Volume 4, Issue 12, December 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

# An Overview of Keyless Image Encryption Technique

**Ranjith C**
PG Scholar, Dept. of CSE,
NMAMIT, Nitte, India

**Manjunath Kamath**
Asst. Professor, Dept. of CSE
NMAMIT, Nitte, India

***Abstract— Nowadays maintaining the security as well as the confidentiality of the images is a dynamic area of research. To maintain these aspects usually two approaches being followed. Firstly encrypting the images using an encryption algorithm by using keys and secondly dividing the images into shares in order to maintain the secrecy of images. However, the former approach is that it involves complex computation and the management of the keys. Improper recovery of the images limits the application of latter approach. In this paper, we discuss and compare the various approaches to encrypt and decrypt an image without using the keys. Finally the SDS algorithm is explained which will generate the random shares with a minimal computation such that the original image is retrieved from the random shares in totality without any loss in image quality.***

***Keywords — Random Shares, Encryption, Decryption, Visual Cryptography, Sieving, Division, Shuffling, Combining.***

## I. INTRODUCTION

The emerging popularity of the internet given a new dimension to the people to think about how data from one party to another party get shared in real time. The Secrecy and the Confidentiality are the major challenges which arise while transferring the data from one party to another party in real time. The major research area is how the cryptographic technique helps into resolve these challenges.

The algorithms such as RSA, DES etc. which are the traditional method of encrypting the images was found to be unsuitable for the bulk sized images and the correlation amongst the pixels [1]. This gave rise to a new approach for encrypting the images. Encryption of images is classified into two different kinds of approaches depending upon the quality of the image regained after decryption. They are 1) Image Encryption using keys and 2) Image Splitting.

***Encryption of images using keys:*** This is a conventional method of encrypting the images using algorithms (and keys). Some of the techniques for image encryption are "Digital Signatures" [2], "Chaos Theory" [3], "Vector Quantization" [4] etc. The disadvantages of these techniques are the use of secret keys and the management of the keys. However, the main advantage of these techniques is the regaining of image in totality.

***Splitting of image:*** This approach deals with splitting of an image into two or more random shares at the pixel level such that the generated random shares don't convey any information about the secret image. However, the secret image can be regained from the generated random shares. In 1979, Adi Shamir [5] introduced the concept of dividing the data into multiple shares. Naor and Shamir [6] in 1995 proposed the concept of "Visual Cryptography", which deals with dividing the image into multiple shares and sharing these generated shares in a secure manner. The limitation of the above schemes is the poor quality of the recovered image. The benefit of these schemes is, key management is not required and decryption involves no computation.

To overcome the limitations of these approaches a new scheme is discussed in this paper which involves encryption and decryption of the images without using keys which aims in regaining an image in totality after the decryption. This scheme involves low computation in encryption and decryption process, low bandwidth and storage requirements.

## II. DIFFERENT KEYLESS ENCRYPTION TECHNIQUES

The concept of image splitting is usually referred as Visual Cryptography Scheme (VCS), which involves splitting of an image into several random shares. The generated random shares don't reveal any information about the secret shares. However, the original image can be recovered back by stacking up the generated random shares. The main limitations of this approach is that the poor quality of the recovered image and the minimal representation of the colour. Many researchers worked regarding this issue, starting from binary image [6] to grey scale image [7] and finally to the colour image [8].

Visual Cryptography is a new type of cryptographic scheme in which an image is recovered from generated random shares with no cryptographic computation. The scheme is secure and easy to implement. Suppose if *n* number of shares is generated from an image, the generated random shares don't reveal any information about the image. The original image is not revealed even if *n-1* shares out of *n* shares are used. Hence to recover an original image all the *n* shares must be required [6].

 

Tzung-Her Chen et al. in [7] proposed a new scheme of encrypting a multiple image by rotating random grids. In this scheme the two secret images are encrypted into two random grids without any pixel expansion. Further the secret images are recovered by stacking the generated random grids and rotating the random grids into several degrees such as 90, 180 or 270 degrees. This scheme is also applied for halftone as well as for colour images. The strength of this proposed scheme is no extra codebook redesigned, no extra pixel expansion, saving of bandwidth and storage, and applicable for wide image format.

Hsien-Chu Wu et al. in [8] proposed a Colour Visual Cryptography Scheme Using Meaningful Shares. In this scheme they proposed a generation of meaningful shares using Colour Visual Cryptography. Since the generated shares are meaningful, the shares don't draw the attention of the hackers and thus provides a high level security. The secret image can be recovered by stacking up the meaningful shares.

