International Journal of Innovative Technology & Adaptive Management (IJITAM)
ISSN: 2347-3622, Volume-1, Issue-7 , April, 2014

An approach of Visual Cryptography Scheme for Color Image by using Even and odd block based digital enveloping.

Ramkrishna Das,
Department of Computer Applications, Haldia Institute of Technology, Haldia, INDIA, 9933718033., (rmkrishnadas9@gmail.com).

Suparna Samanta
PG student, Dept. of Computer science, Vidyasagar University,Paschim Medinipur, WB,INDIA, ,suparna066@gmail.com.

Priya Mondol
PG student, Dept. of Computer science, Vidyasagar University,Paschim Medinipur, WB,INDIA, , priya033@gmail.com.

Saurabh Dutta
Department of Computer Applications, Dr B.C.Roy engineering College, Durgapur, INDIA, 9433411450 (saurabh.dutta@bcrec.org).

Abstract

Visual Cryptography is a special type of encryption technique to obscure image-based secret information which can be decrypted by Human Visual System (HVS).A digital envelope is data container that is used to protect a message through encryption and data authentication. A digital envelope allows users to encrypt data with the speed of secret key encryption and the convenience and security of public key encryption.

In this cryptographic system, we take original and envelope image as input and divide the envelope image into even and odd numbered blocks. Even pixels of original image are being mapped into odd blocks of envelope image and odd pixels of original image are being mapped into even blocks of envelope image at the time of encryption. The decrypted image is being constructed by taking the corresponding bit position's value from the envelope image. Thus an attempt is made for increasing the security.

Keywords- *Digital Enveloping, Even Block, Odd Block, Visual Cryptography.*

1. Introduction.

Cryptography is the practice and study of techniques for secure transmission of information between receiver and sender in the presence of other parties.
Visual cryptography is a cryptographic technique where visual information (Image, text, etc) gets encrypted in such a way that the decryption can be performed by the human visual system without aid of computers [1].
Like other multimedia components, image is sensed by human. Pixel is the smallest unit constructing a digital image.

Each pixel of a 32 bit digital color image is divided into four Parts, namely Alpha, Red, Green and Blue; each with 8 bits. Alpha part represents degree of transparency.
A 32 bit sample pixel is represented in the following figure [1].

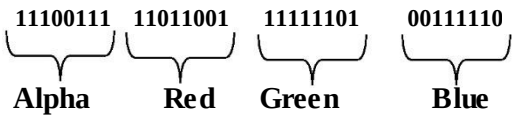


Fig 1: Structure of a 32 bit pixel

We take original and envelope image as input and divide the envelope image into even and odd numbered blocks Two least significant bits of each block of envelope image pixel are replaced by bits of original image's pixel serially. We need four pixels of envelope image for mapping the one pixel of original image where one pixel of the envelope image is used for one 8-bit block of original image. Envelope image is divided by w*h numbers of blocks (where w*h is the size of the original image).Each block size of envelope image is 4*32=128 bits. Even pixels of original image are being mapped into odd blocks of envelope image and odd pixels of original image are being mapped into even blocks of envelope

image at the time of encryption. The decrypted image is being constructed by taking the corresponding bit position's value from the envelope image. Thus an attempt is made for increasing the security.

In this paper section -2 describe the overall process section-3 describes the encryption process; section-4 describes the decryption process. An experimental result is being described in section-5 and section-6 draws the conclusion.

2. Overall Process.

Encryption process:-

Step I: we take the as original and envelope image as input.

Step II: Calculate width (w) and height (h) of original image.

Step III: Calculate t width (w1) and height (h1) of envelope image.

Step IV: If width (w1) and height (h1) of envelope image is less then equal to four times of width (w) and height (h) of original image then error will be occurred..

Step v: Convert the envelope image into w*h (width (w) and height (h) of original image) numbers of block.

Step VI: Read one pixel from original image and convert into 32 bits if the pixel is odd one then plot it into next even block of envelope and vice versa.

Step VII: Two least significant bits of each block of envelope image pixel are replaced by bits of original image's pixel serially. We need four pixels of envelope image for mapping the one pixel of original image where one pixel of the envelope image is used for one 8-bit block of original image. Envelope image is divided by w*h numbers of blocks (where w*h is the size of the original image).Each block size of envelope image is 4*32=128 bits. Even pixels of original image are being mapped into odd blocks of envelope image and odd pixels of original image are being mapped into even blocks of envelope image at the time of encryption.

Step VIII: Construct the enveloped image.

