e-ISSN: 2349-9745
p-ISSN: 2393-8161
Scientific Journal Impact Factor (SJIF): 1.711
International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Retrieving Of Color Images Using SDS Technique

Vishal Arunrao Damedhar[1], Prof. V.S. Nandedkar[2]

[1]*Department of Computer, PVPIT Bavdhan, Pune*
[2]*Department of Computer, PVPIT Bavdhan Pune*

Abstract – How data can be shared from one part of the world to the other in near real time came with the arrival of internet. Along with this they have introduced new challenges like maintaining the confidentiality of transmitting the data. This gave a boost to the research area related to cryptography. Firstly, Encryption of images with the accepted encryption algorithms had significant downside as key management was complicated and limited. Secondly, introduction to new area for encrypting images was splitting the image at its pixel level in to multiple shares. But the major drawback of this approach was that the recovered image had a poor quality. To overcome these mentioned drawbacks we have proposed a new approach which does not attempt to use any type of keys for encryption.

Index Terms – Combining, Division, Image Encryption, Image Decryption, Random shares, Sieving, Shuffling.

I. INTRODUCTION

Maintaining the secrecy and confidentiality of an image is a listless area of study. Two different methods are being followed. Firstly, encrypting the images by using any encryption algorithm with the help of keys and secondly, dividing the image into possible random shares in order to maintain the image secrecy. Further the nature of the recovered image can be classified as lossy or lossless image encryption. Thus this gave rise to two different approaches for maintaining the secrecy of an image.

A. Encryption of image with the use of keys:

The conventional method and this method use an algorithm and a key for encrypting images. Some of the techniques which are being used are Digital Signatures Chaos Theory etc. There are some innate disadvantages with the said techniques; the key management is limited as they rivet the use of secret key and the computation cost is also high. Conversely the greatest advantage is that in most of the designs the original image is recovered entirely.

B. Image Splitting

This approach in primitive form includes splitting an image in to multiple shares may be two or more at its pixel level. The shares of the split images express no information about the original image, but eligible set of shares when combined will produce the original image.
The main disadvantage of this approach was that the image recovered was very poor in quality. To trounce the limitations of these approaches we put forward a new scheme, in which the quality of the recovered image is same as it that of the original image. Many research papers have been published using this approach, starting from a binary image [9] moving to grey scale image and finally employing it to color images. Also in our proposed scheme we do not use any kind of key for encryption which eventually reduces the bandwidth requirement and computational cost.

C. Mixed Approach

Splitting of an image into random shares with the help of using some kind of encryption key comes under his approach. Incze et al. suggested the concept of sieves for the purpose of encrypting images.

In general sieve is a type of binary key. In order to form the shares the original image is placed over the sieve, pixels from the original image goes through and form one share and the pixels that do not cross will form the other share. From the study of cryptographic approaches which involves low computation cost and keyless management guided us to take fresh approach.

D. Visual Cryptography

It is a technique in which encrypts visual information like picture, text in such a way that decryption can be done by human visual systems without the support of computers. Simple algorithms are used; there is no need of cryptography data or complex computations. When concerning security issues it makes certain that hackers do not obtain any clues about the secret image from original image. Visual information like pictures and text which are secret are taken as image and a simple algorithm is used to encrypt to produce n copies of shares. The simplest method is creating a two by two structure scheme in which the secret image is divided in to two shares. Both the shares are required for decryption. The generated shares are dots in random which do not reveal any information about the secret image.

Visual Cryptography is a way of sharing secret images together with a group of members, where definite group combine to get back the original image. The decryption process is fast and easy as the shares are put on transparencies to get back the shared image. The computation cost is also very low

E. Scope and Objectives

The foremost objective of this approach is to encrypt an image without using any type of key. In this scheme the secret image is split into multiple random images and then combined back to form the original image. This results in low computation cost. Here the Sieving, division and shuffling process is used to generate random shares.

II. PROPOSED TECHNIQUE

Our proposed techniques implicate dividing an image into one or more shares. The shares so produced expose no information about the original secret image and to get back the original secret image all the created shares are needed. This technique is executed with the help of sds algorithm which contains three steps.

