International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 10 (2015) pp. 25909-25916

http://www.ripublication.com

Enhancement of Security In Block Based Visual Secret Sharing

G.Shoban Raj[1], Dr.K.R.Manjula[2]
[1]*Department of ADC, School of Computing, SASTRA University, Thanjavur, India.*
[2]*Senior Assistant Professor, School of Computing, SASTRA University, Thanjavur, India.*
E-mail: shobanraj.raj@gmail.com, manjula@cse.sastra.edu

Abstract

Block based Visual Secret Sharing technology is one of the advanced technologies for image encryption scheme, in which human visual system is used to recover the encoded image. In our proposed system, images are decomposed in to different shares and added with a fixed value in the interval of 0/1s. Thus it will make all shares in to similar sizes. Blocks are not expanded in the existing system, though they achieved 50% as their image quality. Hence in our paper, quality of image is improved when comparing to the existing system. Security of the image also enhanced by using DES Rijndael Managed technology to scrambled the pixel values. Similarly in the decryption process, same security features will be used to construct the image from different blocks. Therefore, security of image transmission is ensured. The main advantage of the paper is (i) image can be partitioned as much as possible, (ii) both gray scale and color image can be used, (iii) contrast of the image shares also improved to give good visual ability to the human eye.

Keywords: Steganography, DES, Visual Cryptography, Visual Secret Sharing

Introduction

The visual secret sharing process was introduced by shamir and Moni naor [1] for the application of the picture information in cryptographic technology. Comparing the previous works on encryption and decryption process, VSS possess the advantagesof using the human visual system to decode the secret information's, without any room for hard numerical methods. VSS can be applied to hide information [2] and digital water-marking [3, 4, 5]. In existing process the images are additionally distributed into n shares, and hence quality of blocks expands.The substance of the secret picture is uncovered by step by step process. Security for an image is must when transferring an image form one into another. The reason is that a single image which when viewed

visually can provide a lot of information. These information are much worthier and can cause severe problems when they are hacked thus they need for their security in an image place a predominate role. In this paper security is improved by using the private key through DES Rijndael managed algorithm. The main advantage of these algorithms is the location of the pixels cannot be identified after the completion of shuffling process. This shuffling process is carried over through java object.

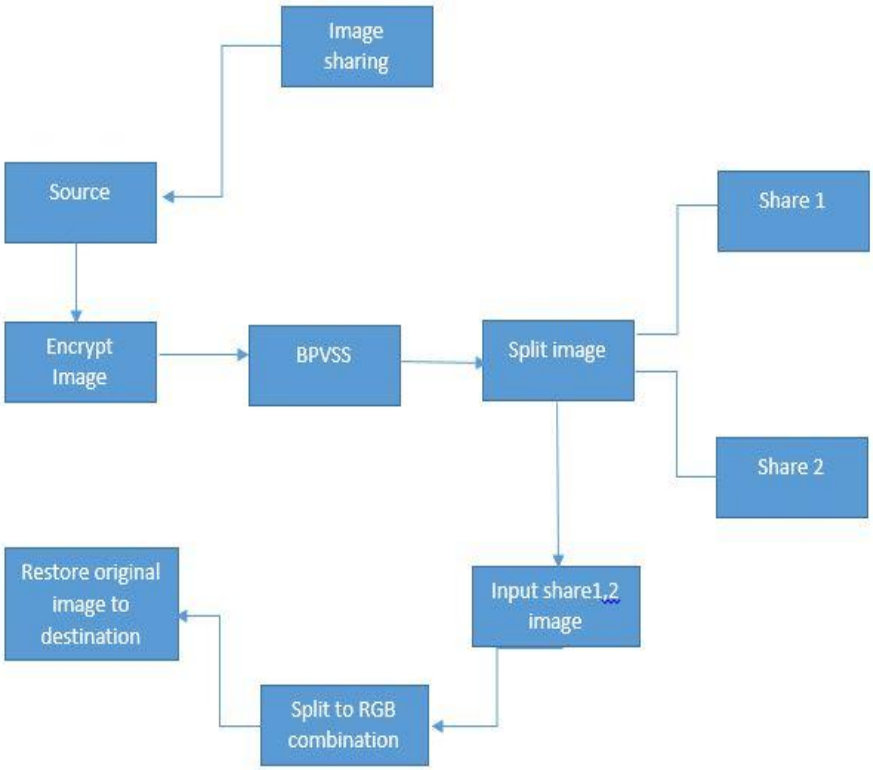
The enhancement of block based secret sharing to be enhanced by its security featuresbut in the previous works had some defects of their security features and their image qualities

1. Since no of shares increases, the relived undisclosed image and super-imposed shares quality decreases which is less than 60%
2. These sharing matrices forms the difficulties to given matrix configuration. Hence restricting the quantity of the members.

