A Keyless Approach to Image Encryption

Mudassira Karishma, Raghu Kumar K S

Abstract - The advent of internet introduced to its users a new dimension as to how data can be shared from one part of the world to the other in near real time. However along with these opportunities came the challenges, such as, how to maintain the confidentiality of the data being transmitted. This gave a fillip to the already vibrant research area of cryptography. Encryption of images with the traditional encryption algorithms such as RSA, DES etc. But drawback of this approach is key management is difficult and keys for encryption are limited. This gave rise to a new area of research for encrypting images that is splitting an image at the pixel level into multiple shares (two or more), such that individually the shares convey no information about the image, but a qualified set of these shares will help to regenerate the original image. But drawback of this second approach is that is quality of the recovered image is poor. So to overcome these drawbacks propose a new approach that is encrypting the image without using any public or private keys. In this approach we are using sieving division shuffling algorithm to generate random shares. After decryption the quality of the recovered image is same as original image and low storage and bandwidth requirements needed.

Keywords: Visual Cryptography, image encryption, image decryption, Random shares, sieving, division shuffling, combining.

1 INTRODUCTION

To maintain secrecy and Maintaining the confidentiality of images is a vibrant area of research, with two different approaches being followed, the first being encrypting the images through encryption algorithms using keys, the other approach involves dividing the image into random shares to maintain the images secrecy. Encryption of images may broadly be classified based on the nature of recovered image as either lossy or lossless image encryption. This classification resulted in the following two different lines of approaches being adopted for maintaining confidentiality of images.

Mudassira Karishma is pursuing masters of technology in Department of computer science and engineering in RYMEC, BELLARY, KARNATAKA, INDIA. Emailid: kmudassira@gmail.com

Raghu Kumar K S is Asst professor in Department of computer science and engineering in RYMEC, BELLARY, KARNATAKA. INDIA. Emailed: ksraghukumar@gmail.com

Image Encryption (using keys): This approach is basically similar to the conventional encryption methods which involved using an algorithm (and a key) to encrypt an image Some of the proposed techniques for encrypting images use Digital Signatures, Chaos Theory , Vector Quantization etc. to name a few.

There are some inherent limitations with these techniques; they involve use of secret keys and thus have all the limitations as regards key management. In addition, in some cases the available keys for encryption are limited (restricted key space). Also high computation involved in encryption as also weak security functions are also an issue. However the greatest strength of most of these schemes is that the original image is recovered in totality.

Image Splitting: This approach, in a very basic form, involves splitting an image at the pixel level into multiple shares (two or more), such that individually the shares convey no information about the image, but a qualified set of these shares will help regenerate the original image (at least partially). Adi Shamir in 1979 is credited for introducing the idea of dividing a secret data into 2 random shares. In 1995, Naor and Shamir , using this as the basis, proposed the concept of Visual Cryptography, which involves secret sharing of an image by dividing it into multiple shares. The limitation of this approach is quality of recovered image is poor (including loss of contrast and colors).

To overcome the limitations of existing two approaches we propose a new scheme, through which the quality of the recovered image is maintained. In addition, this scheme does not involve use of keys for encryption, has low storage and bandwidth requirements, while also keeping the computation cost during encryption/ decryption low.

Hybrid Approach

In this approach using some kind of an encryption key the image is split into random shares. Incze et al.proposed the concept of sieves for encrypting images. Sieve is typically a binary key. The original image is placed over the sieve. Pixels from the original image situated above a hole of the sieve goes through and form one share of the image. The

pixels that stay on the sieve on a black pixel will form the other share. From the analysis of the various cryptographic approaches for images, it is appreciated that the essentials for any cryptographic scheme would involve low computation cost, recovery of original image, absence of keys and robustness. Hence these motivations guide us to take a novel approach.

