ISSN:2320-0790

COMPUSOFT
An International Journal of Advanced Computer Technology

Securing of Colour Images Using Visual Cryptography and Digital Enveloping

Vinita Malik[1], MamtaGhalan[2], DheerajKaushik[3]

[1,2]Assistant Professor Department of Information Technology, Maharaja Surajmal Institute of Technology, New Delhi, India

[3]Student, Department of Electronics and Communications, Maharaja Surajmal Institute of Technology, New Delhi, India

Abstract: Visual Cryptography is a Cryptography scheme which is used to secure images. In this scheme the image to be sent to receiver via sender is divided into number of shares and then they are sent to the receiver. In Decryption processes, these shares of images are combined or stacked together to get an original image. The initial model developed was only for the binary images. Later the black and white images or 0-1 image was further studied for the Coloured Images thatmeans for Red, Green, Blue. For the RGB images various methods have been developed but in all these techniques the received image has degraded quality. In this paper we propose a new algorithm for coloured visual cryptography and making it more secured by applying Digital Enveloping technique on the shares of the image. Digital Enveloping is a technique in which shares, of the image to be sent, are distributed over various sample images to create what is known Enveloped images. At the receiver end, shares are retrieved from the enveloped images and combined to form original image without degrading the quality of image. The important feature of the Visual Cryptography is decryption process is done by human eyes not the computer less computational power is required.

Keywords: *Visual Cryptography, Digital Enveloping, Shares, Image Security, Alpha Component, Encryption, Decryption*

I. INTRODUCTION

Visual cryptography was given by MoniNaor and Adi Shamir in 1994. They demonstrated the original visual secret sharing scheme, where an image was divided up into n shares so that only someone with all n shares could see the original image, while with any n-1 shares he/ she gets no information about the original image. Each share was printed on a different degree of transparency, and decryption was performed by stacking the shares. When all n shares were stacked, the original image would be seen [1][2][5].

Visual cryptography is a cryptographic technique where visual information like Image, data in form of text, etc. gets encrypted in such a waythat the decryption can be performed by the human eye without the use ofcomputers[3][4][9].

In this technique we deal with pixels of the image. Pixel is the smallest unit that denotes an image. We here deal with 32 bit
pixels and these 32 bit pixels are divided into four parts: - Alpha, Red, Green and Blue.

Red, Green and Blue each having 8 bit pixels and are better known as RGB components. Alpha also has 8 bit pixels and is the degree of transparency. A 32 bit sample pixel is denoted in Fig-1.

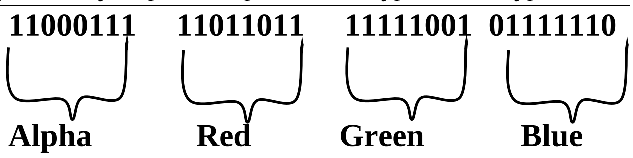


Figure (i): Structure of a 32 bit pixel

Here, we have devised a new algorithm.
In Encryption process for secret sharing, we divide the image into 4 shares namely: - Alpha, Red, Green and Blue. And then we apply Digital Enveloping Technique on these shares by putting each share into an image known as "*Innocent Cover*". So we put these shares in the innocent covers in such a way that we are unable to see the shares in this enveloped image as they are completely hidden and one cannot retrieve the original image if he/she does not have all the 4 enveloped images, hence supporting secret sharing and image security. That is,the image if hacked or interpreted by any other user than intended will open up in any other image but not displaying the data if data is sent in image or shares. This protects the data from being visible as it shows only the encrypted image and hence data is secure during transmission.

In Decryption process, exactly opposite process occurs to that in encryption process. That is, first of all, from all the 4 enveloped images the shares are extracted. And secondly, these shares are stacked or combined together to get the original image without any loss or degradation in the quality of the image.

II. RELATED WORK

A brief survey is given in this section about the related works that had been done till now on Visual Cryptography.

The visual cryptography concept was initially known as secret sharing. This was pioneered by AdiShamir in 1979. He in his paper stated that the secret image, data etc is divided in *n*no. ofpieces and can easily be reconstructed from any of these *k* pieces. He also claimed that the data is surely protected after the encryption technique but the key used for the same is not necessarily to be protected. He thus suggested this secret sharing algorithm to protect the keys that are used for the encryption process.

