NOVEL SECURE TECHNIQUE USING VISUAL CRYPTOGRAPHY AND ADVANCE AES FOR IMAGES

M. Arun Kumar¹ & K. Jhon Singh²

¹School of Information Technology, VIT University, Vellore, India, (arunkumarm88@gmail.com)
²Prof., School of Information Technology, VIT University, Vellore, India, (jhonsingh.k@vit.ac.in)

Abstract: The novel technique is proposed, that uses both Visual Cryptography and Advance AES Encryption methods simultaneously for color images. The Secrete image is transmitted by secrete sharing using visual cryptography technique and the shares are encrypted using secret key and thus provides double layer protection for a digital Image. Experimental results show that the proposed system is resilient to attacks and constantly protects the ownership rights. The Rudin-Osher-Fatemi de-noising algorithm is used to reduce the noise and produce less distortion image. The main goal is to protect the image from unauthorized use and to provide authentication for digital information continuous basis with less distortion.

Keywords: Advanced AES, ROF algorithm, Visual cryptography.

1. VISUAL CRYPTOGRAPHY

VISUAL CRYPTOGRAPHY is a cryptographic technique which allows visual information (pictures) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. The visual cryptography is based on selection of particular pixels from the original cover image instead of random selection of pixels.

1.1. Visual Cryptography Scheme for Binary Image

[6] In 1994, Naor and Shamir proposed the concept of visual cryptography. The visual cryptography does not use any complex computation. Each pixel is sub divided into 4 sub pixels in to two shares. Share 1 is a key and share 2 is a cipher. The sub pixels of the share are aligned using XOR to get half black pixel and full black pixels. The visual cryptography starts with selecting random cells in 6 choices shown below.

The selected random cell is a key. Share 1 does not provide any information. The cipher share2 is generated by choosing complementary cell for black sub pixel and same cell for white sub pixel. Then two shares are stacked to view the original information. The key share is generated by random selection of 6 pixels. The pixel is selected from the secrete message, if the pixel is black then the complementary cell is selected in cipher share for corresponding cell in the key and vice versa, thus the entire secrete message is divided in to two shares. The two shares are stacked XOR’ed to view the entire secrete image. The sizes of shares generated by the visual cryptography are double the original image. So get the image of original size the combined shares are sub sampled [2].

1.2. Visual Cryptography Scheme for Color Image

[8] In1997 ‘Verheul and VanTilborg’ proposed visual cryptography for color image. Color image is seen as array of pixels. Image can look up with gray levels. Each pixel is expanded to m sub pixels. Each pixel can take one of the color after look up with gray level. After all shares are stacked, and color i is revealed, if corresponding sub pixel of all shares are of color i. Otherwise, the level of black is revealed.

![Figure 1: Random Secrete Key for Visual Cryptography](image)

2. HALFTONING

Half toning is process image reproduction for various computer devices with limited colors. According to physical properties of different media uses different methods to represent a color level of
image. The general dot matrix and laser printers can only control a single pixel to be printed. The half toning is applied to image to render the illusion of continuous tone image on the devices that is capable of producing only binary image. This illusion is achieved because our eyes perform spatial integration.

2.1. Error Diffusion

[7] Error diffusion is used in our scheme to convert the gray component to binary image. The Jarvis error filter is used to distribute the error to error to neighboring pixels to obtain the continuous halftone image. The Floyd Steinberg error filter uses 4 tags for error distribution, but Jarvis error filter uses 12 tag filter. Thus Jarvis error diffusion provides sharper halftone image.

The pixel \( j[n] \) of a continuous tone digital image is processed from right to left and from top to bottom. At each step of algorithm the grey value current pixel represented by 0 to 255 is compared to threshold value. If the grey value is greater than threshold then the pixel is black and output \( j[n] \) value is set to 1, else if the value is lesser than threshold then th pixel is white and output \( j[n] \) is set to 0. The difference between the original gray pixel and threshold is error. To achieve continuous tone effect the error is distributed to 12 neighboring pixels that have to process yet using Jarvis error filter. [3] The Jarvis halftone is substantially sharper than Floyd Steinberg halftone.

