]C. Blundo and A. De Santis, "Visual cryptography schemes with perfect reconstructions of black pixels," Compute. Graph., vol. 22, no. 4,pp. 449–455, 1998.

[4]Y. C. Hou, Visual cryptography for color images, PatternRecognition, Vol. 36, 2003, pp. 1619-1629.

[5] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryp- tography for general access structures," Inf. Comput., vol. 129, no. 2, pp. 86–106, Sep. 1996.

[6] G. Blakley, "Safeguarding cryptographic keys," in Proc. AFIPS Nat. Conf., 1979, p. 313.

[7] C. Blundo, A. De Santis, and M. Naor, "Visual cryptography for grey level images," Inf. Process.Lett., vol. 75, no. 6, pp. 255–259, Nov. 2000.

[8] C. Blundo, P. D'Arco, A. De Santis, and D. R. Stinson, "Contrast op- timal threshold visual cryptography schemes," SIAM J. Discrete Math., vol. 16, no. 2, pp. 224–261, 2003.

[9] C. C. Chang and J. C. Chuang, "An image intellectual property protec- tion scheme for gray-level image using visual secret sharing strategy," Pattern Recog. Lett., vol. 23, no. 8, pp. 931–941, Jun. 2002.