According to Naor and Shamir, the algorithm is *k-n* secret sharing algorithm [1].The simplest structure given by them was the 2 by 2 scheme where the source image would be encrypted into 2 shares and both the shares are needed for a successful decryption [1][2][13]. In 2 by 2 scheme the black and white image was taken and each pixel of it was divided in 2 sub-pixels, and an example of 2-2 scheme is shown below in Fig-2.

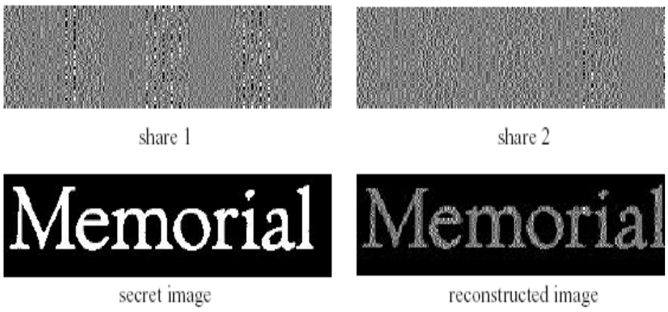


Figure (ii): Implementation of 2-2 VCA

The major drawback of this scheme was that it can be applied to only black and white images not the colored ones. CheLee used this scheme for authentication that is based on the 0-1 images with the limitation that the binary image should be in png format. In binary images, only two possibilities of pixels are there viz. black and white. So one can use 0 to represent black and 1 to represent white [6].

So, based on this ideal algorithm the researchers enhanced and performed their survey on visual cryptography. In these surveys of Visual Cryptography schemes they found out that the this technique not only works for black and white images but also colored images.[10][12]

Various cryptography schemes likeAlgorithm for General Access Structure, Half toning scheme, For Grey images, Multiple secret sharing, Extended VC, Progressive VC, Region VC, Segmented VC etc. were made for secure transfer[3].

After some years of these great works on visual cryptography, works on Digital Enveloping was done[5][11]. With Digital enveloping came the Digital Watermarking and its various techniques [4][14][7]. Initially, the coding of these algorithms were done on MATLAB but for greater security since past few years JAVA language is preferred [8][9]. Watermarking Techniques like Single Watermark Embedding and Multiple Watermark Embedding which is extension to Single Watermarking techniques were made [14]. Also a technique called LSB replacement [4] was made which we have used here along with our new algorithm.

Recently, the workto build a physical visual cryptographic system is going on that is based on optical interferometry [15]. But, all of these earlier results of the works while decrypting the image generates an image of reduced quality.

III. OVERALL PROCESS

Step I: The sample/source image is divided into 4 shares using our new algorithm called ARGB Algorithm such that all these 4 shares when combined gives us the original image.

Step II: Each of the 4 shares generated in Step I is embedded into 4 different envelope images or innocent covers using LSB replacement.

Step III: 4 enveloped images generated in Step II are taken and reverse LSB process is applied to generate the shares of the encrypted image

Step IV: Finally, these shares are combined to retrieve the original image at the receiver end.

IV. ARGB ALGORITHM FOR VISUAL CRYPTOGRAPHY

A. Scheme:-

The source image is taken as the input. We already know the number of shares that are 4. Now, the following algorithm is applied to divide the source image at sender's end into 4 ARGB shares: -

Step I: Take an image IMG as input and calculate its width and height. Make 4 copies of it using following process for storing ARGB components

img = read(file); // where file is the input image IMG
img1 = read(file);
img2 =.read(file);
img3 = read(file);
img4 = read(file);

Step II: Now extract the Alpha, Red, Green and Blue components from this image by extracting first 8 bit for alpha, next 8 bit for red and so on using following process.

for(y = 0 to height-1)
{
for(x = 0 to width-1)

```
  {
    p =getRGB(x,y) //extracting overall pixels of image
in
                              //RGB format
    a = (p>>24)&0xff      // extracting alpha component
```

Step III: Now save these ARGB components in the copied files we made in Step I by setting the extracted components in those copied images using the following process.

```
for( y = 0 to height-1)
{
for( x = 0 to width-1)
   {
    p=r<<24
    img1.setRGB(x, y, p)        /* setting images with
ARGB
```

```
    r = (p>>16)&0xff      // extracting red component
    g = (p>>8)&0xff       // extracting green component
    b = p&0xff            // extracting blue component
  }
}

    p=r<<16 components extracted in Step II*/
    img2.setRGB(x, y, p)
    p=g<<8      /*Both Step II and Step III
    img3.setRGB(x,  y,  p)                    works
simultaneously/*
    p=b
    img4.setRGB(x, y, p)
   }
 }
```

This Encryption process is shown in Fig-3.

