International Journal of Current Engineering and Technology ISSN 2277 – 4106

Available at http://inpressco.com/category/ijcet

Research Article

A Secure Approach to Image Encryption of color image without using key

Shobha Patil[a*] and V.R.Udupi[b]

[a]Department of PG Studies Visvesvaraya Technological University, Belgaum, India
[b]Gogte Institute of Technology, Belagaum, India

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.

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

*Corresponding author: **Shobha Patil**

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.

1.1 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.

1.2 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.

1.3 Scope and objective

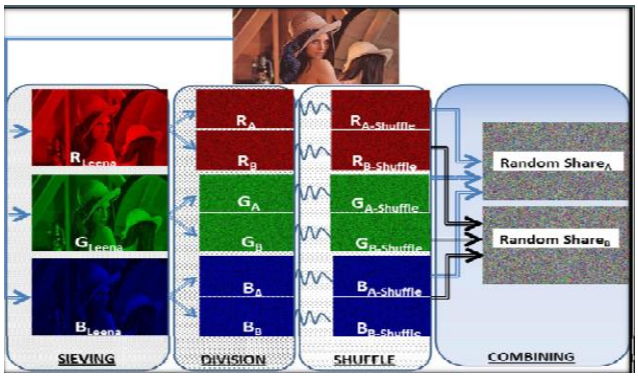
The main objective of this approach is to provide conventional image encryption schemes without using keys and a secret image is split into multiple random images and with minimum computation cost the original secret image can be retrieved back. The original secret image can be retrieved in totality. 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.



Steps involved in generating two Random Shares

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 , 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 pixel. If x be the number of bits used for representing any primary color, then a total of 23x colors can be represented by mixing the three primary colors. The values of each primary color will then vary from 0 to (2x-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.

2.1 Visual cryptography for color image

Basic principles of color

The additive and subtractive models as shown in fig 1 are commonly used to describe the constitutions of colors. In the additive system, the primaries are red, green and blue (RGB), with desired colors being obtained by mixing different RGB components. By controlling the intensity of red (green or blue) component, we can modulate the amount of red (green or blue) in the compound light. The more the mixed colored-lights, the more is the brightness of the light. When mixing all red, green and blue components with equal intensity, white color will result. The computer monitor is a good example of the additive model.

In the subtractive model, color is represented by applying the combinations of colored-lights reflected from the surface of an object (because most objects do not radiate by themselves). Take an apple under the natural light for example. The surface of the apple absorbs green and blue part of the natural light and reflects the red light to human eyes, so it becomes a red apple. By mixing cyan (C) with magenta (M) and yellow (Y) pigments, we can produce a wide range of colors. The more the pigment we add, the lower is the intensity of the light, and thus the darker is the light. This is why it is called the subtractive model. C, M and Y are the three primitive colors of pigment, which cannot be composed from other colors. The color printer is a typical application of the subtractive model.

In the additive model, any color mixed with white color is still white color. It thus seems more reasonable to use red, green, blue, and black colors to fill the blocks. On the other hand, in the subtractive model, the combination of any two of R, G, and B colors results in black color. R, G or B combined with white color will not change and can only result in the same color. Consequently, it is more appropriate to fill the blocks with cyan, magenta, yellow and white colors. In computer systems, Application Interfaces (APIs) provided by most image processing software as well as the Windows operating system are based on the RGB model. This is mainly because they use monitors as the primary output media. Monitors themselves generate color images by sending out RGB light into human's retina. In true color systems, R, G, B are each represented by 8 bits, and therefore Each single color of R, G, B can represent 0–255 variations of scale, resulting in 16.77 million possible colors. When using (R, G, B) to describe a color pixel, (0; 0; 0) represents full black and (255; 255; 255) represents full white.

In visual cryptography, we use sharing images as the decryption tool; that is, the Enal outputs are transparencies. Because the subtractive model is more suitable for printing colors on transparencies, we will use the CMY model to represent colors in what follows. Because (R, G, B) and (C, M, Y) are complementary colors, in the true color model, (R, G, B) and (C, M, Y) possess the following relationships: C = 255−R, M = 255−G, Y = 255−B: Thus, in the (C, M, Y) representation, (0; 0; 0) represents full white and (255; 255; 255) represents full black.

