ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Keyless Approach to Image Encryption Using SDS Algorithm

Noonela Yerni Raju
M.Tech Student
Department of CSE,
Chaitanya Engineering College,
Madhurawada,Visakhapatnam,
AP, India.

Satish Kumar Yanamadala, M.Tech
Assistant Professor
Department of CSE,
Chaitanya Engineering College,
Madhurawada,Visakhapatnam,
AP, India.

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.

Keywords- ***Visual Cryptography, Sieving, Shuffling, Random shares.***

I.INTRODUCTION

The advent of internet introduced to its users a whole 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. 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.

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" [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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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 [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.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 [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. 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 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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

have to be secure and computationally inexpensive. Table 1 gives a comparison of six such techniques.

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

C. 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.

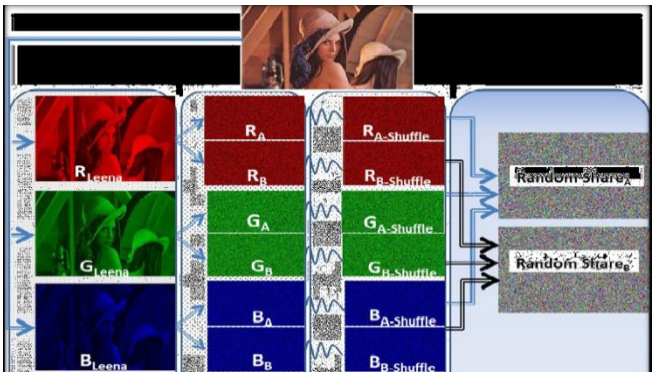

Figure 1. Steps involved in generating two Random Shares

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 involve 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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. The scheme implemented using the SDS (Sieve, Division, and Shuffle) algorithm involves the following three steps:

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.

Figure 2. R/G/B representation for individual pixels

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.

$$R \quad (R_A, R_B, R_C, \text{----------}, R_Z)$$
$$G \quad (G_A, G_B, G_C, \text{----------}, G_Z)$$
$$B \quad (B_A, B_B, B_C, \text{----------}, B_Z)$$

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 (Refer Figure 4).

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Figure 3. Representation of the Sieving operation

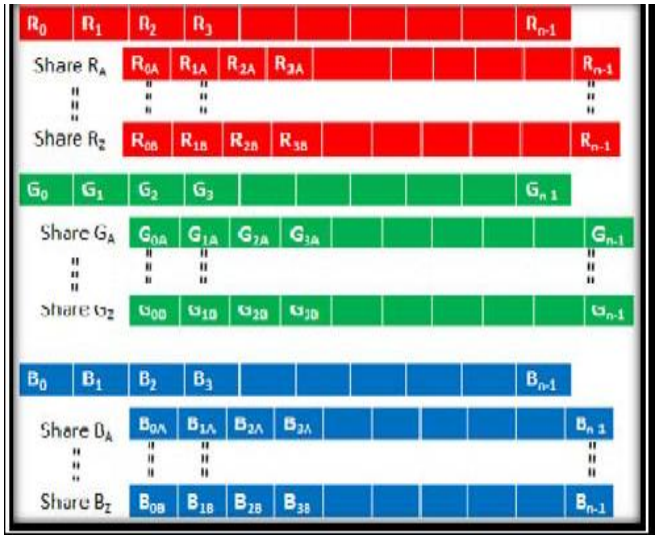

Figure 4. Representation of the Division operation

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

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

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

- - - -

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

   $Aggr\_Sum_i = \_ R_{ki}$

   }
   R_{zi} =(max_val + Ri – ($Aggr\_Sum_i$ % max_val)) % max_val
3. Shuffle
   Repeat for $R_{A\text{-}Z}$, $G_{A\text{-}Z}$ and $B_{A\text{-}Z}$ (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 (RSA ,RS B ---------- RSk).

III. 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). The various parameters as defined in the generic algorithm above thus take the following values.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

$n = (300 * 168) = 50400$ (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-shuffle) and R/G/B(B-shuffle), thereafter from the individual shuffled shares the original RA, GA , BA and RB, G B , BB are generated. Using this original image is then generated. The retrieved image is same as original and no loss of picture quality occurs.

V. 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. [7],[9],[10] do not support 24 bit true color scheme. Our scheme along with Tsai et.al scheme[13] 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 [16] scheme supporting true color, the size of each share increases three times. Similarly in Lukac and Plantonis [14] (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 [13] 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 [13] 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 [13], 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 [13] 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.

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

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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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

	SCHEMES			
FEATURES	Proposed Scheme	Tsai, Chen et.al. [13]	Lukac, and Plataniotis [14]	Chang and Yu's scheme [15]
Noise Correlation	Always 1.000	Always< 1.000	1.000	Always< 1.000
Image delivery Transparency	No	Yes	No	Yes
Additional Data Structure	No	Yes AX, BX	No	Yes S-E table (Local)
Key Management	No	Yes S, BX have to be kept secret	No	No
Pixel Expansion (256 color, (n, n) scheme)	No expansion	1 : 9 expansion	$1:2^{n(1}$	1 : 529

V CONCLUSIONS

In this paper a new enhanced visual cryptographic scheme is presented, 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]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.

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

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

[10]Chin-Chen Chang, 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), 2005.

[11]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.

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

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

[14]R. Lukac, K.N. Plataniotis "Bit-level based secret sharing for image encryption", The Journal of Pattern Recognition Society, 2005.

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

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