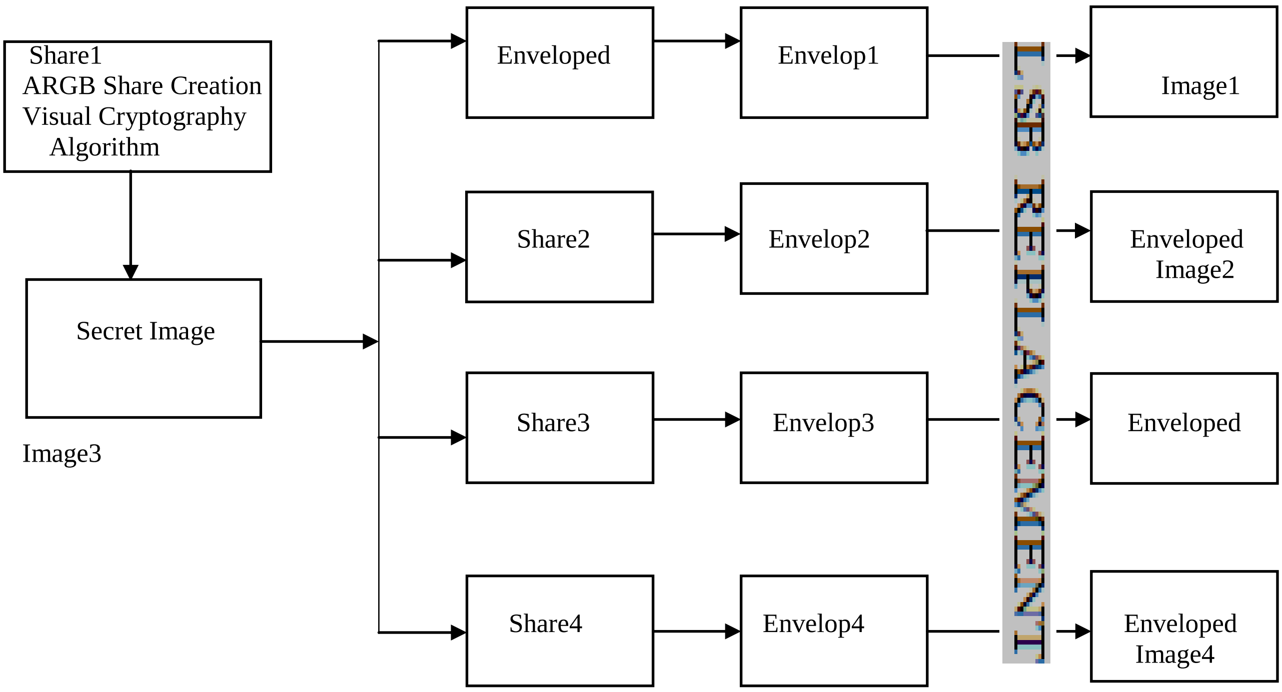


Figure (iii): Secret Sharing with Digital Enveloping (ENCRYPTION)

V. DIGITAL ENVELOPING

Using this step the shares that of the original image that were divided are enveloped within other image. Least Significant Bit (LSB) replacement digital enveloping technique is used for this enveloping process. It is already discussed that a 32 bit image pixel is divided into four parts namely alpha, red, green and blue; each with 8 bits. This algorithm shows that if the last two bits of each of these shares are changed; the changed colour effect is not detected by human eyes. This process is called invisible digital watermarking [4][10][14].

For using up all the 32 bits of a pixel of shares, that are divided, 4 pixels of the innocent cover are required. It means to envelope a share with dimensions sw X sh (share width and share height); we need a cover image with sw X sh X 4 pixels. Here we have taken each /cover envelope of size 4 X sw X sh. The following fig-3 describes the LSB replacement procedure. For replacement of 8 bit alpha share, one pixel of the envelope is required. In the same way red, green and blue (RGB) shares are enveloped using three other pixels of the cover image.

The enveloping is done using the following algorithm: -

Step I: Take the 4 shares that were created using ARGB as input and for each share = 0 to 3 repeat Step II to Step IV.