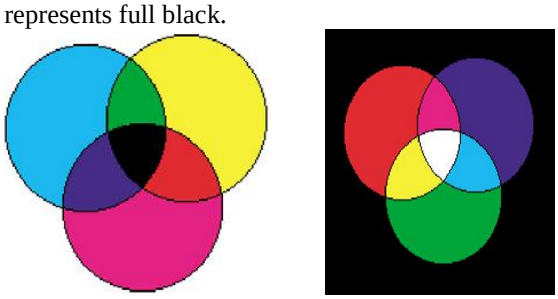


Fig. 1. (a) Additive model, and (b) Subtractive model.

2.2 Print of color

Because most color printers use C, M, Y inks to display color, a color image must be processed by the color-decomposed procedure before printing. Color decomposition mainly is to separate C, M, and Y colors from colors within every pixel of the image. These three components form three monochromatic images. (Because colored ink is expensive and the mechanical tolerances may cause the three inks to be printed slightly out of register, the black edges will suffer colored tinges. So, some printers add the black ink when printing black color,

resulting in four separate color images.) These monochromatic images are like gray-level images in which every pixel has its own color level and has to be transformed into a halftone image before printing. The three monochromatic halftone images will be (cyan, white), (magenta, white) and (yellow, white) binary images, respectively. After stacking these images, all kinds of the colors in the original image can be displayed.

3. Design And Implementation

- Image Encryption using Sieving, Division, Shuffling & Random Share Generation.
- Email Sending: This session used to send the Random Shares to other users.
- Image Decryption using Reverse process of Random Share, Shuffling, Division, Sieving.

This system has two types of users one is Admin and another is Member user.

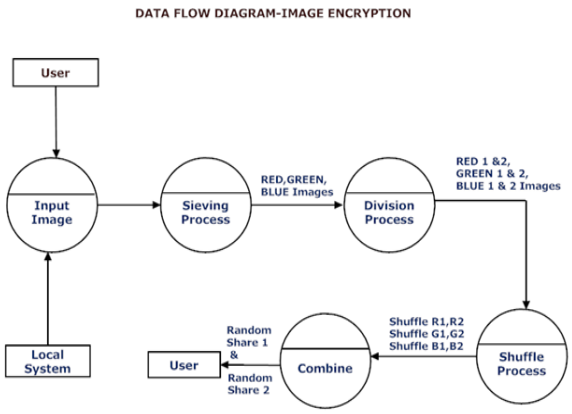


Fig. 3.1: Data flow diagram for the image encryption

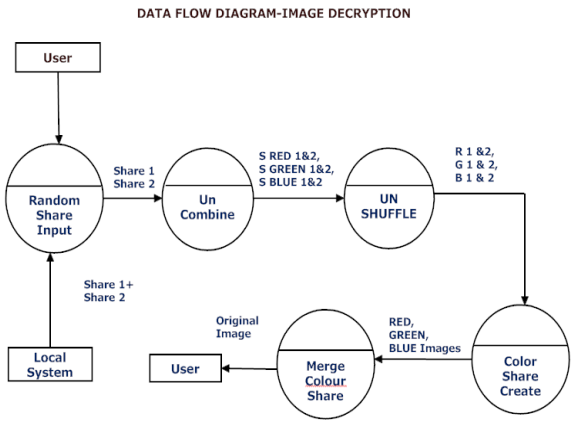


Fig. 3.2: Data flow diagram for the image decryption

Admin Session
- Login
- Profile
- Member User Creation
- Member User Details
- Change Password

Member user Session
- Login
- Image Encryption
- Email Module
- Image Decryption
- Change Password

