SDS Algorithm for Image Sharing

Vasantha Kumari N
Department of CA
Presidency College
Bangalore,India
Vasantha.kn@gmail.com

Vinod Kumar
Department of Computer Science
City Engineering College
Bangalore
Selvamvinodh78@gmail.com

Abstract— **Maintaining the secrecy and 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. Unfortunately heavy computation cost and key management limit the employment of the first approach and the poor quality of the recovered image from the random shares limit the applications of the second approach. In this paper we propose a novel approach without the use of encryption keys. The 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.This paper also involves decryption of an image without using any keys using reverse process of SDS Technique.**

Keywords— Visual Cryptography, Sieving, Shuffling, Random shares.

INTRODUCTION

With the rapid advancement of network technology, multimedia information is transmitted over the Internet conveniently. Various confidential data such as military maps and commercial identifications are transmitted over the Internet. While using secret images,security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want .To deal with the security problems of secret images, various image secret sharing schemes have been developed.

Encryption of images with the traditional encryption algorithms such as RSA, DES etc. was found inapt due to some typicality's of images such as its bulk size as also the correlation amongst the pixels [1]. This gave rise to a new area of research for encrypting images. 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.

.

ENCRYPTION TECHNIQUES

A . Encryption technique 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" [2], "Chaos Theory" [3], "Vector Quantization" [4] 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 [5]. However the greatest strength

of most of these schemes is that the original image is recovered in totality.

B. Random shares technique : 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 [6] in 1979 is credited for introducing the idea of dividing a secret data into 2 random shares. In 1995, Naor and Shamir [7], using this as the basis, proposed the concept of "Visual Cryptography", which involves secret sharing of an image by dividing it into multiple shares. Many variations to the scheme proposed in [7] have been researched to overcome its limitations, each having their own merits and demerits. Despite the advancements made in this line of research, the quality of the recovered secret images still remains an area of concern due to the poor quality of these recovered images(including loss of contrast and colors). Despite its limitations the greatest strength of these schemes is that firstly, there is no requirement of key management and secondly the decryption involves no computation.

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. In Section 2 we present the related work followed by our proposed technique and the results in section 3 and 4 respectively. In Section 5 we compare our technique with some similar techniques.

II ENCRYPTION SYSTEM

In the past few years the security and integrity of data is the main concern. In the present scenario almost all the data is transferred over computer networks due to which it is vulnerable to various kinds of attacks. To make the data secure from various attacks and for the integrity of data we must encrypt the data before it is transmitted or stored. Government,
military, financial institution, hospitals and private business deals with confidential images about their patient (in Hospitals) , geographical areas(in research) ,enemy positions (in defense), product , financial status. Most of this information is now collected and stored on electronic computers and transmitted across network to other computer. If these confidential images about enemy positions, patient and geographical areas fall into the wrong hands, than such a breach of security could lead to declination of war, wrong treatment etc. Protecting confidential images is an ethical and legal requirement.

Cryptography is a method of storing and transmitting data in a form that only those, it is intended for can read and process. It is a science of protecting information by encoding it into an unreadable format. It is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths.

A. Image Encryption Techniques

Alok Sinha and Kehar Singh [4] have presented a new technique to encrypt an image for secure image transmission. The digital signature of the original image is added to the Encoded version of the original image. Image encoding is Done by using an appropriate error control code, such as a Bose-Chaudhuri Hochquenghem(BCH) code. At the receiver End, after the decryption of the image, the digital signature can be used to verify the authenticity of the image.

Last few decades have seen lots of schemes being proposed for image encryption using keys, some of the prominent ones have been here. Manniccam and Bourbakis [3] in 1992 proposed an image encryption and compression scheme using SCAN language. The scheme was fundamentally based on chaos theory. However this was applicable to only grey scale images. Similarly Xin and Chen [1] in 2008 following up on the work of [3], proposed a two stage image encryption scheme. Step one involved fusion of the original image and the key image and step two involved encryption of the fused image using Henon chaotic system. Chen, Hwang and Chen [4] in 2000 proposed the use of Vector Quantization (VQ) for designing a cryptosystem for images. In VQ images are first decomposed into vectors and followed by sequential encoding of these vectors. Thereafter traditional cryptosystems from commercial can be used.

B. Visual Cryptography

Noar and Shamir [1]. Introduced Visual cryptography is introduced by first in 1994. Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation. This property makes visual cryptography especially useful for the low computation load requirement.The idea of Image splitting more often referred to as Visual Cryptography Schemes (VCS) involves splitting a secret image into n random shares such that these shares individually reveal no information about the secret image (but for its size) but a qualified subset of the shares(as specified by the encrypter) when stacked up reveal the secret image. The random image shares (qualified set) are merely printed on transparencies and stacked up revealing the original image). The major issues which restrict its employment is the poor quality of the recovered image limited color representation etc.