Visual cryptography

Visual Cryptography is an emerging cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by human visual system, without the aid of computers. It uses a simple algorithm unlike the complex. It needs neither cryptography knowledge nor complex computation. Visual cryptography technique (for black and white images) is introduced by Naor and Shamir in 1994 during EUROCRYPT'94. For security concerns, it also ensures that hackers cannot perceive any clues about a secret image from individual cover images. Any visual secret information (pictures, text, etc) is considered as image and encryption is performed using simple algorithm to generate n copies of shares depending on type of access structure schemes. The simplest access structure is the 2 out of 2 scheme where the secret image is encrypted into 2 shares and both needed for a successful decryption. These shares are random dots without revealing the secret information. Basic visual cryptography is expansion of pixels.
Visual cryptography is a method of sharing a secret image among a group of participants, where certain group of participants is called as qualified group who may combine their shares of the image to obtain the original, and certain other group is defined as forbidden group who cannot obtain any information on the secret image, even if they combine knowledge about their parts. The scheme gives an easy and fast decryption process that is done by stacking the shares onto transparencies to reveal the shared image for visual inspection. It does not require very complicated cryptographic mechanism and computation.

Application of visual cryptography

Today the growth in the information technology, especially in computer networks such as Internet, Mobile communication, and Digital Multimedia applications such as Digital camera, handset video etc. has opened new opportunities in scientific and commercial applications. But this progress has also led to many serious problems such as hacking, duplications and malevolent usage of digital information. Being a type of secret sharing scheme, visual cryptography can be used in a number of applications including access control. For instance, a bank vault must be opened every day by three tellers, but for security purposes, it is desirable not to entrust any single individual with the combination.

Scope and objective

The main objective of this approach is to provide conventional image encryption schemes without using keys and a secret image is split into multiple random images and with minimum computation cost the original secret image can be retrieved back. The original secret image can be retrieved in totality. This approach employs Sieving, Division and Shuffling to generate random shares such that with minimal computation, the original secret image can be recovered from the random shares without any loss of image quality. The scope of this project is to encrypt the image without use of encryption keys and recover the original secret Image from random shares without any loss of image quality. . This approach employs Sieving, Division and Shuffling to generate random shares such that with minimal computation, low storage and bandwidth requirements.

2 PROPOSED SYSTEM

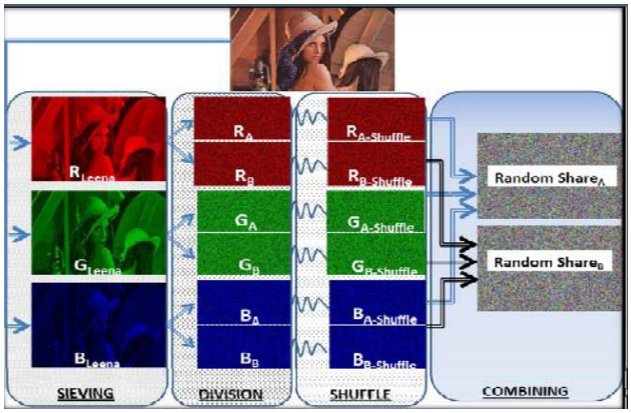
Our proposed technique involves splitting an image into multiple shares. The shares so generated reveal no information about the original secret image and to retrieve the secret image all the shares are required. The proposed technique is implemented with the SDS algorithm and involves three steps.

1. In step one (Sieving) the secret image is split into primary colors.

2. In step two (Division) these split images are randomly divided.

3. In step three (Shuffling) 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.



3 MODULES DESCRIPTION

1. User registration
2. Image Encryption
• Sieving
• Division
• Shuffling
• Combine

3. Email Sending
4. Image Decryption
• Uncombined
• Reshuffling
• Integrate & Red, Green, Blue Share Creation
• Merge Color Shares & Create Original Image

Image encryption

Sieving:

• Sieving as the name suggests involves filtering the combined RGB components into individual R, G and B components.

• The granularity of the sieve depends the range of values that R/G/B component may take individually.

• To make the process computationally inexpensive, sieving uses the XOR operator.

