Keyless Approach to Image Encryption

Kaustubh Chaudhari[1] Pankaj Pallewar[2] Rohit Jaisinghani[3] Saurabh Shelke[4] Prof. Shivprasad Patil[5]

[5]Professor

[1,2,3,4,5]Department of Information Technology

[1,2,3,4,5]NBNSSOE, Pune, India

Abstract— Confidentiality and secrecy of images can be achieved using two approaches, one is encrypting of image and maintaining key for decryption and retrieval of original image. Another approach is encryption of image using Sieving, Division, Shuffle (SDS) algorithm. In this paper we propose encryption method for image without use or preparation of key and with the use of SDS algorithm. This implementation mainly consists of sieving, division and shuffling of image and creates shared having minimum computation and maximum security for image encryption and decryption process.

Key words: Sieving, Division, Shuffling, Encryption, Decryption, Cryptography, Random shares

I. INTRODUCTION

Now a day's large amount of data is shared or exchanged over internet. Therefore it is necessary to protect the data to maintain its confidentiality and secrecy so that any unauthorized party cannot access and manipulate the data. Data can be anything like text, video, image, etc. When it comes to protection of data then vibrant research area of cryptography can be used.

Cryptography can be defined as a process of generation of such security scenario which helps in preventing intruders as well as provides confidentiality to data. Cryptography mainly consists of two processes one is encryption and other one is decryption. There are some traditional algorithms are present which are already implemented for image encryption like Ron Rivest, Adi Shamir and Leonard Adleman (RSA), Data Encryption Standard (DES), Advanced Encryption Standard (AES), etc. In these traditional algorithms image is first encrypted and key is generated with specific length and necessary for decryption of image. Here security of key is an overhead. Hence we are proposing SDS algorithm which does not generate key, helps in reduces security overheads as well as provides more confidentiality.

A. Image Encryption:

Traditional image encryption involves use of algorithm and secret key. Some of them use "Vector quantization" [1], "Digital signature" [2], "Chaos theory" [3], etc. which has limitations like key generation and key management resulting into high computation and weak security.

B. Image Splitting:

This approach involves division of image at pixel level into multiple shares. Because of multiple shares information of image cannot be obtained from individual share but qualified set of these shares will help in regenerating the original image. Adi Shamir [6] in 1979 introduced the technique of dividing image into two shares. In 1995, Naor and Shamir [7] used this as base and proposed concept of "Visual Cryptography" which involves secret sharing of image by dividing it into multiple shares.

II. RELATED WORK

Image Encryption: In last few decades, lots of schemes are proposed for image encryption with the help of key. In 1992, Manniccam and Bourbakis [3] proposed an image encryption and compression method using SCAN language which was based on chaos theory and applicable only to grey scale images. In 2000, Chen and Hawang [4] proposed use of Vector Quantization (VQ) which involves decomposition of image into vectors and their sequential encoding. In 2008, Xin and Chen [1] proposed two stage image encryption methods. Stage one involves fusion of original and secret image. Stage 2 involves encryption of fused image with the help of Henon chaotic system.

A. Image Splitting:

This phenomenon is referred as "Visual Cryptography Schemes" (VCS) which involves division of image into multiple shares such that these shares individually reveals no information about original image and when stacked regenerates original image. In 1995, Naor and Shamir [7] proposed method with one pixel expansion resulting into random four shares for binary image. In 2005, Wu and Chang [9] proposed method with two pixel expansion resulting into four random shares for binary image. In 2005, Chin-Chen.et al [10] proposed a method with one pixel expansion resulting into four meaningful shares for binary image. In 2008, Tzung-Her Chen et al [11] proposed a method with "n(n>=2)" pixel expansion resulting into four random shares for binary, grey and color image. In 2008, F.Liu at al [12] proposed a method with one pixel expansion resulting into one random share for color image. In 2009, Du-Shiau Tsai [13] proposed a method with one pixel expansion resulting into nine meaningful shares for color image.

III. PROPOSED TECHNIQUE

Our proposed technique is implemented with the help of SDS algorithm which do not use any kind of secret key for image encryption. Our proposed technology consists of three stages. In first stage, secret image is split into three primary colors that are red, green and blue, this process is called sieving. In second stage, these three images are divided into random shares, this process is called division. In third stage, divides shares are shuffled randomly each within itself. And these shares are combined to generate the desired random shares.