Decryption process:-

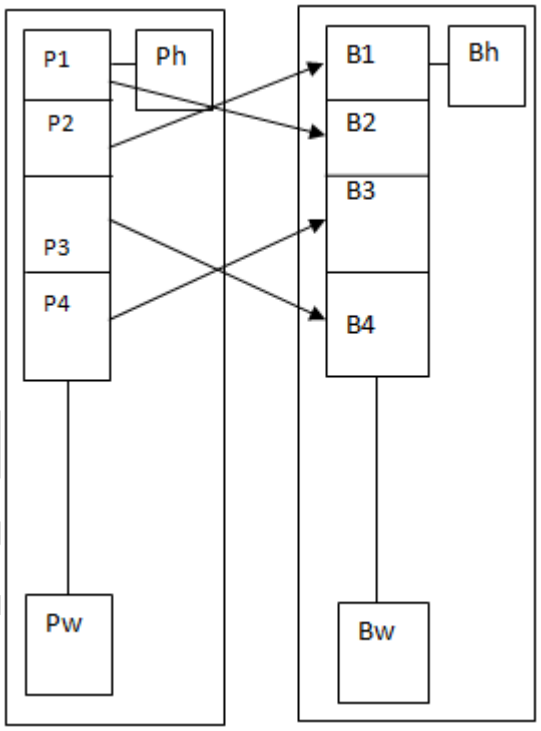
Step I: Read the enveloped image

Step II: Convert it into(w1*h1)/4 numbers of blocks(w1-width of envelope image, h1-height of envelope image).

Step III: Read two least significant bits of each block of each pixel in the referred block of the envelope image to the corresponding original pixel.

Step IV: Construct the decrypted image.

Figure[2] and figure[3] described the overall procedure.



P1, P2, P3……PN are the pixels of original image.
B1, B2, B3……BN are the blocks of envelope image.
Ph and Pw are height and width of original image.
Bh and Bw are height and width of envelope image.
Bh*Bw=Ph*Pw

Fig2: Mapping of original pixels to envelope blocks

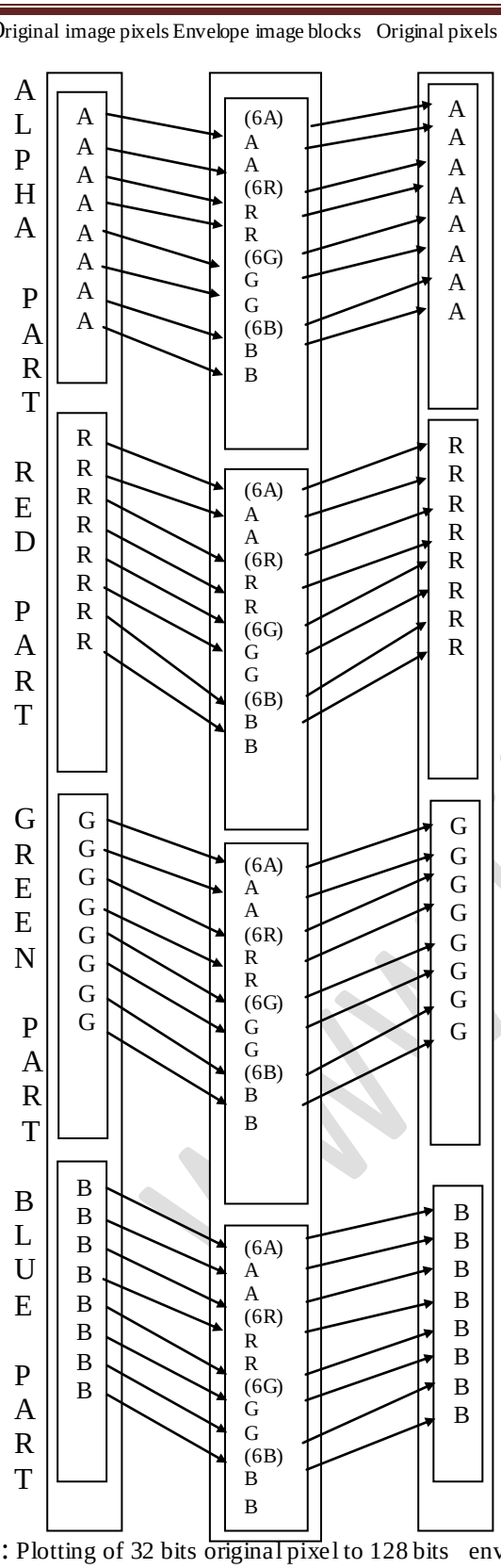


Fig3: Plotting of 32 bits original pixel to 128 bits envelope blocks

3. Encryption process:-

Step I: we take the as original and envelope image as input.