1. The first step is the sieving process in which the primary colors of the secret images are split into Red, Green and Blue.
2. The second step is the Division process in which the split images of the secret images are randomly divided.
3. The third step is the shuffling process in which the shares of the divided secret image are shuffled among themselves.

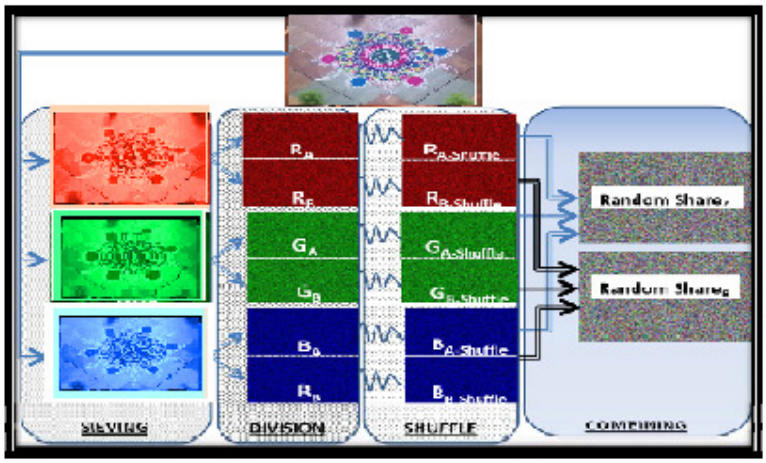

Fig.1.1 Steps for generating random shares

When we represent colors in their additive and subtractive form they are the most chosen models. Red, Green and Blue which are the three primary colors are mixed to get the desired colors. The example of additive models is when colors are shown on computer monitor. Likewise the subtractive model when using Cyan, Magenta and yellow the degree of light is reflected by the colored matter. The desired ranges of colors are produced by the Cyan, Magenta and Yellow pigments. This model is used in printers. The additive color model is used because of computation during encryption and decryption in our proposed system. It is worth mentioning that in the techniques based on [6], [7] since the shares were printed on transparencies, hence subtractive model was the natural choice for such applications the constitutions of colors are described by the additive and the subtractive models.

III. DESIGN AND IMPLEMENTATION

This system consists of two types of user module one is the admin module and the other is the member user module. Encryption of image is done by Sieving, Division and Shuffling process. The secret image is divided in to random shares and later on combined back to get back the original image. Decryption of image is just the reverse process of Image encryption.

A. Admin Session and Member user Session

The Admin session include the Login, Profile, Member user creation and the member user details whereas the Member user session comprises of Login, Image Encryption, email module, Image decryption and changing of password.

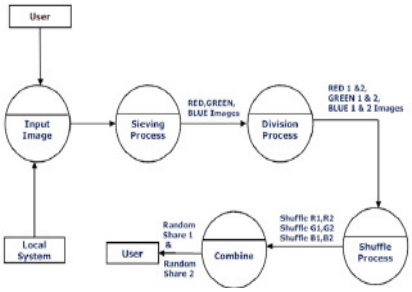

Fig.2.1 Image encryption – DFD

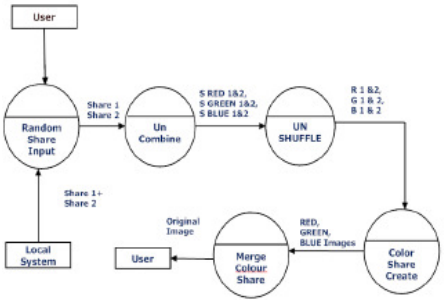

Fig.3.1 Image Decryption – DFD

IV. MODULES DESCRIPTION

A. Registration of user

This module consists of registering the user details and provides the information which they want. Once the user is registered a sieving and shuffling image is created. These images can be downloaded and saved. When the user tries to login to his account he has to upload both the sieving and shuffling image.

B. Encryption of Image

Filtering the combined Red, Green and Blue components into its individual Red, Green and Blue components is the sieving process. The levels of the sieve actually depend upon values taken by the Red, Green and Blue components independently. The XOR operator used reduces the computation cost. After filtering the Red, Green and Blue components it is divided in to z parts per share.