The above diagram shows the Jarvis error filter. Jarvis algorithm uses 12 tag for error filter uses 12 tags for error distribution.

3. ROF DEINOISING

[4] The error distributed by Jarvis error diffusion method is removed using ROF de noising. The general idea behind most of denoising method is to get noisy image \( f \) as being obtained by corrupting a noiseless image \( u \). The desire image \( u \) is then a solution of inverse process. Most of de noising procedures employ some sort of regularization. A very successful algorithm is that of Rudin, Osher, and Fatemi which uses Total variation regularization. The ROF algorithm is based on Total variance [5]. The main characteristics of TV procedure is as follows.

(1) It has simple fixed filter structure and an exact formula for the filter coefficients that exactly encode the edge information.

(2) Unlike most filters, The digital filter is based on functional analysis and geometry.

(3) The digital TV filter is quite flexible in the sense that it applies to general data on a graph, signals like color images and non flat image such as chromaticity.

Let be the \( U0(X) \) noise contaminated signal of a clean signal \( U(X) \).

\[
U0(X) = U(X) + n(X) \quad [2]
\]

Here, denotes random noise with mean 0 and variance[2]

\[
En(X)=0, En2(X)=\sigma^2 \quad (1)
\]

The TV anisotropic diffusion model was invented by Rudin, Osher and Fatemi and is now one of the most successful tools for image restoration. That is, one minimizes the total variation.

\[
TV [U] = \int_{\Omega} |\nabla u| \ dx \quad (2)
\]

\( \Omega \) Here denotes the continuous signal domain, the \( \Delta u \) gradient, and \( dx \) the area element of \( \Omega \).

The assumptions on the noise (1) now lead to two constraints for the minimization of the TV [2]

\[
\int_{\Omega} u \ dx \int_{\Omega} u^2 \ dx / |\Omega| \int_{\Omega} \hat{U}(u-u)^2 \ dx = \sigma^2 \quad (3)
\]

Where \( |\Omega| \) is the area of the image domain \( \hat{U} \). Therefore, (2) and (3) together define a constrained optimization problem.
Due to the translation invariance of the TV norm: $TV[u+c]=TV[u]$ for any constant $c$, the first constraint is in fact automatically encoded. We only need to consider the second fitting constraint. By introducing the Lagrange multiplier $\bar{e}$, one can define a new energy functional

$$j[u]=\int_{\Omega}|\Delta u| \ dx + \lambda/2 \int_{\Omega} (u-u^*)^2 \ dx$$

(4)

The Euler-Lagrange equation of $j$ is

$$-\Delta_\alpha (\Delta u / |\Delta u|) + \lambda (u-u^*)^2 = 0$$

(5)

To avoid singularities in flat region equation (5) is regularized to

$$|\Delta u|_{\alpha} = \sqrt{(|\Delta u|^2 + \alpha^2)}$$

for some small positive parameter. Then the modified Euler-Lagrange equation (5) in fact minimizes the regularized energy functional.

$$j[u]_{\alpha}=\int_{\Omega} |\Delta u_{\alpha}| \ dx + \lambda/2 \int_{\Omega} (u-u^*)^2 \ dx.$$ 

4. ENCRYPTION

[9] The AES Algorithm is a symmetric key cipher in which both the sender and receiver uses same key for encryption and decryption. The data block is fixed size of 128 bits, the key length can vary from 128, 192, 256 bits. AES algorithm is an iterative algorithm. Each iteration is called round. The number of rounds vary from 10, 12, 14 depends on the key size 128, 192, 256 respectively. The 128 bit image block is divided in to 16 bytes. These bytes are mapped in to 4x4 arrays called states. All the internal operations of AES algorithm are performed on the states. In AES encryption and decryption each round consist four transformations. The transformation performed on the state are similar among all versions but the number of transformation rounds depends on the cipher key length. The final Aes differ slightly from the first $N_r-1$ rounds as it has one less transformation performed on the state. Each round of AES cipher consists of following rounds:

- **Sub bytes**
- **Shift rows**
- **Mix columns**
- **Add round key.**

**Sub bytes:** Operates in each byte of state independently. Each byte is substituted by corresponding byte in S-box.

**Shift rows:** Cyclically shift the rows of the state over different offsets.

**Mix columns:** This transformation operates on column of the state. Each column of states are considered as polynomial over $GF(2^8)$ and are multiplied with fixed polynomial. The mix column does not operate in last round of the algorithm.