Step II: Take all the 4 shares, let that be Share1 to Share4 and the name of the covers be, ENV1 to ENV4 as input. Let the width and height of the shares be sw and sh and the width of the covers must be 4 times of the width of Shares. But height must be same as that of Share.

Step III: Create an array ORG_SH of size sw*sh*32 to store the pixel values of the SHARE using the following loop

```
for(y = 0 to sh-1)
{
```

```
for(x = 0 to sw-1)
  {
    p = img.getRGB(x,y)
for( j=0 to 31)
      ORG_SH[y*sw*32+x*32+j]=s.charAt(j)
```

Step IV: Use the marker value as M= −1. Using the following given procedure the SHAREs are embedded within ENV.

```
for(j = 0 to 4*sw*sh-1)
{
    ENV [j*32+ 6] = ORG_SH [++M]
    ENV [j*32+ 7] = ORG_SH [++M]
    ENV [j*32+14] = ORG_SH [++M]
    ENV [j*32+15] = ORG_SH [++M]
    ENV [j*32+22] = ORG_SH [++M]
    ENV [j*32+23] = ORG_SH [++M]
    ENV [j*32+30] = ORG_SH [++M]
    ENV [j*32+31] = ORG_SH [++M]
}
```

Now the Alpha, Red, Green and Blue shares are embedded or enveloped in the 4 innocent covers to generate and enveloped image and hence the image or data is encrypted in form of another image which cannot be seen by any other person other than the receiver who will get all the 4 enveloped image. The Decryption process at the receiver is explained in the following paragraph.

VI. DECRYPTION PROCESS

In this step 4 enveloped images are taken as input. From these enveloped images (taken one at a time), for each pixel, the shares alpha, red, green and blue are extracted and the OR operation is performed to retrieve the original source image. It is already known that human eye acts as an OR function [4][14].

The decryption process is performed by the following algorithm.

```
   }

 }
```

Create the array of ENV of size 4*sw*sh*32 that would store the pixel values of the ENV1 to ENV4.

Step I: Input the 4 enveloped images that were generated in encryption process; eheight (h) and ewidth (w) of each image.

Step II: Now extract the RGB components from the enveloped images and using following process

```
for(y = 0 to eheight-1)
{
for(x = 0 to ewidth-1)
  {
        p = .getRGB(x,y)
        s= Integer.toBinaryString(p)
for(j=0 to 32)
        ENV[y*ewidth*32+x*32+j]=s.charAt(j)
   }
 }
```

Step III: Now saving these extracted components into different shares which are $1/4^{th}$ of these envelope images using following algorithms.

```
for(int j = 0 to 32*ewidth*eheight-1)
{
       ORG [++M]=ENV [j+ 6];
       ORG [++M]=ENV [j+ 7];
       ORG [++M]=ENV [j+ 14];
       ORG [++M]=ENV [j+ 15];
       ORG [++M]=ENV [j+ 22];
       ORG [++M]=ENV [j+ 23];
       ORG [++M]=ENV [j+ 30];
       ORG [++M]=ENV [j+ 31];
  }
```

Now by shifting of ARGB pixels to its appropriate places while combining the shares (just in the opposite way as we did in Step II of Encryption process) gives us the original image IMG.

This Decryption Process is shown in Fig-4.