R	G	B
R	0	0
0	G	0
0	0	B

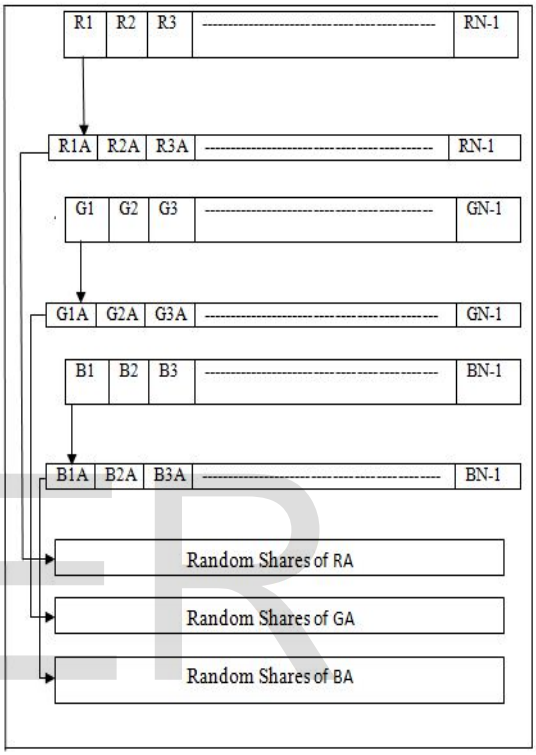
Division:

• 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)

• While dividing it is ensured that each element in RA-Z, GA-Z and BA-Z is assigned values randomly, such that the entire domain is available for randomized selection; in case x = 8, then individual elements should be randomly assigned a value varying from 0- 255.

• The shares so generated should be such that (RA, RB, RC,---------- RZ) should regenerate R and similarly for G/B components.



Shuffling:

• Though experimental results have shown that the random shares created by division in no way exhibit any resemblance to the original image, but as a second step towards randomizing the generated shares i.e. RA-Z, GA-Z and BA-Z , we perform the shuffle operation.

• This involves shuffling the elements in the individual shares. 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.

Combine:

• Having carried out the above three operations the generated shares are combined to generate the final z random shares (RS).

RSA _ (RA- shuffle, GA- shuffle and BA- shuffle)
RSB _ (RB- shuffle, GB- shuffle and BB- shuffle)
- - - -

RSZ _ (RZ,- shuffle GZ- shuffle and BZ- shuffle)
☐ The random shares so generated individually convey no information about the secret image, however to recover the original image all the random shares would be required.

Email sending

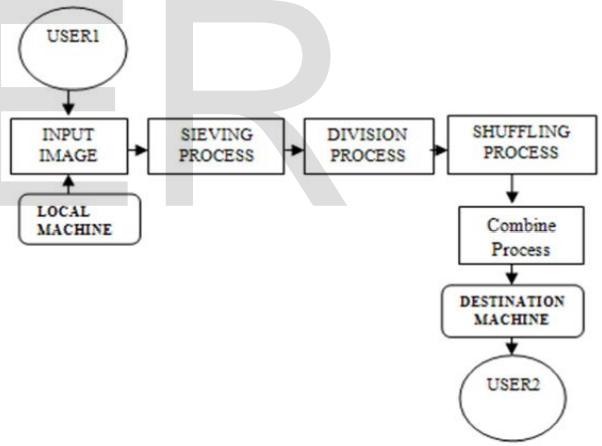
• In this model we attach any one share to send it through secure channel to authorized user and also with some message.
• Only one share will send through secure channel i e email.
• Other share can send through unsecure channel

Image decryption

This Module is used to retrieve the secret image. All the shares are required to get original Image. The Following techniques are used to decrypt the original image.
• Uncombined: Get the two encrypted shares
• Unshuffle: these uncombined shares are then unshuffled each within itself to get original image.
• Color Share Creation: the unshuffled image is split into primary colors.
• Merge: To merge the primary colors, we will get the original secret image without any loss of pixels.