**Add round key:** This involves bit wise XOR operation.

The key used in AES algorithm can be easily hacked using statistical analysis, so we have to go for advanced AES encryption [1]. This scheme uses random key generator to generate 128 bit key, using this 128 bit key generated the shares are encrypted. This scheme provides better security.

![Random Key Generator](Figure 5: Advance AES Encryption [1])

The above figure shows the Advanced AES scheme. The 128 bit key generator is used to generate key, using this key the plain image is converted in to cipher image using traditional AES encryption algorithm as discussed above.

5. PROPOSED SYSTEM

In visual cryptography scheme for color image, the secrete image is separated in to individual R,G,B component and Jarvis error diffusion algorithm is applied to each component to get binary half tone image, then 2x2 visual cryptography is applied to each halftone component to get secret shares of each component, then the secret shares are encrypted using Advanced AES encryption and the encrypted shares are transmitted to receiver side.
Thus our proposed scheme uses both visual cryptography technique and Advance AES algorithm to provide double layer security for images with less distortion.

6. RESULT & DISCUSSION

The R, G, B component are separated for the secrete image then, the each channel is treated as gray-scale image to which the halftone and Visual cryptography are applied independently. After the binary shares are generated for each channel, the channels after de-noising are combined to create the RGB image.

In receiver sides the encrypted shares are decrypted and decrypted shares are super imposed using XOR operation and then the superimposed shares are sub sampled to get the original halftone R, G, B component. ROF de noiseing algorithm is applied to each halftone component, then R,G,B components are combined to get the original secrete image with less distortion.

![Flow Diagram of Proposed System-sender Side](image1)

![RGB Components of Original Image](image2)

![Flow Diagram of Proposed System-receiver Side](image3)

![Halftone RGB Components](image4)
The shares are decrypted in receiver side and the shares are superimposed using XOR operation to get the original secrete image. The halftone images contain noise so Rudin-Osher-Fatemi (ROF) de-noising algorithm is applied to reduce noise. The denoised RGB components are combined to get the original secrete image.

The above generated shares are encrypted using advanced AES encryption and then send to receiver. The encrypted shares of RED, GREEN, BLUE shares are shown below respectively.

<table>
<thead>
<tr>
<th>Table 1</th>
<th>PSNR Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Components</td>
<td>PSNR value for image using color error diffusion</td>
</tr>
<tr>
<td>RED</td>
<td>25.49</td>
</tr>
<tr>
<td>GREEN</td>
<td>25.45</td>
</tr>
<tr>
<td>BLUE</td>
<td>25.43</td>
</tr>
</tbody>
</table>

The PSNR values are calculated shown above for image obtained by color error diffusion method and for the image obtained by the proposed system. The values calculated shows that the proposed system gives high resolution output.

7. CONCLUSION AND FUTURE WORK

The proposed visual cryptography scheme for the color images uses the Jarvis error diffusion dithering on color channels. The use of ROF algorithm...
improves the quality of image. The XOR operation is used in stacking which produces the better quality of image and there is no expansion in the size of image. The quality of decrypted image will be better than the other schemes which use different dithering techniques. This has been proved by experimental results obtained by using PSNR. The use of advanced AES encryption provides better security, the shares generated by visual cryptography is encrypted using advanced AES so the secrete image is transferred with double layer security. Further work can be done to reduce the time taken to encrypt the shares generated and improve the quality of halftone shares.

REFERENCES