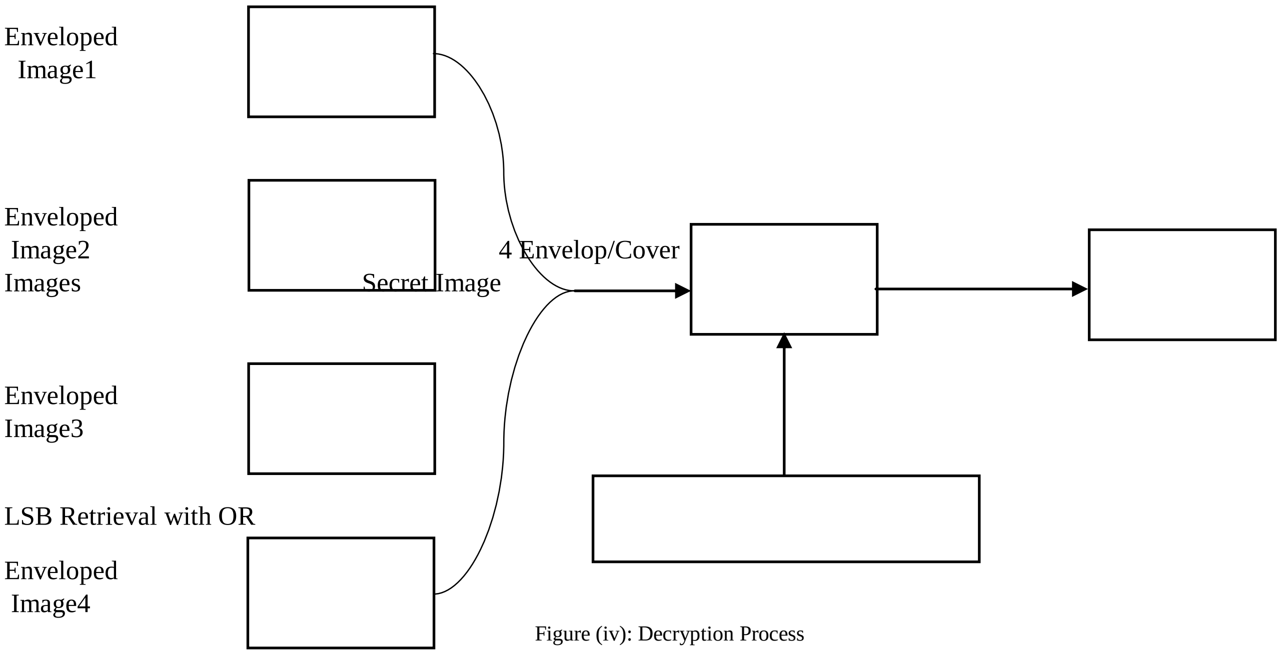


Figure (iv): Decryption Process

VII. EXPERIMENTAL RESULTS

A. Dividing into shares using Visual Cryptography:

Secret Image: Sample_1.jpg
Secret image to be sent by sender to the receiver on a network is:

Figure (v): Secret Image to be sent

Number of Shares: 4
Image shares produced after applying ARGB Algorithm are:

Alpha (Degree of Transparency) generated by extracting first 8 pixels of the Secret image to be sent.

Figure (vi)a: Share1-Alpha (Degree of transparency)

Red Component is generated by extracting next pixels of the Secret image.

Figure (vi)b: Share2-Red Component

Green Component is generated by extracting next pixels of the Secret image.

Figure (vi)c: Share3- Green Component

Blue Component is generated by extracting next pixels of the Secret image.

Figure (vi)d: Share4- Blue Component

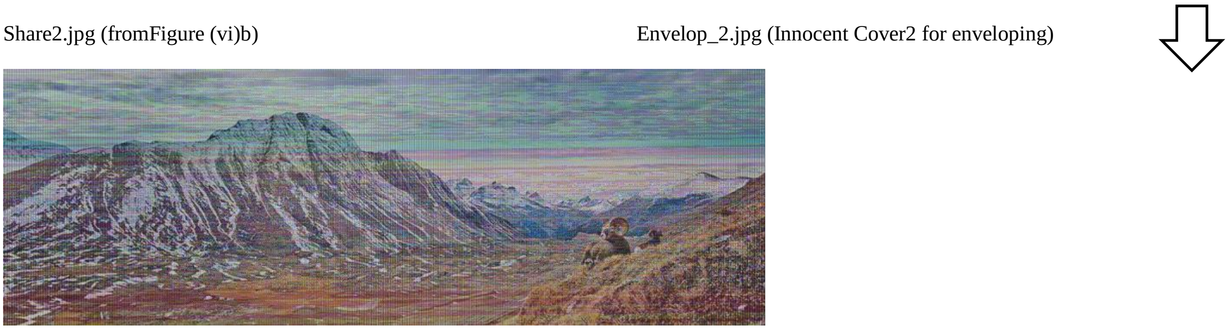
B. Digital Enveloping:

Share1.jpg (fromFigure (vi)a)Envelop_1.jpg (Innocent cover1 for enveloping)

Enveloped_1.jpg (After Enveloping- Share1+Envelop1)

Figure (vii)a: Enveloping of (Share1.jpg OR Envelope_1.jpg)

Share2.jpg (fromFigure (vi)b) Envelop_2.jpg (Innocent Cover2 for enveloping)



Enveloped_2.jpg (After Enveloping- Share2+Envelop2)