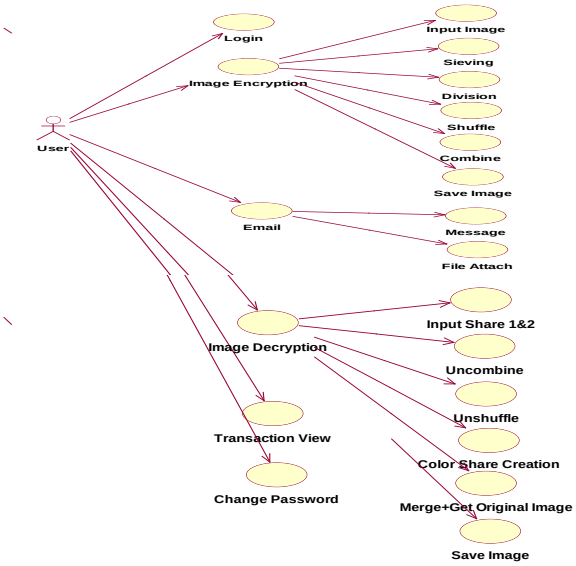


Fig. 3.3 System Architecture

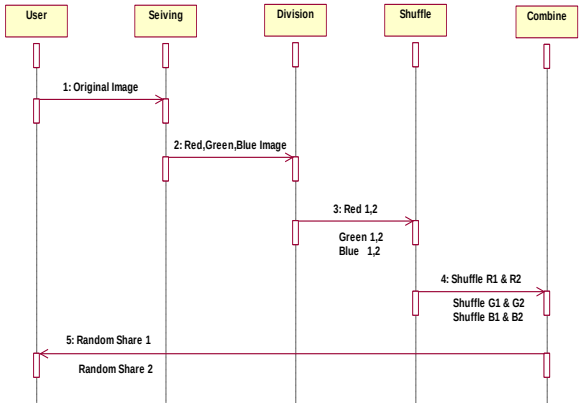


Fig. 3.3 Sequence diagram

4. 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

4.1 User registration

- In this module, we are going to register the user details and give the information which they ask.
- When we will register the sieving image and shuffling image will get download. After save the Image .
- when you try to login to your account you have to upload those sieving Image and Shuffling Image.

4.2 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.

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.

4.3. 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

4.4. 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.

5.SDS algorithm

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).

6. 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 java platform using eclips. 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). 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 = 2x = 28 = 256, x = 8
PtrLastVac = (n-1) = 50399

The process of retrieving the original image involves sieving the random shares and retrieving R/G/B(A-shuffle) and R/G/B(B-shuffle), thereafter from the individual shuffled shares the original RA, GA , BA and RB, GB , BB are generated. Using these the original image is then generated. The retrieved image is same as original and no loss of picture quality occurs.

7. Analysis and comparison

Image encryption may be classified as lossy / lossless image encryption. The conventional VCS schemes all generate a degraded image quality of the recovered image and hence some modifications to VCS often referred to as Variants to Visual Secret Sharing schemes have also been proposed. Hence a true comparison of our scheme would involve comparing it to the other proposed VCSs as also its variants. Most of the digital cameras today support 24 bit true color schemes and upwards, hence it is natural that most of the secret sharing schemes would need to support 24 bit color schemes. Many do not support 24 bit true color scheme. Our scheme along with Tsai et.al scheme supports 24 bit true color schemes. Another important factor is how the size of the share increases with increase in the number of shares and the number of colors. This is a very critical factor when considering the bandwidth constraint i.e. transmitting the shares on the net as also the storage size of each of these shares. In the extended Thien and Lin's scheme supporting true color, the size of each share increases three times. Similarly in Lukac and Plantonis (n,n) threshold scheme each share becomes 2n-1 times larger, thus with increase in number of shares i.e. n, the size of the share doubles for each new participant. In our scheme the size of the random share is not a function of the number of colors in the image or the number of shares. The size of the random share thus is always constant i.e. equal to the size of the secret image. Thus the proposed schemes perform better on the bandwidth and storage requirement parameters.

In our proposed technique both during encryption and decryption the computation cost is low since the majority of the operations use logical XOR, OR and AND operators. The scheme involves 3 steps, initial training, encoding and decoding. The initial training phase involves Principal Component Analysis (PCA) and Forward Neural Network (FFN). The initial training phase itself involves heavy computation cost though the encoding and the decoding phases in and our scheme are comparable.