Related Works

It is not necessary to embed the watermark, since it generates secret image and public image and the watermark can be recovered through XOR operation. This scheme is robust to noise, cropping and certain blurring attacks [6]. (2, n) secret sharing scheme generates rebuild signal image and also generates random shadows of gray scales [7]. Successive progressive of image sharing is done. The main advantage of this method is faster decoding and a clear distinguish is shown such that their respective shares can be found [8]. VCRGn is a simple encoding technique where pixel expansion is not needed and hence this algorithm is practically applicable [9]. During image sharing pixel expansion and lossy compression are the two main problems. These can be overcome by using linear equations to divide the images into sub categories. Random grid plays a vital role in reconstruction of images [10]. VSS plays a vital role in preventing the undisclosed image. But increasing contrast became a major problem. To overcome this white pixels are implemented thus improving the contrast [11]. In visual secret sharing pixel expansion became a major problem. (k.n) VSS scheme is presented and its value is set to 1, so that no pixel expansion is required [12]. Analyzing the structure of schemes of visual cryptography and considering graph based structures makes sharing of images clear [13]. Novel visual secret sharing scheme is planned in this share blocks are generated and visual patterns are characterized to generate two share images. The main advantage is that the secret images are not restricted in terms with number [14].

Block Diagram For Visual Secret Sharing



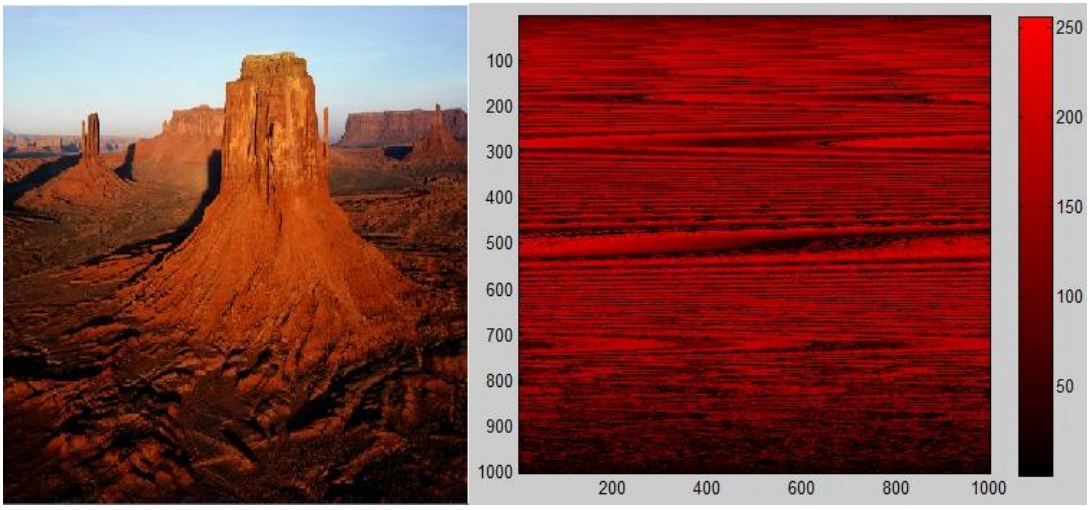
The image which has to be shared is made to act as a source. The source is encrypted using Data Encryption Standard (DES) - Rijndael managed algorithm. The images are made be divided to Red, Green and Blue color. These algorithms per mutate the pixels of an image through shuffling or scrambling. Thus the alignment of the pixel gets changed and hence the original image gets changed. This is the path for encryption and they are divided into many shares. No one can identify where the pixel is. Here we have implemented the concept for two shares. During the decryption process of Data Encryption Standard (DES) - Rijndael managed algorithm the shared image is read and they are separated as Red, Blue and Green in color. Then the images are stacked over the other. The original image is read by sharing a private key.