Many research papers have been published using this approach, starting from a binary image [7, 9] moving to greyscale image [11] and finally employing it to color images[12, 13]. Though with each subsequent research paper the quality of the recovered image improved, however, but for [14] no other scheme was able to completely recover the original image from the shares. When evaluating the performances of these suggested solutions they are often evaluated on performance measures such as contrast, accuracy, security, computational complexity etc. Thus an ideal solution would regenerate the original image from the shares in terms of colors and contrast, it would also have to be secure and computationally inexpensive. Table 1 gives a comparison of six such techniques.

C. *Encryption using Hill Cipher*

This paper, has been proposed new encryption algorithm using two different images, one is cover image which acts as key image which is shared by both sender and receiver and other is Informative image. As first step, XOR cover image with informative image to obtain resultant image. The resultant image is decomposed into (n x n) blocks which passed to the Hill Cipher algorithm to form encrypted blocks. The encrypted blocks are transformed into new locations using permutation table. The Hill cipher works on groups of letters in a somewhat different manner. The Hill cipher works by viewing a group of letters as a vector, and encryption is done by matrix multiplication [12]. Each letter is first of *n* letters is then considered as a vector of n dimensions, and multiplied by an n × n matrix, modulo 26. The whole matrix is considered the cipher key, and should be random provided that the matrix is invertible (to ensure decryption is possible). A Hill cipher is another way of working out the equation of a matrix.[13]

D. Hybrid Approach

In this approach using some kind of an encryption key the image is split into random shares. Incze et al.[8] 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.

III. PROPOSED TECHNIQUE

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. 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 (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.

Figures and Tables

TABLE I. COMPARISON OF VISUAL CRYPTOGRAPHY SCHEMES

Authors Year	Pixel Expansion	Number of Secret Images	Image Format	Type of Share generated
Naor and Shamir [7]-1995	1	4	Binary	Random
Wu and Chang [9] 2005	2	4	Binary	Random
Chin-Chen et. al [10] 2005	1	4	Binary	Meaningful
Tzung-Her Chen et al [11] 2008	n(n>=2)	4	Binary, gray, Color	Random
F. Liu et al [12] 2008	1	1	Color	Random
Du-Shiau Tsai et al [13] 2009	1	9	Color	Meaningful

While representing colors, additive and the subtractive color models are the most preferred models. In the RGB or the additive model, the three primary colors i.e. Red, Green, Blue are mixed to generate the desired colors. The colors as visible on the computer monitor are an example of the additive model. Similarly when using the CMY or the subtractive model, the colors are represented by the degree of the light reflected by the colored objects. In this scheme Cyan (C) Magenta (M) and Yellow (Y) pigments are used to produce the desired range of colors. This model is extensively used in printers

Since our proposed techniques involves computation during the encryption and decryption stages and the results are to be viewed on the computer monitors hence it is natural for us to use the additive color model. It is worth mentioning that in the techniques based on [11], [12] since the shares were printed on transparencies, hence subtractive model was the natural choice for such applications.

On a monitor an image may be thought as Width X Height 2-dimensional matrix, with each entry in the matrix representing a pixel value. Each of these pixels are a series of bits composed of values representing the RGB values. 8 bit(2 bits each for R,G,B), 16 bits (4 bits each for R,G,B), 24 bits((8 bits each for R,G,B), 48 bits (16 bits each for R,G,B) etc. are some of the commonly used RGB schemes. Figure 2 represents the representation of R/G/B values for an individual

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. R_{A-Z}, G_{A-Z} and B_{A-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 R_B decides how R_A is shuffled, R_C decides how R_B is shuffled, ------------ R_Z decides R_{Z-1} is shuffled and R_A decides how Rz is shuffled. The shuffling operation uses the comparison operator on the LSB of the determining element to decide the shuffle sequence

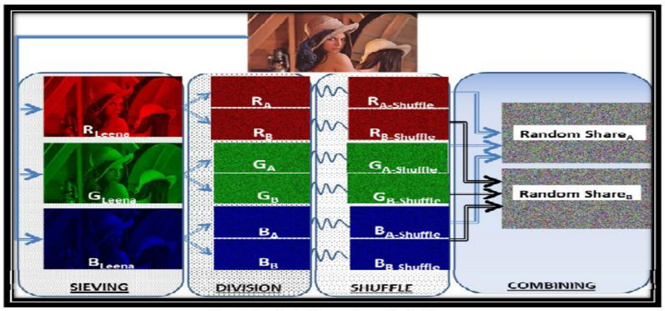

Figure 1. Steps involved in generating two Random Shares

Sieving : Sieving as the name suggests involves filtering the combined RGB components into individual R, G and B components (refer Figure 3). 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.