SDS Algorithm

1. Sieving
Input _ Secret Image
Sieve(Secret Image)
Output _(R, G, B components)
2. Division
n = total number of pixels (0 to n-1)
Ri / Gi / Bi = individual values of the ith pixel in the R, G, B components
z = total number of random shares
x =number of bits representing each primary color
max_val = 2x
Repeat 2 for R, G, B component
2(a) for i = 0 to (n-2)
{ for share k = A to (Z-1)
Rki = Random(0, max_val)
Aggr_Sumi = _ Rki
}
Rzi =(max_val + Ri – (Aggr_Sumi % max_val)) % max_val
3. Shuffle
Repeat for RA-Z, GA-Z and BA-Z (all generated shares)
for k = A to Z
{ Rk-shuffle = Rk
PtrFirstVac = 1
PtrLastVac = n-1
For i = 1 to (n-1)
{ If (R(k+1)(i-1) is even)
{ R(k-shuffle) PtrFirstVac = Rki
PtrFirstVac ++, i++
}
Else
{ R(A-shuffle) PtrFirstVac = RAi
i++, PtrLastVac --
} } }
4. Combine
For k = A to Z
RSk = (Rk-shuffle XOR Gk-shuffle XOR Bk-shuffle)
Thus at the end of the above process we have Random shares (RSA ,RSB ---------- RSk).



4 EXPERIMENTAL RESULTS

To validate our algorithm we implemented a modified (2,2) threshold VCS. This scheme was identified to validate the results as this could have it's real world application to authenticate a user. A photograph of a user could be clicked and divided into two shares. One of the shares would be held
by the authenticating agency and the other would be held by the user who is being authenticated. The process of creating two random shares has been represented in Figure 1.

We implemented the scheme on the .net platform using C#. The scheme was run over a wide range of photographs including bright/dull, colored/black and white etc. A jpg image titled Leena.jpg is used to demonstrate the results (Figure 1). It is a 300 X 168 pixel image with an image depth of 24 bits (8
bits each for R/G/B).

5 CONCLUSION

In this paper a new enhanced encryption method is introduced using visual cryptographic scheme which is a hybrid of the traditional VCS and the conventional image encryption schemes. A secret image is split into multiple random images and with minimum computation the original secret image can be retrieved back. The proposed algorithm has the following merits (a) The original secret image can be retrieved in totality (b) There is no pixel expansion and hence storage requirement per random share is same as original image (c) Key management is not an issue since there are no secret keys involved as encryption is carried out based on the distribution of values amongst various shares (d) the scheme is robust to withstand brute force attacks.
The scheme is suitable for authentication based application or where trust cannot be reposed 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 in to commence a nuclear strike; the said code could be converted into an image and split into random shares, held with the collective decision making body. To retrieve the secret code random share of all the participants would be required.

REFERENCES

1. 1. "A Keyless approach to image encryption" Siddharth Malik, Anjali Sardana(2011).
2. 2. An improved scheme for secret image sharing Adi Shamir in 1979.
3. 3. A Hyper-chaos Based Image Encryption Algorithm Chen zaiping, Li haifen, Dong enzeng, Du yang in
4. 2010
5. 4. AlokaSinha and Kehar Singh, "A technique for image encryption using digital signature", Optics
6. communications(2003).
7. 5. S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", Pattern
8. Recognition 34 (2001), pp 1229-1245.
9. 6. X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process. Lett., vol. 18, no. 4, pp.
10. 255–258, Apr. 2011.
11. 7. Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encryption algorithm for image
12. cryptosystems", The Journal of Systems and Software 58 (2001), pp. 83-91.
13. 8. Mohammad Reza Keyvanpour, Famoosh Merrikh-Bayat in 2010 "A New Encryption Method For
14. Secure Embedding"
15. 9. Nidhi Sethi and Deepika Sharma in 2012 "A New Cryptology Approach for Image Encryption"
16. 10. Analysis on an Image Encryption Algorithm Shubo Liu1,2, Jing Sun1, Zhengquan Xu2, Jin Liu2 2008
17. 11. M. Lakshmi, S. Kavitha, keyless user defined optimal security encryptionISSN:2319-7242 Volume 2
18. Issue 6 June, 2013 Page No. 1788-1793
19. 12. Du-Shiau Tsai , GwoboaHorng , Tzung-Her Chen , Yao-Te Huang , "A Novel Secret Image Sharing
20. Scheme For True-Color Images With Size Constraint", Information Sciences 179 3247–3254 Elsevier,
21. 2009.
22. 13. Xin Zhang and Weibin Chen, "A new chaotic algorithm for image encryption", International
23. Conference on Audio, Language and Image Processing, 2008. (ICALIP 2008), pp 889-892.