Step II: Calculate width (w) and height (h) of original image.

Step III: Calculate t width (w1) and height (h1) of envelope image.

Step IV: If width (w1) and height (h1) of envelope image is less then equal to four times of width (w) and height (h) of original image then error will be occurred..

Step v: Convert the envelope image into w*h (width (w) and height (h) of original image) numbers of block.

Step VI: Read one pixel from original image and convert into 32 bits if the pixel is odd one then plot it into next even block of envelope and vice versa.

Step VII: Two least significant bits of each block of envelope image pixel are replaced by bits of original image's pixel serially. We need four pixels of envelope image for mapping the one pixel of original image where one pixel of the envelope image is used for one 8-bit block of original image. Envelope image is divided by w*h numbers of blocks (where w*h is the size of the original image).Each block size of envelope image is 4*32=128 bits. Even pixels of original image are being mapped into odd blocks of envelope image and odd pixels of original image are being mapped into even blocks of envelope image at the time of encryption.

Step VIII: Construct the enveloped image.

Figure [4] and figure [5] described entered procedure.

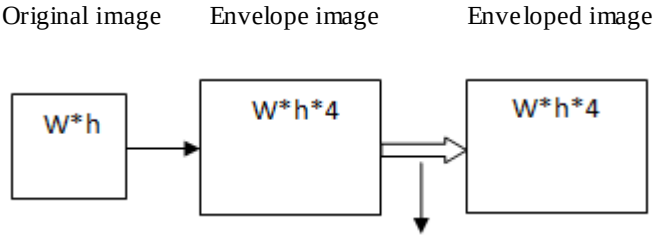


Fig4: Encryption

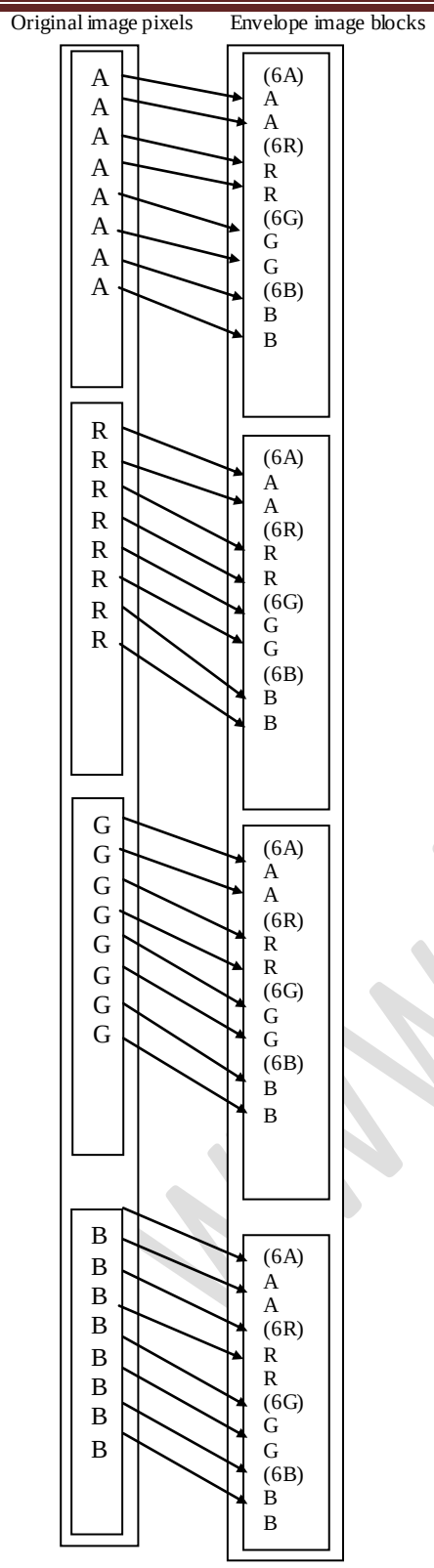


Fig5: Encryption by plotting pixels and blocks

4. Decryption process:-

Step I: Read the enveloped image

Step II: Convert it into (w1*h1)/4 numbers of blocks(w1-width of envelope image, h1-height of envelope image).

Step III: Read two least significant bits of each block of each pixel in the referred block of the envelope image to the corresponding original pixel.

Step IV: Construct the decrypted image.

Figure [6] and figure [7] described entered procedure.

