International Journal of Engineering Research and General Science Volume 3, Issue 3, May-June, 2015
ISSN 2091-2730

A REVIEW ON KEYLESS APPROACH TO IMAGE ENCRYPTION

Vishal Arunrao Damedhar[1], Prof. V.S. Nandedkar[2]

Department of Computer, PVPIT Bavdhan, Pune, vishal.damedhar@rediffmail.com
Department of Computer, PVPIT Bavdhan Pune, vaishu111@yahoo.com

Abstract – How data can be shared from one part of the world to the other in near real time came with the arrival of internet. Along with this they have introduced new challenges like maintaining the confidentiality of transmitting the data. This gave a boost to the research area related to cryptography. Firstly, Encryption of images with the accepted encryption algorithms had significant downside as key management was complicated and limited. Secondly, introduction to new area for encrypting images was splitting the image at its pixel level in to multiple shares. But the major drawback of this approach was that the recovered image had a poor quality. To overcome these mentioned drawbacks we have proposed a new approach which does not attempt to use any type of keys for encryption.

Keywords - Combining, Division, Image Encryption, Image Decryption, Random shares, Sieving, Shuffling.

INTRODUCTION

Maintaining the secrecy and confidentiality of an image is a listless area of study. Two different methods are being followed. Firstly, encrypting the images by using any encryption algorithm with the help of keys and secondly, dividing the image into possible random shares in order to maintain the image secrecy. Further the nature of the recovered image can be classified as lossy or lossless image encryption. Thus this gave rise to two different approaches for maintaining the secrecy of an image.

Encryption of image with the use of keys:

The conventional method and this method use an algorithm and a key for encrypting images. Some of the techniques which are being used are Digital Signatures Chaos Theory etc. There are some innate disadvantages with the said techniques; the key management is limited as they rivet the use of secret key and the computation cost is also high. Conversely the greatest advantage is that in most of the designs the original image is recovered entirely.

Image Splitting

This approach in primitive form includes splitting an image in to multiple shares may be two or more at its pixel level. The shares of the split images express no information about the original image, but eligible set of shares when combined will produce the original image.
The main disadvantage of this approach was that the image recovered was very poor in quality. To trounce the limitations of these approaches we put forward a new scheme, in which the quality of the recovered image is same as it that of the original image. Many research papers have been published using this approach, starting from a binary image [9] moving to grey scale image and finally employing it to color images. Also in our proposed scheme we do not use any kind of key for encryption which eventually reduces the bandwidth requirement and computational cost.

Mixed Approach

Splitting of an image into random shares with the help of using some kind of encryption key comes under his approach. Incze et al. suggested the concept of sieves for the purpose of encrypting images. In general sieve is a type of binary key. In order to form the shares the original image is placed over the sieve, pixels from the original image goes through and form one share and the pixels that do not cross will form the other share. From the study of cryptographic approaches which involves low computation cost and keyless management guided us to take fresh approach.

Visual Cryptography

It is a technique in which encrypts visual information like picture, text in such a way that decryption can be done by human visual systems without the support of computers. Simple algorithms are used; there is no need of cryptography data or complex computations. When concerning security issues it makes certain that hackers do not obtain any clues about the secret image from original image. Visual information like pictures and text which are secret are taken as image and a simple algorithm is used to encrypt to produce n copies of shares. The simplest method is creating a two by two structure scheme in which the secret image is divided in to two shares. Both the shares are required for decryption. The generated shares are dots in random which do not reveal any information about the secret image.

Visual Cryptography is a way of sharing secret images together with a group of members, where definite group combine to get back the original image. The decryption process is fast and easy as the shares are put on transparencies to get back the shared image. The computation cost is also very low

Scope and Objectives

The foremost objective of this approach is to encrypt an image without using any type of key. In this scheme the secret image is split into multiple random images and then combined back to form the original image. This results in low computation cost. Here the Sieving, division and shuffling process is used to generate random shares.

LITERATURE SURVEY

Image Encryption means that, convert the image into unreadable format. Digital visual data is organized into rectangular arrays-frames. Elements of array are denoted as pixel. Each pixel is a numerical value. In "Digital Signatures" [1], the digital signature issued to encrypt the message by adding it, bit-wise, to the encoded version of the original image. The digital signature is treated like additive noise, which can be recovered at the receiver end. To be able to recover the digital signature, an error control code is used to encode the original image. An error control code takes in the original image and adds redundancy in a known manner so that the bits corrupted by noise can be recovered. In our case, the digital signature is the noise that is added to the image after error control coding. The addition operation is equivalent to the XOR operation. We have used the BCH error control code to encode our original image. The original image is used to compute the digital signature. The image is then encoded using an appropriate BCH code. The digital signature is added block wise to the encoded image. The resulting image is the encrypted image.