Des Rijndael Managed Algorithm

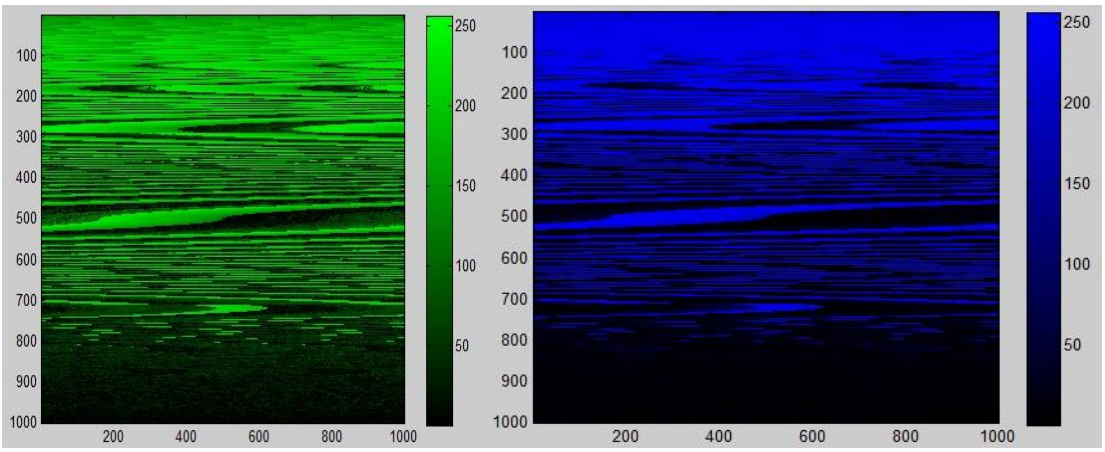
Rijndael is also known as Advanced Encryption Standard (AES), since it was selected as a candidate by U.S National Institute of Standards and Technology. AES comes under the category of symmetric key algorithm. In case of symmetric key algorithm, a single key is employed during encryption and decryption purposes. Substitution-Permutation Network is the basic concept of Advanced Encryption Standard. The block size of AES is 128 bits, which is fixed. Rijndael succeed Data Encryption

Standard (DES). DES is known for its tough Cryptography. The key length of DES is of 56 bits. DES is a block cipher. Brute Force attack is a well known one, since it is used to retrieve the hidden or secret information. It tries to decrypt the encrypted data with various possible keys. Rijndael algorithm is against Brute Force attacks. This is possible, since the key size is greater than 128 bit.

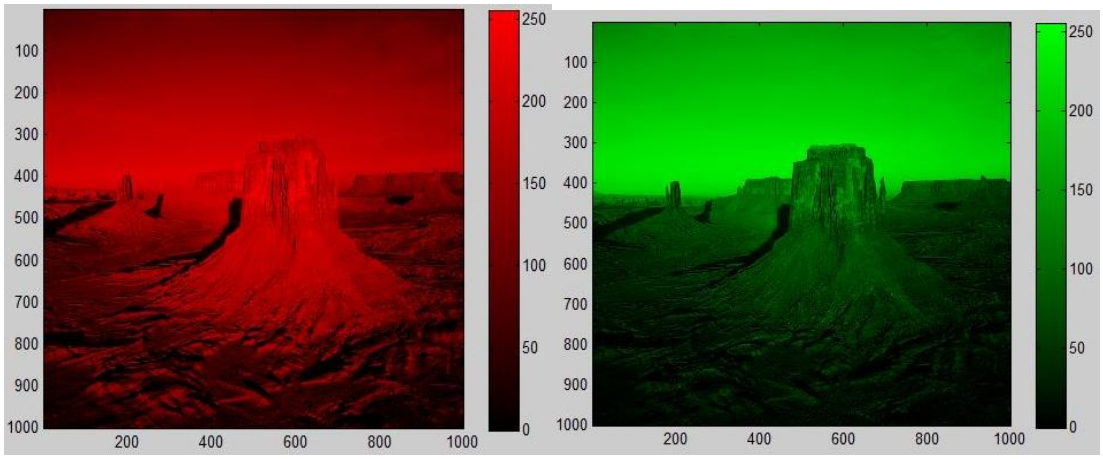
Here the image is taken as an input. The image is encrypted. They are separated into three colors named Red, Green and Blue. Then the pixels values are shuffled by calling Java Object. Thus there are termed as Share1 image and Share 2 images. Then these two split images are read. Again Red, Green and Blue color separation is done. The pixels values are shuffled once again and are decrypted to get an original image.