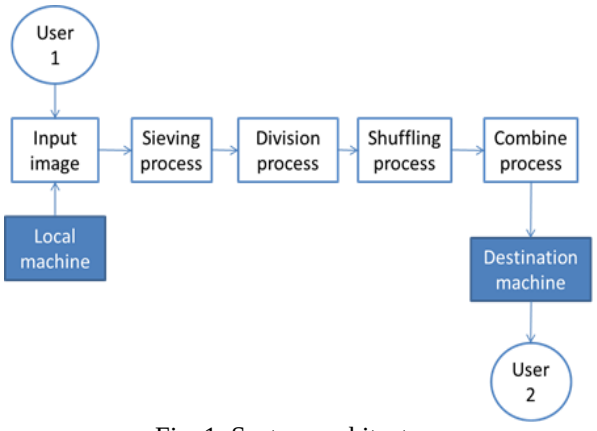

Fig. 1: System architecture

For our proposed methodology we have use the system architecture which is shown in figure 1.This involves sieving, division, shuffling and combine operations by providing interface between sender and receiver. In figure 1 user 1 is sender and user 2 is receiver. As shown in figure, secret image is encrypted at sender end and decrypted at receiver end.

Since our proposed technique 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. 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 is a series of bits composed of values representing the RGB values. 8 bit (2 Bits each), 16 bits (4 bits each), 24 bits (8bits each), 48 bits (16 bits each) etc. are some of the commonly used RGB components. Figure 2 represents the RGB values for an individual pixel. If x is the number of bits used for representing any color, then total of 2^{3x} colors can be represented by mixing three primaries that is RGB colors. Value of each primary color will vary from 0 to (2^x-1).

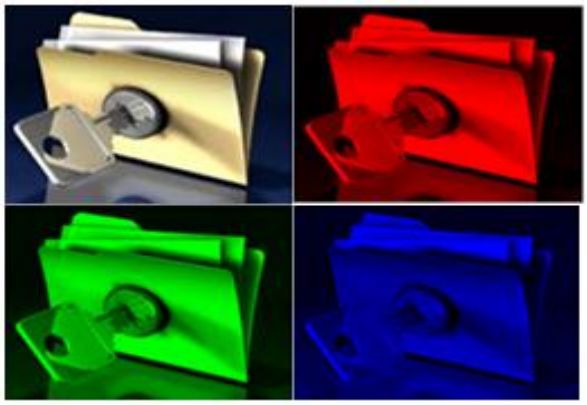

Fig. 2: Sieving

In above figure, first is the original secret image. Sieving process involves filtering of combined RGB components into individual R, G, and B components. To make sieving process computationally inexpensive, we have used XOR operator for sieving operation.

After performing sieving operation, images obtained after sieving into individual R, G, and B components are further divided into 'z' parts each.

- $RC = (RC_a, RC_b, \ldots\ldots\ldots\ldots, RC_z)$
- $GC = (GC_a, GC_b, \ldots\ldots\ldots\ldots, GC_z)$
- $BC = (BC_a, BC_b, \ldots\ldots\ldots\ldots, BC_z)$

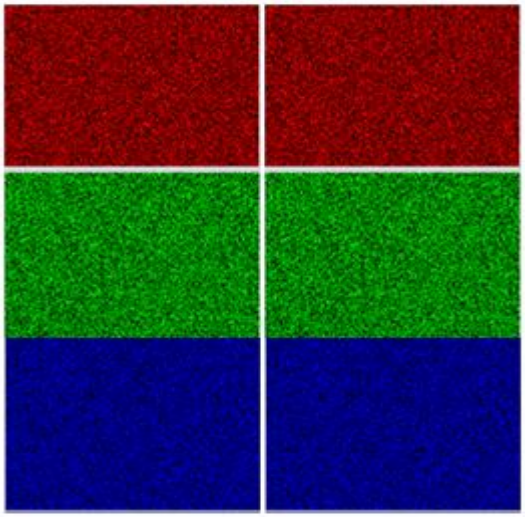

Fig. 3: Division and Shuffling

As shown in above figure, after performing division and shuffling operation, two shares are generated of each primary color.