In our proposed scheme there are no keys involved and hence there is no key management. All that is required is to transmit one of the random shares on a secret channel while transmitting the rest on an unsecure channel. In , the decoding step involves use of a weighted matrix B generated during the training phase and a seed 's' used in the encryption phase, thus handling of these two secret elements raises issues similar to key management in an encryption algorithm. In the quality of the recovered image is almost similar to the original secret image, however the fact remains that the recovered image is not same as the original secret image. In our scheme the recovered image is an exact replica of the original image as no data is lost during the sieving division and shuffling operations. The results were validated using Normalized Correlation (NC). NC is used to measure the correlation between the original secret image and the recovered images from the random shares.

$$NC = \sum_{i=1}^{w} \sum_{j=1}^{h} \frac{(Sij \oplus Rij)}{w \times h}$$

S represents the secret image and R the recovered image. w, h represents the width/height of the photographs and ⊕ represents the exclusive OR operator. We repeated the test over multiple images, the NC for all the recovered images

was 1.000. The generated random shares are highly secure as the spatial correlation between the pixels is eliminated by employing the randomization function thrice for each pixel value per share. A comparison of our scheme with similar other schemes is listed in Table 2.

Table 2. Comparison of techniques

Features	Proposed Scheme	Tsai,Chen et.al.	Lukac, and Plataniotis	Chang and Yu'sscheme
Noise Correlation	Always 1.000	Always< 1.000	1	Always< 1.000
Image delivery	NO	YES	NO	YES
Transparency				
Additional Data	NO	YES	NO	YES
Structure		AX,BX		S-E table(local)
Key Management	NO	YES	NO S,BX have to be kept secret	NO
Pixel Expansion	No expansion	1:9 expansion		
(256 color, (n, n)			1:2(n-1)	0.221527778
scheme)				

8. Related work

A. Image Encryption

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 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 in 2008 following up on the work of , 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 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. Image Splitting

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 imag moving to greyscale image and finally employing it to color images. Though with each subsequent research paper the quality of the recovered image improved, however, but for 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. 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.

Naor and Shamir 1995	**1**	**4**	**Binary**	**Random**
Wu and Chang 2005	2	4	Binary	Random
Chin-Chen et. al 2005	1	4	Binary	Meaningful
Tzung-Her Chen et al 2008	n(n>=2)	4	Binary,gray,color	Random
F. Liu et al 2008	1	1	Binary	Random
Du-Shiau Tsai et al 2009	1	9	Random	meaningful

9. 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

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

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

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

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

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

A. Shamir (1979), How to share a secret, Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.

M. Naor and A. Shamir (1995), Visual cryptography, in Proc. EUROCRYPT' 94, Berlin, Germany, vol. 950, pp. 1–12, *Springer-Verlag*, LNCS.

Arpad Incze (2010), Pixel sieve method for secret sharing & visual cryptography RoEduNet IEEE International Conference Proceeding Sibiu 24-26 , ISSN 2068-1038, p. 89-96.

H.-C. Wu, C.-C. Chang (2005), Sharing Visual Multi-Secrets Using Circle Shares, *Comput. Stand. Interfaces* 134 (28) ,pp. 123–135.

Chin-Chen Chang (2005), Jun-Chou Chuang, Pei-Yu Lin , Sharing A Secret Two-Tone Image In Two Gray-Level Images, Proceedings of the 11th *International Conference on Parallel and Distributed Systems (ICPADS'05*

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

F. Liu1, C.K. Wu X.J. Lin (2008), Colour Visual Cryptography Schemes, *IET Information Security*, vol. 2, No. 4, pp 151-165.

Du-Shiau Tsai , Gwoboa Horng , Tzung-Her Chen , Yao-Te Huang (2009) , A Novel Secret Image Sharing Scheme For True-Color Images With Size Constraint, Information Sciences 179 3247–3254 *Elsevier*

R. Lukac, K.N. Plataniotis (2005), Bit-level based secret sharing for image encryption, *The Journal of Pattern Recognition Society*.

C.C. Chang, T.-X. Yu (2002), , Sharing a secret gray image in multiple images, in: Proceedings of First International Symposium on Cyber Worlds,pp. 230–240.