Since in all the above techniques discussed, the quality of the recovered image is improved, but none of the techniques provide a solution to recover the exact copy of the secret image. When evaluating the performance of the above suggested solutions, they are often evaluated on the performance factors such as accuracy, computational complexity, contrast, security etc. Hence, an ideal solution is to recover an original image from the generated random shares.

Siddharth Malik et al. in [9] proposed a SDS algorithm to encrypt the image without using any keys. In this technique an image is splitted into random shares and the secret image is recovered back by using all the generated random shares. The SDS (Sieving, Division, Shuffling) algorithm involves 3 steps. In the first step, the secret image is split into primary colours. In the second step, the split images are divided randomly. In the third step, the divided shares are shuffled within itself. Ultimately these shuffled shares are combined to generate the desired random shares. The steps involved in generating two random shares during encryption are depicted in Figure 1.

There are two most preferred models for the representation of colours, additive and subtractive colour models. In the additive colour models or RGB, the three primary colours namely Red, Green, and Blue colours are mixed to get the desired colours. The example for the additive colour model is the colours that visible on the computer monitor. While in the subtractive colour model or CMY, Cyan, Magenta, and Yellow pigments are used to get the desired colours. This subtractive colour model is widely used in printers [9].

Since the results of encryption and decryption proposed in the technique [9] are viewed on the computer monitors hence, it is natural to use the additive colours in the proposed technique.

The encryption process of the SDS algorithm is as follows

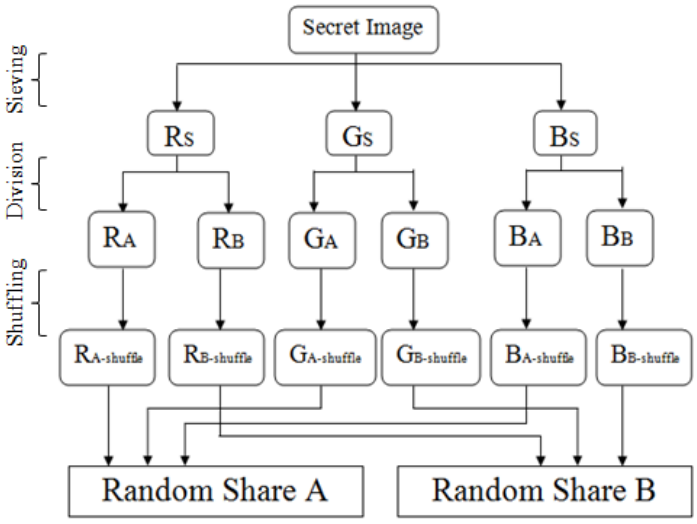


Fig. 1 Steps involved in encryption of a secret image to generate two random shares.

***Sieving:*** In this process the secret image is filtered into three primary components namely, R, G and B. Sieving uses XOR operator to make the process computationally inexpensive.

***Division:*** After sieving process the next step is to divide the R, G, and B components into z parts/ shares each.

$$\mathbf{R \rightarrow (R_A, R_B, R_C, \ldots\ldots\ldots\ldots, Rz)}$$
$$\mathbf{G \rightarrow (G_A, G_B, G_C, \ldots\ldots\ldots\ldots, G_Z)}$$
$$\mathbf{B \rightarrow (B_A, B_B, B_C, \ldots\ldots\ldots\ldots, B_Z)}$$

While dividing it should be taken care each element in $R_{A\text{-}Z}$, $G_{A\text{-}Z}$, and $B_{A\text{-}Z}$ is assigned with a random values, such that entire domain is available for random selection.

***Shuffling:*** Since the generated random shares doesn't reveal any information about the original image, to provide more security a shuffle operation is performed. In this process the elements within the individual shares are shuffled with respect to the value of the other shares generated from the same primary colours.

After performing the above three operations the final random shares are generated from the shuffled shares. The random share doesn't convey any information about the original image. However, to obtain the original image all the generated random shares are required.

 

The decryption process of the SDS algorithm is as follows

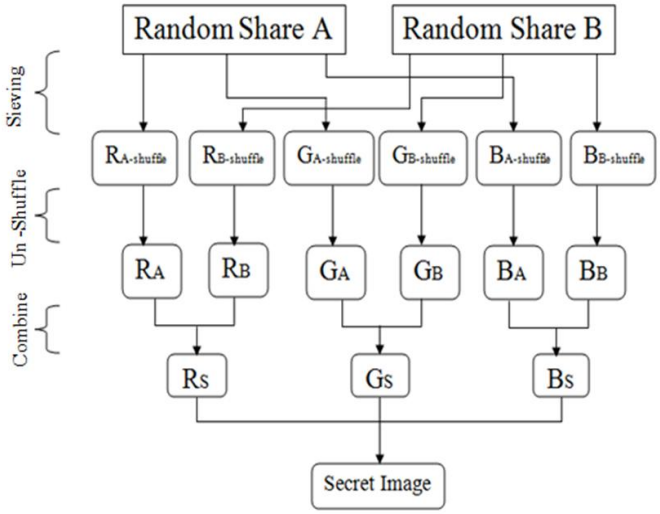


Figure 2: Steps involved in decryption of random shares to retrieve secret image.