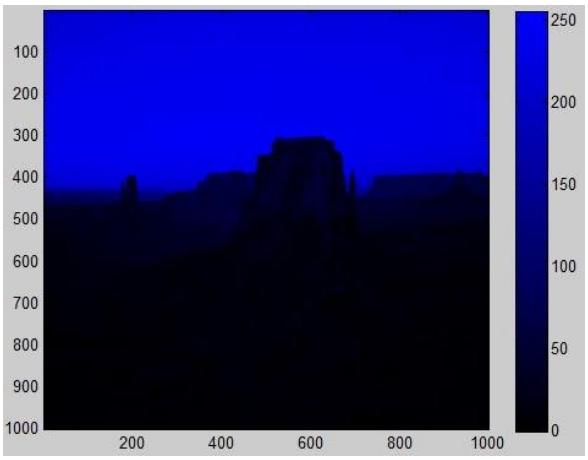
(a) (b)



(c) (d)



(e) (f)



(g)

Figure: (a) represents an input image. Later the images are separated into Red, Green and Blue in color. Using Java Object their pixels are shuffled and is shown in the figure (b), (c) and (d). Hence part of Encryption ends. Then the images are stacked and are read in the form of Red, Green and Blue in color and pixels are rearranged. They are shown in the figure (e), (f) and (g). Thus decryption is done and original image is obtained.

Encryption

Step-1: Input image
Step-2: Encryption
Step-3: Red, Green and Blue color separation
Step-4: Reshuffling of Pixels
Step-5: Obtaining two split images
Step-6: Process of encryption ends with a single private key
//Get the image name from the user
//Read the image name

```
//Separate Red, Green and Blue color by using
red=img(:,:,1)
//Concatenate the image by using
imag= cat(3,red,green,blue);
//shuffle the image by calling javaObject
obj=javaObject('diag_tra'); ‘diag_tra’ is the class name of java program
Example red
di_red=(obj.shufj(red,size(red,1)))
//Concatenate the image and write the image
di_imag=cat(3,(di_red),(di_green),(di_blue))
imwrite(uint8(di_imag),'di_img.png');
//Share1 image is obtained by
red1=di_red(1:size(di_red,1),1:(size(di_red,2)/2))
green1=di_green(1:size(di_green,1),1:(size(di_green,2)/2))
blue1=di_blue(1:size(di_blue,1),1:(size(di_blue,2)/2))
//Share2 image is obtained by
red2=di_red(1:size(di_red,1),((size(di_red,2)/2)+1):size(di_red,2));
green2=di_green(1:size(di_green,1),((size(di_green,2)/2)+1):size(di_green,2));
blue2=di_blue(1:size(di_blue,1),((size(di_blue,2)/2)+1):size(di_blue,2));
```

Decryption

```
Step-1: Split image is taken as an input
Step-2: Realignment of Pixels in an ordered manner
Step-3: Red, Green and Blue color separation
Step-4: Stacking of shares
Step-5: Same private key is used for decryption
Step-6: End result is obtaining an original image.
//Read Share1 Image
 img_d_1=imread(‘share1.png’);
//Red, Green and Blur color separation
Example for Green
s_g_1=img_d_1(:,:,2)
//Read Share2 Image
img_d_2=imread(‘share2.png’);
//Red, Green and Blur color separation
Example for Red
s_r_2=img_d_2(:,:,1)
//combining image of share1 and share2
c_r=horzcat(s_r_1,s_r_2);
c_g=horzcat(s_g_1,s_g_2);
c_b=horzcat(s_b_1,s_b_2);
if(red==even)
{
Swap green(1) with blue(n-1+1)
}
```

```
//call javaObject to reshuffle the image
Example red
r_di_red=(obj.reshuf(c_r,size(c_r,1)));
//Concatenate the shuffled values to get original image
org_img=cat(3,r_di_red,r_di_green,r_di_blue);
//write the obtained image
imwrite(uint8(org_img),'orginal.png');
```