"Chaos Theory" [2], the image encryption algorithm includes two steps. Firstly, the image fusion is completed between the original-image and the key-image. Then the pixel values of the fusion-image are encrypted by Henon chaotic system.

"Shared key" [3], the scheme directly works on the quantized DCT coefficients and the resulting noise-like shares are also stored in the JPEG format. The decryption process is lossless preserving the original JPEG data. Monochrome Images: The lossy version of JPEG image compression uses discrete cosine transforms (DCT). A monochrome image is first split into 8×8 non-overlapping blocks of pixels. An 8×8 DCT is applied to each block and the resulting coefficients are scalar quantized using a quantization matrix. The quantized coefficients are then converted from a two-dimensional representation to a one-dimensional vector by a process known as zigzag scanning and sent to an entropy coder that uses either Huffman or arithmetic coding. Color Images and JPEG Modes: This scheme uses the same JPEG approach to handle color images. Since the resulting image shares are JPEG images, any color space that can be handled by JPEG is also suitable for our application. JPEG supports up to 255 components in one image and hence support for a large variety of image formats.

PROPOSED TECHNIQUE

Our proposed techniques implicate dividing an image into one or more shares. The shares so produced expose no information about the original secret image and to get back the original secret image all the created shares are needed. This technique is executed with the help of sds algorithm which contains three steps.

1. The first step is the sieving process in which the primary colors of the secret images are split into Red, Green and Blue.
2. The second step is the Division process in which the split images of the secret images are randomly divided.
3. The third step is the shuffling process in which the shares of the divided secret image are shuffled among themselves.

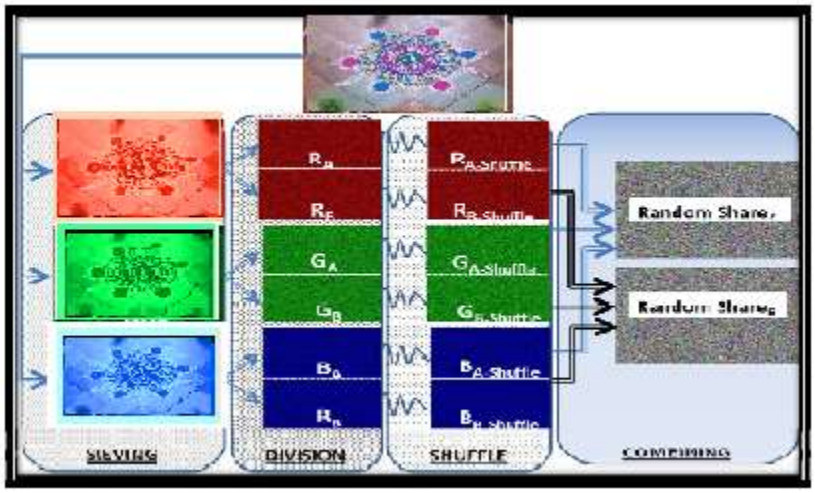

Figure1. Steps for generating random shares

In step one (Sieving) the secret image is split into primary colors. In step two (Division) these split images are randomly divided. In step three, these divided shares are then shuffled each within itself. Finally these shuffled shares are combined to generate the desired random shares. The various steps involved in generating two random shares are depicted in Figure 1. The scheme that we present here is a (z, z) threshold scheme i.e. for retrieving a secret image that has been divided into z shares all z shares are required. No shares individually convey any information about the secret image, nor do a combination of subset of random shares, the original image will only be retrieved from the complete set of random shares. The scheme implemented using the SDS (Sieve, Division, and Shuffle) algorithm involves the following three steps:

Sieving: Sieving involves filtering the combined RGB components into individual R, G and B components. The granularity of the sieve depends on the range of values that R/G/B component may take individually. To make the process computationally inexpensive, sieving uses the XOR operator.

Division: Having filtered the original image into the R, G and B components, the next step involves dividing the R, G and B components into z parts/ shares each.