***Sieving:*** In the decryption process the resultant random shares of encryption is Sieved and the R/G/B (shuffle) components are retrieved.

***Un-shuffle:*** In the decryption process sieving of random shares is carried out and R/G/B (A-shuffle) and R/G/B (B-shuffle) are retrieved, thereafter the individual shuffled shares are reshuffled to get the original RA, GA, BA and RB, $G_B$, $B_B$ shares.

**Combine:** Each $R_A/R_B$, $G_A/G_B$, and $B_A/B_B$ is combined using which the original image is generated.

## III. COMPARISON OF THE VISUAL CRYPTOGRAPHIC SCHEMES

The below Table I gives the comparison of the discussed four techniques. The first three techniques in the table exhibits improvement in the quality of the recovered image. They don't give an ideal solution of how the original image is recovered in totality. The fourth technique provides a solution of exact retrieval of an original image with no pixel expansion.

TABLE I COMPARISON OF VISUAL CRYPTOGRAPHY SCHEMES

| Author Year | Expansion of Pixel | No. of Secret images | Image Format | Type of share generated |
|---|---|---|---|---|
| Naor and Shamir [6]-1995 | 1 | 4 | Binary | Random |
| Tzung-Her Chen et al [7] 2008 | n(n>=2) | 4 | Binary, gray, Colour | Random |
| F. Liu et al [8] 2008 | 1 | 1 | Colour | Meaningful |
| Siddharth Malik et al. [9] 2012 | No | 1 | Colour | Random |

## IV. FUTURE RESEARCH DIRECTIONS

The SDS algorithm proposed in [9], is applied for the jpg image. However, the algorithm can be extended for other image formats such as png, gif etc. The multimedia applications are gaining popularity in the field of Computer Science and hence maintaining confidentiality of videos is also a major concern where the special properties of video data must be authenticated. The SDS algorithm can be applied to meet these confidential requirements. Video is considered to be continues sequence of images or a continuous frames of images. Thus the SDS algorithm can be applied in parallel to all the frames of images of a video. By this we can aim to encrypt and decrypt the videos without using any keys.

## V. CONCLUSIONS

In this paper, we discussed various visual cryptographic schemes which don't use any keys. Though each of the techniques has its own merits and demerits, SDS algorithm will overcome the problem of retrieving the complete image where, a secret image is divided into two or more random shares. These generated random shares are used to recover the

 

original image without any complex cryptographic computation. This technique has the following benefits: i) the exact copy of the original image is retrieved back after the decryption process, ii) The storage requirements for the generated random shares is same as that of the original image as there is no pixel expansion, iii) Key management is not required since no keys are used during encryption and the decryption process, iv) The scheme is robust to withstand brute force attack. Having these benefits, the SDS technique can be applied for various image formats and videos also.

**REFERENCES**

[1] Xin Zhang and Weibin Chen, "A new chaotic algorithm for image encryption", International Conference on Audio, Language and Image Processing, 2008. (ICALIP 2008), pp 889-892.

[2] Aloka Sinha and Kehar Singh, "A technique for image encryption using digital signature", Optics Communications(2003), 218(4-6), pp 229-234, online [http://eprint.iitd.ac.in/dspace/handle/2074/1161]

[3] S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", Pattern Recognition 34 (2001), pp 1229-1245.

[4] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encryption algorithm for image cryptosystems", The Journal of Systems and Software 58 (2001), pp. 83-91.

[5] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.

[6] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT' 94, Berlin, Germany, 1995, vol. 950, pp. 1–12, Springer-Verlag, LNCS.

[7] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multiple-Image Encryption By Rotating Random Grids", Eighth International Conference on Intelligent Systems Design and Applications, pp. 252-256 , 2008.

[8] F. Liu1, C.K. Wu X.J. Lin , "Colour Visual Cryptography Schemes", IET Information Security, vol. 2, No. 4, pp 151-165, 2008.

[9] Malik, S. ; Sardana, A. ; Jaya J. ,"A Keyless Approach to Image Encryption", Communication Systems and Network Technologies (CSNT), 2012 International Conference on DOI: 10.1109/CSNT.2012.189 pp. 879-883, 2012.

 