Results and Discussion

An image is encrypted. Then the image is separated according to colors like Red, Green and Blue. Java Object is called to shuffle the pixels. Thus the images are in a sliced manner. Now, the sliced images are arranged into stacks. They are split into two images named Share1 image and share2 image. These procedures help us to get rid form the security issues. Even though the image is hacked, it is very difficult to identify the arrangement of pixels. Main advantage of this procedure is that complex encryption is obtained without any complicated Mathematics. It also handles Brute Force Attack. Thus, DES Rjndael managed algorithm provides good Security and thus enhancing Reliability.

Conclusion

Hackers play a predominant role in breaking the encrypted image. The broken information's are revealed and this results in heavy loss. Thus it causes a major threat to the users. Hence, there is a much demand for security issues. This paper provides good security by slicing and shuffling the image which is taken as input. Even though the single key which is used during the process of encryption and decryption is broken, rearrangement of pixels of an image is a herculean task.

References

[1] C.S. Hsu, S.F. Tu, Y.C. Hou, A document protection scheme using innocuous messages as camouflage, WSEAS Transactions on Information Science and Applications, vol 6, issue 4, pp 694-703, 2009.

[2] C.S. Hsu, Y.C. Hou, Copyright protection scheme for digital images using visual cryptography and sampling methods, Optical Engineering, vol 44, issue 7, pp 1-10, 2005.

[3] Ching-Nung Yang, "New visual secret sharing schemes using probabilistic method", Pattern Recognition, vol 25, pp 481–494, 2004

[4] D.C. Lou, H.K. Tso, J.L. Liu, A copyright protection scheme for digital images using visual cryptography technique, Computer Standards & Interfaces, vol 29, pp 125–131, 2011.

[5] Daoshun Wang, Feng Yi and Xiaobo Li, "Probabilistic visual secret sharing schemes for grey-scale images and color images", Information Sciences, vol 181, pp 2189–2208, 2011.

[6] Der-Chyuan Lou, Hao-Kuan Tso and Jiang-Lung Liu, "A copyright protection scheme for digital images using visual cryptography technique", Computer Standards & Interfaces, vol 29 , pp 125–131, 2007

[7] Giuseppe Ateniese, Carlo Blundo and Alfredo De Santis and Douglas R. Stinson, "Visual Cryptography for General Access Structures", Information and Computation, vol 129, pp 86 to106, 1996.

[8] Jen-Bang Feng, Hsien-Chu Wu, Chwei-Shyong Tsai, Ya-Fen Chang and Yen-Ping Chu, "Visual secret sharing for multiple secrets", Pattern Recognition, vol41, pp 3572 – 3581, 2008

[9] M. Naor, A. Shamir, Visual cryptography, in: Advances in Cryptology-EUROCRYPT '94, LNCS, vol. 950, Springer-Verlag, pp. 1–12, 1995.

[10] Shyong Jian Shyu, "Image encryption by multipler and omgrids", Pattern Recognition, vol 42, pp 1582 – 1596, 2009.

[11] T. Hoang Ngan Le, Chia-Chen Lin, Chin-Chen Chang and Hoai Bac Le, "A high quality and small shadow size visual secret sharing scheme based on hybrid strategy for grayscale images", Digital Signal Processing, vol 21, pp 34–745, 2011

[12] Wei-Kuei Chen, "Image sharing method for gray-level images", The Journal of Systems and Software, vol 86, pp 581– 585, 2013

[13] Wen-Pinn Fang, "Friendly progressive visual secret sharing", Pattern Recognition, vol 41, pp 1410 – 1414, 2008

[14] Y.C. Hou, P.H. Huang, An ownership protection scheme based on visual cryptography and the law of large numbers, International Journal of Innovative Computing, Information and Control, vol 8, issue 6, pp 4147-4156, 2012.