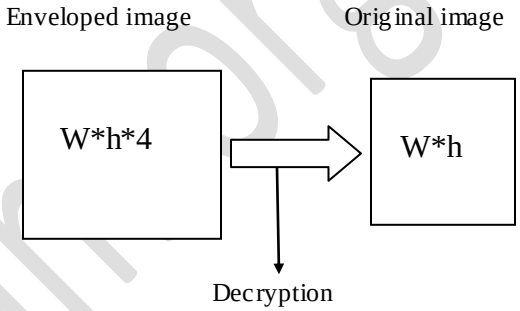


Fig5: Decryption

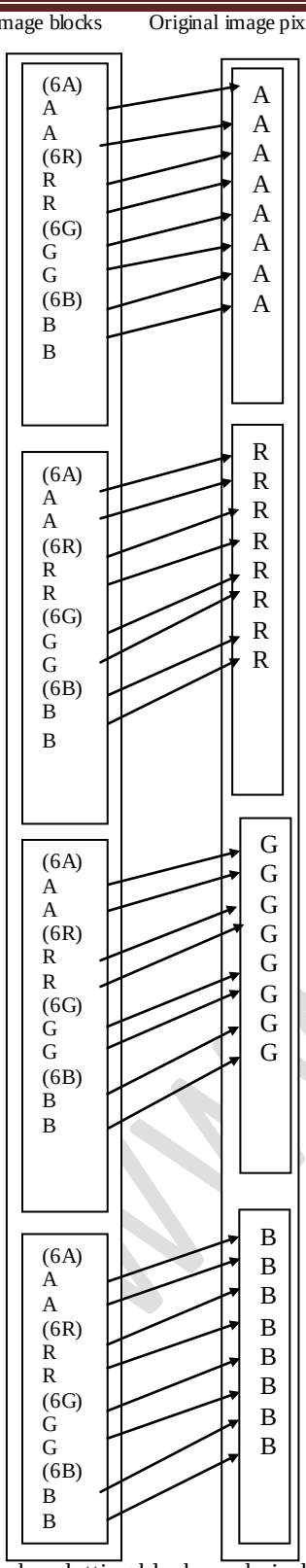


Fig7: Decryption by plotting blocks and pixels

5. Experimental Results and Discussion:-

Encryption using digital enveloping:

Enter original image- Parrot.jpg
Original image is:-

Parrot .jpg
Image size-200*150

Enter envelope image- Scenery.jpg
Envelope image is:-

Scenery.jpg
Image size-800*600
Enveloped image-Escenery.jpg
Enveloped image is:-

Scenery.jpg

Image size-800*600

Decryption using digital enveloping:

Enter enveloped image-Escenery.jpg
Enveloped image is:-

Escenery.jpg
Image size-800*600

Original image- Parrot.jpg

Original image is:-

Parrot .jpg

Image size-200*150

6. Conclusion

Decryption part of visual cryptography is based on OR Operation, so if a person gets sufficient n number of Shares; the image can be easily decrypted. In this current Work we have increased the security by using several level of encryption procedure.

We have spited the image into several pieces so if anyone has to reconstruct the image then he must have to collect all the pieces which is very hard to collect. Thus the security is increased.

We have performed the text key encryption and image key encryption on each share .Text key and image key are dedicated for a particular piece and the keys are only being known by receiver and sender. Thus the security is increased.

The division of an image into n number of pieces is done by using the user choice, The decrypted image reconstruction is done by proper arrangement of the defined numbers of pieces. Thus provide a great security.

We have to send huge additional information of image key, text key, piece arrangement with the normal envelope image. Thus need additional memory space. In future we will focus on it and proposed some scheme which needs less amount of memory.

References:

[1] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology-Eurocrypt'94, 1995, pp. 1–12.
[2] P. Ranjan, "Principles of Multimedia", Tata McGraw Hill, 2006.
[3] John F Koegel Buford, Multimedia Systems, Addison Wesley, 2000.
[4] KandarShyamalendu, MaitiArnab, "K-N Secret Sharing Visual Cryptography Scheme For Color Image Using Random Number" International Journal of Engineering Science and Technology, Vol 3, No. 3, 2011, pp. 1851-1857.
[5] Naskar P., Chaudhuri A, ChaudhuriAtal, Image Secret Sharing using a Novel Secret Sharing Technique with Steganography, IEEE CASCOM, Jadavpur University, 2010, pp 62-65.
[6] Hartung F., Kuttter M., "Multimedia Watermarking Techniques", IEEE, 1999.
[7] S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung. Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications. IEEE Journal on Selected Areas in Communications, Vol16, No.4 May 1998, pp.573–586,.