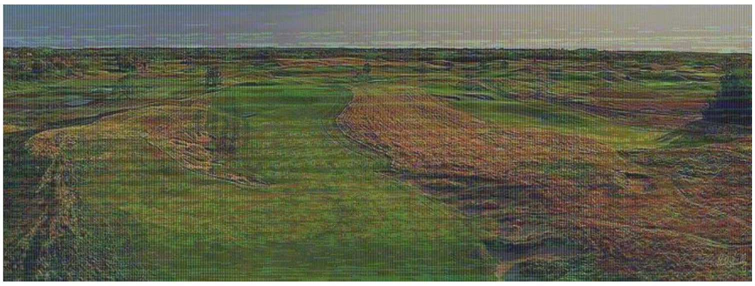
Figure (vii)b: Enveloping of (Share2.jpg OR Envelope_2.jpg)

Share3.jpg (fromFigure (vi)c)Envelop_3.jpg (Innocent cover3 for enveloping)

Enveloped_3.jpg (After Enveloping- Share3+Envelop3)

Figure (vii)c: Enveloping of (Share3.jpg OR Envelope_3.jpg)

Share4.jpg (fromFigure (vi)d)Envelop_4.jpg (Innocent cover3 for enveloping)



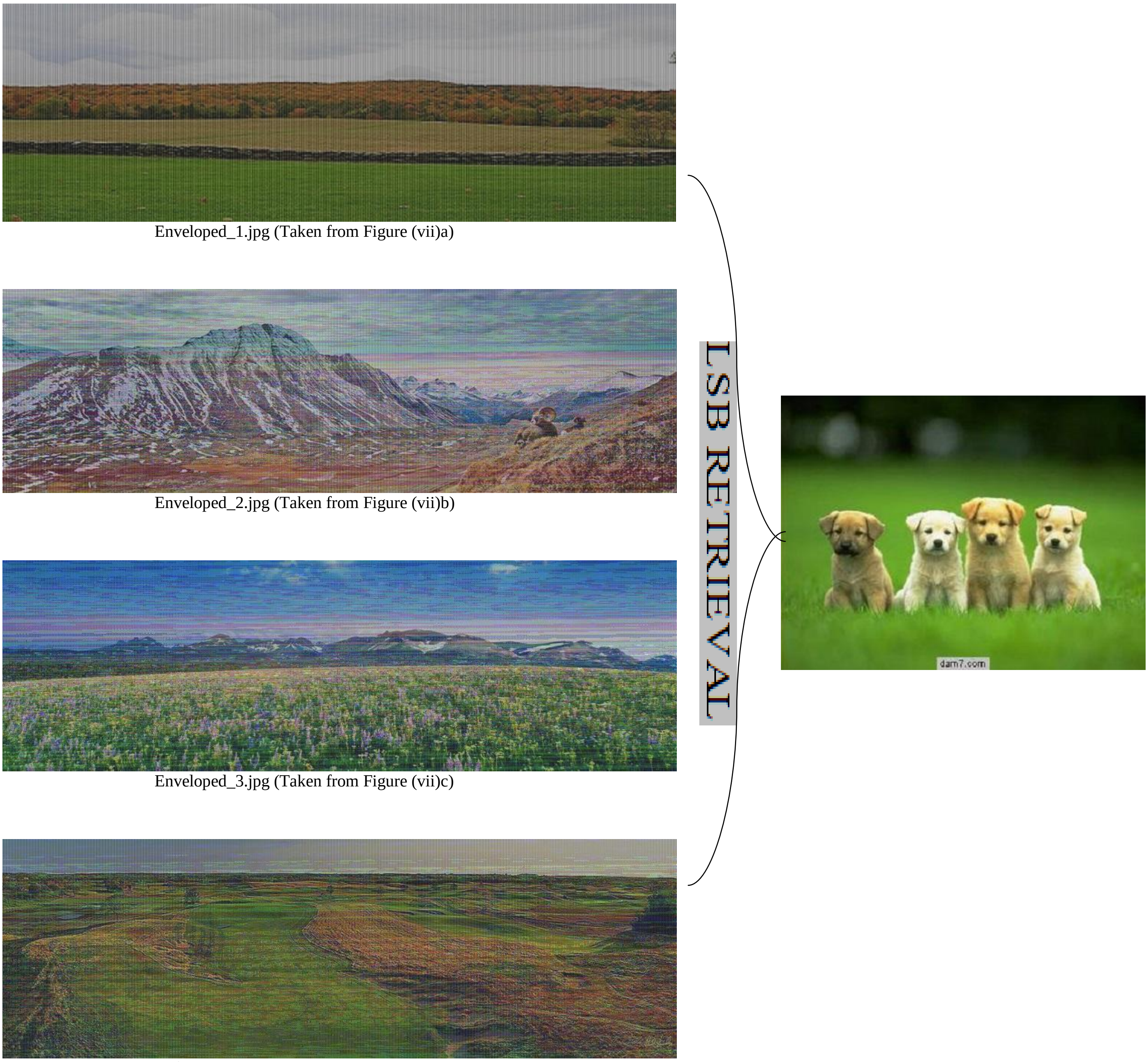
Enveloped_4.jpg (After Enveloping- Share4+Envelop4)