$R\_ (R_A, R_B, R_C, R_D.....R_Z)$
$G\_ (G_A, G_B, G_C, G_D.....G_Z)$
$B\_ (B_A, B_B, B_C, B_D.....Bc)$

On dividing it is made certain that each element in R_A to R_Z, G_A to G_Z and B_A to B_Z are assigned random values in such a way that the values are available for random selection. If he case is that when the value of x=8 the values from range 0-255 are randomly assigned. The generated shares should be in such a ways that it should generate Red, Green and Blue. Results have shown that by division the random shares have no similarity with the original image. To randomize the shuffling operation is performed which involves shuffling of elements individually. The value of one share depends on the shuffling of the elements with the individual shares. Combining the generated shares yields the original image.

C. Sending email

In this process we attach any one of the share which is to be sent to the authorized user containing some message. Out of the two shares generated one share is sent as an attachment to the authorized user and the other share is kept with the unit.

D. Decryption of Image

To get back the original image all the generated shared are required. The reverse process of encryption is followed to retrieve the image. The two encrypted shares are uncombined and the uncombined shares are un-shuffled among it to restore the original image.

E. Sequence Diagram

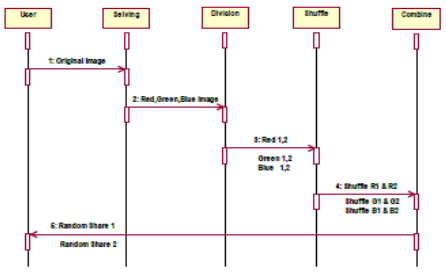

Fig. 4.1 Sequence Diagram

V. PROPOSED SDS TECHNIQUE

Input (Secret Image)
Sieve (Secret Image)
Output (R, G, B components)
n = total number of pixels (0 to n-1)
R_i / G_i / B_i are unit values z are random shares x are no. of bits representing each primary color max value is 2x
Repeat 2 for Red, Green, Blue component
for i = 0 to (n-2)
{ for share k = A to (Z-1)
R_{ki} = Random (0, maximum _value)
aggregate _ Sum $_i$ = _ R_{ki} } Rzi=(max_val + Ri – (Aggregate_Sum$_i$ % max_val)) % max_val
R_A to R_Z, G_A to G_Z and B_A to B_Z (generated shares) for k = A to Z
{ Rk-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-shuffle) $PtrFirst_{Vac}$ = R_{Ki}
$PtrFirst_{Vac}$ ++, i++ }
Else
{ R(A-shuffle) $PtrFirst_{Vac}$ = R_{Ai}
i++, $PtrLast_{Vac}$ --
} } }
Combine
For k = A to Z
R_{SK}= (R_K-shuffle XOR G_k-shuffle XOR B_K-shuffle)
Thus we have Random shares (R_{SA}, R_{SB}---------- R_{SK}).

VI. ANALYSIS

Image encryption can be categorized as lossy / lossless image encryption. Visual Cryptography System schemes all produce a tainted image quality of the recovered image. Modifications to VCS frequently submitted to as Variants. We compare this scheme with other VCS. Digital cameras support 24 bit true color schemes therefore most of the secret sharing schemes should support 24 bit color schemes.. Our scheme along with Also as the size of the share increases with number of shares and colors. When considering the bandwidth factor the size of the share should be small so that they can be transmitted with ease. If the size is apparently large it is very costly. The random share size is not a function of the color images or the shares; in our system the size is constant thus providing better bandwidth and storage methods. In this system the computational cost is reduced as logical XOR, OR operators are used.

In our system there is no key management as there are no keys used. The only thing that is required is to send one share through secured channel and the other through unsecured channel. In other schemes the recovered original image is not the same as the original image but in our system the quality of the recovered image is as same as the original image since there is no data loss during the sieving division and shuffling method.

The results can be confirmed using Normalized Correlation. For measuring the NC, the given formula is used.

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

Where S is the secret image and R is the recovered image, w and h represent width and height of the image.