R→ (RA, RB, RC, ----------, RZ)
G → (GA, GB, GC, ----------, GZ)
B → (BA, BB, BC, ----------, BZ)

Shuffling: The sequence in which the elements within the shares are shuffled depends on the value of one of the other shares generated from the same primary color. In other words RB decides how RA is shuffled, RC decides how RB is shuffled, ---------- RZ decides RZ-1 is shuffled and RA decides how Rz is shuffled. The shuffling operation uses the comparison operator on the LSB of the determining element to decide the shuffle sequence. Having carried out the above three operations the generated shares are combined to generate the final z random shares (RS).

Paper name	***A technique for image encryption using digital signature***	***A new chaotic algorithm for image encryption***	***Shared key encryption of JPEG color images***	***A Keyless Approach to Image Encryption***
Technology	Based on Digital signature	Based on Henon chaotic maps	Works on the quantized DCT coefficients	Implemented with the SDS algorithm
Working	DSS of the original image is added to the encoded version of the original image	Based on non linear systems and mapping	Encryption is done inside the DCT coefficient	It employs Sieving Division and Shuffling,

Computational speed	Fast	Low	Low	Fast
Key transmission	No need to transmit key	Key need to be transmitted to receiver	Key need to be transmitted to receiver	Keyless approach
Security	Secure	Secure	Weak security	More secure

CONCLUSION

In this paper a new encryption scheme has been brought up using VCS which is a mixed version of image encryption schemes and traditional VCS. An image is split in to random images and the combination of them retrieves the original image with low computation cost. The advantages of his scheme are that the original and the retrieved images are the same. There is no pixel expansion and thus the requirement for storage is same as that of the original image. No secret keys are involved hence there is no key management. This scheme is vigorous to any attacks. This scheme is suitable for authentication based application or where trust cannot be responded in any one participant for decision making and a collective acceptance is required to proceed. A typical scenario for this could be thought of as a secret code which has to be fed into commence of a nuclear strike, the said code could be converted into and image and split into random shares. To retrieve the secret code all participants must provide the random shares.

REFERENCES:

[1] Thomas Verbraken, Wouter Verbeke, and Bart Baesens developes ,"A Novel Profit Maximizing Metric for Measuring Classification Performance of Customer Churn Prediction Models" IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 25, NO. 5, MAY 2013

[2] Qingbo Li, Wei Wang,Xiaofeng Ling, and Jin Guang Wu , "Detection of Gastric Cancer with Fourier Transform Infrared Spectroscopy and Support Vector Machine Classification" , BioMed research international, 2013 - hindawi.com

[3] Zhen-Yu Chen, Zhi-Ping Fan, "A Hierarchical Multiple Kernel Support Vector Machine for Customer Churn Prediction Using Longitudinal Behavioural Data" European Journal of Operational Research, 2012 – Elsevier

[4] Anshuman Sharma explains," Handwritten digit Recognition using Support Vector Machine", arXiv preprint arXiv: 1203.3847, 2012 - arxiv.org

[5] Dragan Matic´, Filip Kulic´, Manuel Pineda-Sanchez , Ilija Kamenko ,"Support vector machine classifier for diagnosis in electrical machines: Application to broken bar" Expert Systems with Applications 39 (2012) 8681–8689.

[6] Ashis Pradhan "SUPPORT VECTOR MACHINE-A Survey", (ISSN 2250-2459, Volume 2, Issue 8, August 2012).

[7] Hsu, Chih-Wei, Chih-Chung Chang, and Chih-Jen Lin. "A practical guide to support vector classification", http://www.csie.ntu edu. tw/~ jlin/papers/guide/guide. pdf (2009).

[8] Theodore B. Trafalis, Huseyin Ince , "SUPPORT VECTOR MACHINE FOR REGRESSION AND APPLICATIONS TO FINANCIAL FORECASTING" IJCNN '00 Proceedings of the IEEE-INNS-ENNS International Joint Conference on Neural Networks (IJCNN'00)-Volume 6.

[9] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT' 94, Berlin, Germany, 1995, vol. 50, pp. 1–12, Springer-Verlag, LNCS.

[10] Kyung-Shik Shin, Taik Soo Lee, Hyun-jung KimAn "application of support vector machines in bankruptcy prediction model" Expert Systems with Applications 28.1 (2005): 127-135.

[11] Huang, Zan, et al. "Credit rating analysis with support vector machines and neural networks: a market comparative study." *Decision support systems* 37.4 (2004): 543-558.

[12] C.C. Thien, J.C. Lin, "Secret image sharing", Computers & Graphics, Vol. 26, No. 5, 2002, pp. 765-770