At the time of division, it is ensured that in R_{a-z}, G_{a-z} and B_{a-z} is assigned values randomly, so that entire domain is available for randomized selection.

After performing division operation, shuffling is done which involves shuffling the elements in individual shares. Sequencing of the elements within the shares is depends on the value of one of the other shares generated from the same primary color. In other words R_b decides how R is shuffled, R_c decides how R_b is shuffled, R decides R_{z-1} is shuffled and R decides how R_z is shuffled. This uses the comparison operator on the LSB of the determining element to decide the shuffle sequence.

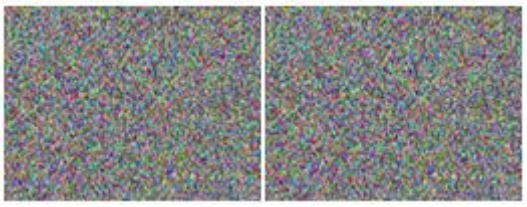

Fig 4: Combine

After performing division and shuffling, shares generated for each primary color are combined resulting into only two shares. As shown in figure 4 two shares were generated after performing combine operation.

IV. ALGORITHM

1) Sieving
   Input - secret image
   Output - R,G,B components
2) Division
   n = total number of pixels (0 to n-1)
   $R_i/G_i/B_i$= individual values of the i^{th}pixel in R,G,B components
   z = total number of random shares
   x = number of bits representing each primary color
   $max\_val = 2^x$
   Repeat II for R,G,B components.
   For i = 0 to (n-2)
   { For share k = a to z-1
      R_{ki}= Random (0, max_val)
      $Aggr\_Sum_{i} = \sum R_{ki}$

}

R_{zi}= (max_val + R_i -(Aggr_Sum_i % max_val)) % max_val

3) Shuffle

Repeat for R_{a-z}, G_{a-z}, B_{a-z}

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++, PtrLastvac--

}

}

}

4) Combine

For k = a to z

RS_k = ($R_{k\text{-}shuffle}$ XOR $G_{k\text{-}shuffle}$ XOR $B_{k\text{-}shuffle}$)

After finishing the above process we get random shares (RS_a,RS_b,RS_c,.....,RS_z)

V. Experimental results and Analysis

To validate our algorithm we implemented a modified threshold VCS to validate the results as this could have its real world application to authenticate a user. A photograph of a user can be clicked and divided into two shares. One of the shares will be held by the authenticating party and the other will be held by the user who is being authenticated.

We have implemented the scheme on java platform using swing. The scheme was run over a wide range of photographs including bright/dull, colored/black and white etc. A jpg image titled encrypt.jpg is used to demonstrate the results. It is a 300 X 168 pixel image with an image depth of 24 bits, 8 bits for each 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 this original image is then generated. The retrieved image is same as original and no loss of picture quality occurs.

In our proposed methodology, during encryption as well as decryption computation cost is low as we have used XOR, OR and AND operator in most of the operations.

There are no keys involved hence there is no key management. Transmission of random shares on secret channel is required. The quality of recovered image is almost similar to the original secret image. 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 there covered images from the random shares.

$$NC = \sum^{w}_{i=1}\sum^{h}_{j=1}(Sij \overline{XOR} Rij) / w \text{ X } h$$

VI. Conclusion

In this paper a new cryptography method is introduced which provides maximum confidentiality and secrecy to image with less security overheads. It completely avoids key management scheme.

1) The original secret image can be retrieved completely.
2) There is no pixel expansion therefore space occupied by share is same as original secret image.
3) Key management is not a problem as use of key is not involved.
4) Scheme is robust to withstand brute force attack.

References

[1] 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.

[2] Aloka Sinha and Kehar Singh, "A technique for image encryption usingdigital 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] Xin Zhang and Weibin Chen, "A new chaotic algorithm for imageencryption", International Conference on Audio, Language and Image Processing, 2008. (ICALIP 2008), pp 889-892.

[5] S.Behnia, A.Akhshani, S.Ahadpour, H.Mahodi,A. Akha-van, A fastchaotic 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.