Feature	Proposed	Chang Scheme
Image Delivery	1	Less than 1
Transparency	No	Yes
Key Management	No	Yes
Pixel expansion	No	Yes
Noise correlation	1	Less than 1

Table 6.1 Comparison of techniques

VII. RESULTS

To authenticate the algorithm, a photograph of a user was divided in to two shares. Two shares which have been generated; one will be kept with the authenticating group and other will be kept by the user who is to be authenticated. The implementation is being carried out in .Net platform using C#. The scheme will be tested with all categories of images. The process of getting back the original image without the loss of any quality involves sieving of random shares and retrieving the shuffled shares. The retrieved image has no loss of quality. A jpg image named leena.jpg will be been used to demonstrate the final results. We consider a 300 x 192 pixel image which has an image depth of 24 bits. The parameters in the algorithm take the following values.

n= (300*192) = 57600 (n varies from 0 to 57599)
z=total random shares = 2 (Share A, B)
max_val = 2x = 28 = 256, x=8
$PtrLast_{Vac}$ = (n-1) = 57599

VIII. CONCLUSION

In this paper a new encryption scheme has been brought up using VCS which is a mixed version of image encryption schemes and traditional VCS. An image is split in to random images and the combination of them retrieves the original image with low computation cost. The advantages of his scheme are that the original and the retrieved images are the same. There is no pixel expansion and thus the requirement for storage is same as that of the original image. No secret keys are involved hence there is no key management. This scheme is vigorous to any attacks. This scheme is suitable for authentication based application or where trust cannot be responded 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 into commence of a nuclear strike, the said code could be converted into and image and split into random shares. To retrieve the secret code all participants must provide the random shares.

REFERENCES

[1] Thomas Verbraken, Wouter Verbeke, and Bart Baesens developes ,"A Novel Profit Maximizing Metric for Measuring Classification Performance of Customer Churn Prediction Models" IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 25, NO. 5, MAY 2013

[2] Qingbo Li, Wei Wang,Xiaofeng Ling, and Jin Guang Wu , "Detection of Gastric Cancer with Fourier Transform Infrared Spectroscopy and Support Vector Machine Classification" , BioMed research international, 2013 - hindawi.com

[3] Zhen-Yu Chen, Zhi-Ping Fan, "A Hierarchical Multiple Kernel Support Vector Machine for Customer Churn Prediction Using Longitudinal Behavioural Data" European Journal of Operational Research, 2012 – Elsevier

[4] Anshuman Sharma explains," Handwritten digit Recognition using Support Vector Machine", arXiv preprint arXiv: 1203.3847, 2012 - arxiv.org

[5] Dragan Matic´, Filip Kulic´, Manuel Pineda-Sanchez , Ilija Kamenko ,"Support vector machine classifier for diagnosis in electrical machines: Application to broken bar" Expert Systems with Applications 39 (2012) 8681–8689.

[6] Ashis Pradhan "SUPPORT VECTOR MACHINE-A Survey", (ISSN 2250-2459, Volume 2, Issue 8, August 2012)

[7] Hsu, Chih-Wei, Chih-Chung Chang, and Chih-Jen Lin. "A practical guide to support vector classification ", http://www. csie. ntu. edu. tw/~ jlin/papers/guide/guide. pdf (2009).

[8] Theodore B. Trafalis, Huseyin Ince , "SUPPORT VECTOR MACHINE FOR REGRESSION AND APPLICATIONS TO FINANCIAL FORECASTING" IJCNN '00 Proceedings of the IEEE-INNS-ENNS International Joint Conference on Neural Networks (IJCNN'00)-Volume 6.

[9] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT' 94, Berlin, Germany, 1995, vol. 50, pp. 1–12, Springer-Verlag, LNCS.

[10] Kyung-Shik Shin, Taik Soo Lee, Hyun-jung KimAn "application of support vector machines in bankruptcy prediction model" Expert Systems with Applications 28.1 (2005): 127-135.

[11] Huang, Zan, et al. "Credit rating analysis with support vector machines and neural networks: a market comparative study." *Decision support systems* 37.4 (2004): 543-558.