Figure (vii)d: Enveloping of (Share4.jpg OR Envelope_4.jpg)

Figure (vii): Enveloping ARGB shares using Digital Watermarking (Encryption technique) at Sender

C. Decryption Process:

Number of Enveloped images: 4
Name of the images: Enveloped_1.jpg, Enveloped_2.jpg, Enveloped_3.jpg, Enveloped_4.jpg



Enveloped_1.jpg (Taken from Figure (vii)a)

Enveloped_2.jpg (Taken from Figure (vii)b)

Enveloped_3.jpg (Taken from Figure (vii)c)

Enveloped_4.jpg (Taken from Figure (vii)d)

Figure (viii): Decryption Technique (Image retrieval) at Receiver

VIII. CONCLUSION

Decryption technique of visual cryptography algorithm is based on OR operation that is 0+1=1, 1+0=1, 1+1=1 and 0+0=0, so if any person gets all the shares; then he would be able to decrypt the image easily. In our current work, with new ARGB Algorithm for secret sharing of colored images along with enveloping technique that was earlier proposed where the ARGB shares are enveloped inside innocent covers of images or pictures using LSB replacement. Hence, this technique increases the security to visual cryptography technique from attack by the hacker as he is not able to retrieve the images without having all the 4 enveloped images. That is we here have doubled the security, first, by making shares of the original image and secondly, by enveloping it into other innocent images. The division of an image into 4 shares is done by simple extraction of ARGB components, which is a new technique devised. This technique needs no to very less mathematical calculation as compared to other existing algorithms for visual cryptography.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology-Eurocrypt'94, 1995, pp. 1–12.

[2] M. Naor, A. Shamir, in: M. Lomas (Ed.), Visual Cryptography, II: Improving the Contrast via the Cover Base,Presented at Security in Communication Networks, Amalfi,Italy, September 16–17, 1996. Lecture Notes inComputerScience, Vol. 1189, Springer, Berlin, 1997, pp. 197–202

[3] Suhas B. Bhagate 1, P.J.Kulkarni 2 "An Overview of Various Visual Cryptography Schemes".

[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] Monish Kumar Dutta and AsokeNath "Scope and Challenges in Visual Cryptography".

[6] Wen Tsai Che Lee, Authentication of binary images in png format based on a secret sharing technique. Proceedings of IEEE International Conference on System and Engineering, pages 506-510, July 2010.

[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.

[8] Schildt, H. The Complete Reference Java 2, Fifth Ed. TMH, Pp 799-839

[9] Krishmoorthy R, Prabhu S, Internet & Java Programming, New Age International, pp 234.

[10] F. Liu1, C.K. Wu1, X.J. Lin, Colour visual cryptography schemes, IET Information Security, July 2008.

[11] Kang InKoo el. at., Color Extended Visual Cryptography using Error Diffusion, IEEE 2010.

[12] SaiChandana B., Anuradha S., A New Visual Cryptography Scheme for Color Images, International Journal of Engineering Science and Technology, Vol 2 (6), 2010.

[13] Li Bai , A Reliable (k,n) Image Secret Sharing Scheme by, IEEE,2006.

[14] B Surekha, Dr GN Swamy and Dr K SrinivasaRao "A Multiple Watermarking Technique for Images based on Visual Cryptography"

[15] S.-S. Lee, J.-C.Na, S.-W.Sohn, C. Park, D.-H.Seo, and S.-J. Kim, "Visual cryptography based on an interferometric encryption technique," *ETRI Journal*, vol. 24, pp. 373–380, 2002, available at http://etrij.etri.re.kr/etrij/pdfdata/24-05-05.pdf.