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 3 (R_A, R_B, R_C,----------------, R_Z)

G 3 (G_A, G_B, G_C,----------------, G_Z)

B 3 (B_A, B_B, B_C,----------------, B_Z)

While dividing it is ensured that each element in R_{A-Z}, G_{A-Z} and B_{A-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 (R_A, R_B, R_C,---------------R_Z) should regenerate R and Having carried out the above three operations the generated shares are combined to generate the final z random shares (RS).

RS_A 3 ($R_{A\text{- shuffle,}}$ $G_{A\text{- shuffle}}$ and $B_{A\text{- shuffle}}$)

RS_B 3 ($R_{B\text{- shuffle,}}$ $G_{B\text{- shuffle}}$ and $B_{B\text{- shuffle}}$)

- - - -

RS_Z 3 ($R_{Z\text{,- shuffle}}$ $G_{Z\text{- shuffle}}$ and $B_{Z\text{- shuffle}}$)

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. The generic algorithm for the above described process is as under:

Algorithm

```
1.  Sieving
    Input 3 Secret
    Image
    Sieve(Secret
    Image)
            Output 3(R, G, B components)
2.  Division
    n = total number of pixels ( 0 to n-1)
    Ri / Gi / Bi = individual values of the i^th
        pixel in the R, G, B components
        z = total number of random shares
    x =number of bits representing each
        primary color max_val = 2^x
    Repeat 2 for R, G, B
    component 2(a) for i = 0 to
        (n-2)
        {   for share k = A to (Z-1)
                $R_{ki}$ = Random(0, max_val)

            $Aggr\_Sum_i$ = 3 $R_{ki}$
        }
    $R_{zi}$ =( max_val + Ri – ($Aggr\_Sum_i$ %
        max_val)) % max_val
3.  Shuffle
    Repeat for $R_{A-Z}$, $G_{A-Z}$ and $B_{A-Z}$ (all
        generated shares)
        for k = A to Z
    {  $R_{k\text{-shuffle}}$ = $R_k$
        $PtrFirst_{Vac}$ = 1
        $PtrLast_{Vac}$ =  n-1
        For i = 1 to (n-1)
        { If ($R_{(k+1)(i-1)}$   is even)
            {  $R_{(k\text{-shuffle})\ PtrFirstVac}$ = $R_{ki}$
                $PtrFirst_{Vac}$ ++, i++
            }
          Else
            {   $R_{(A\text{-shuffle})\ PtrFirstVac}$ = $R_{Ai}$
                i++,  $PtrLast_{Vac}$ --
            }
        }
    }
4.  Combine
    For k = A to Z
        $RS_k$ = ($R_{k\text{-shuffle}}$ XOR $G_{k\text{-shuffle}}$ XOR  $B_{k\text{-shuffle}}$)
```

Thus at the end of the above process we have Random shares (RS_A ,RS_B ------------------ RS_k).

``

IV 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 bi\ each for R/G/B). The various parameters as defined in the generic algorithm above thus take the following values.

n = (300 * 168) = 50400 (n varies from 0 to 50399)

z = total random shares = 2 (Share A, B) max_val = 2^x = 2^8 = 256, x = 8

$PtrLast_{Vac}$ = (n-1) = 50399

The process of retrieving the original image involves sieving the random shares and retrieving R/G/$B_{(A\text{-shuffle})}$ and R/G/$B_{(B\text{-shuffle})}$, thereafter from the individual shuffled shares the original R_A, G_A , B_A and R_B, G_B , B_B are generated. Using these the original image is then generated. The retrieved image is same as original and no loss of picture quality occurs.

Image Decryption

This paper involves decryption ie reverse process of encryption .SDS algorithm is used in reverse process to get the Original image which is efficient and high quality without loss of any pixels.Each process of sieving ,division and shuffling is done individually to get back the image.After encryption of any image ,has to be decrypted at the other end to get back the original image.

The proposed algorithm has following merits:

1.The original secret image can be retrieved in totality.

2. There is no pixel expansion and hence storage requirement per random share is same as original image.

3. 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 .

4. The scheme is robust to withstand brute force attacks

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] S.Behnia,A.Akhshani,S.Ahadpour,H.Mahmodi,A. Akha-van, A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps,*Physics Letters* A 366(2007):391-396.

[6] A. Shamir, “How to share a secret,” *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[7] M. Naor and A. Shamir, “Visual cryptography,” in *Proc. EUROCRYPT’ 94*, Berlin, Germany, 1995, vol. 950, pp. 1–12, Springer-Verlag, LNCS.