ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

# Protection Of User's Data Using Image Encryption Domain: Image Encryption <ASP.NET>

Balamurugan.S[1], S.Sureshkumar[2]

Assistant Professor, Computer Science and Engineering, V K S College of Engineering and Technology, Karur[1]

Final Year ME, Computer Science and Engineering, V K S College of Engineering and Technology, Karur[2]

**Abstract:** In recent area of research maintain the secrecy and confidentiality of images is a vital role, with two different approaches being followed, the first approach is being encrypt the images through encryption algorithms (RSA or DES) using keys, the second approach involves dividing the image into random shares to maintain the secret of image. Unfortunately intense computation cost and key management limit the service 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 narrative approach without the use of encryption keys. The new proposal employs Sieving, Division and Shuffling (SDS) to generate the random shares and also overcome the above two approach with minimal computation and the unique secret image can be recovered from the random shares with high quality.

**Keywords:** Image encryption, Image decryption, SDS, Random shares.

## I. INTRODUCTION

Encryption is a process of converting messages, information or data from readable format to unreadable format. Encrypted data must be decrypted, before it can be read by the user that is recipient. The origin of the word encryption 'crypt' comes from the Greek word crypto's meaning hidden. In its earliest form, people have been challenge to cover certain information that they wanted to keep to their own possession by substituting parts of the information with symbols, numbers and pictures, in chronology the history of Cryptography throughout the centuries. For this types of different reason humans are interested in protecting their messages. The Assyrians were interested in protecting their trade secret of manufacturing of the pottery. The Chinese were interested in protecting their trade secret of manufacturing silk.

Cryptanalysis is the art of breaking cryptosystems. Cryptology is the study of both cryptography and cryptanalysis. Cryptosystems can be divided into two categories: symmetric and asymmetric. First method Symmetric crypto systems use the same key (the secret key) to encrypt and decrypt a message, and the second method asymmetric cryptosystems use one key (the public key) to encrypt a message and a different key (the private key) to decrypt it by some algorithms.

Encryption has been used by people in all situations such as in corporate, military and personal information. Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot be read this, but that authorized persons can read it. In this method, the message or information (referred to as plaintext and image) is encrypted using an encryption algorithm, turn it into unreadable format i.e. cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the cipher text using a decryption algorithm that usually requires a key which adversaries do not have access to.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

There are two basic types of encryption schemes: Symmetric-key and public-key encryption. In these symmetric-key schemes, both the encryption and decryption keys are the same. Therefore communicating parties must be agree on a secret key before they wish to communicate. In public key schemes, the encryption key is published for anyone to use and encrypt messages.

Other approach adopted for maintaining confidentiality of images is image splitting involves splitting an image at the pixel level into multiple shares ( may be two or more), such that individually the shares communicate no information about the secret image, but a qualified set of these shares will help regenerate the original image (at least partially). It is also referred as Visual Cryptography Schemes (VCS) involves splitting a secret image into n random shares such that these shares are individually reveal no information about the original or secret image (but for its size) but a qualified subset of the random shares(as specified by the sender) 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.

## II. PROBLEM STATEMENT

Problem of heavy computation cost and key management limit of the existence approach and the poor quality of the recovered image from the random shares limit the applications, without the use of encryption keys. In addition, involving use of keys for encryption has low storage and bandwidth requirements, meanwhile also keeping the computation cost during encryption / decryption.

For secure communication, the hiding of data into encrypted image by keyless approach technique is employed in the proposed system. Use data hiding technique one can send the information to the accurate user without noticing to third person. Data can be hidden using different cover Medias like video, audio or images, text. Here the image is taken has a cover media. As Internet based communication of images increased day by day, encryption of images has become an important way to protect images especially on the Internet time is useful to us. In proposed system data hide into the encrypted image and then at receiver side receives both original image and data without the use of encryption keys. Cryptography is an image encryption technique used to hide the secure information in images. It allows the encryption of secret image into *n* number of shares and distributed into *n* number of participants.

The approach employs (SDS algorithm) Sieving, Division and Shuffling to generate random shares for color images which will take the R, G, B values separately and distributed into n number of participants with minimal computation, the original secret image can be recovered from the random shares without any loss of image quality.

## III. PROJECT SCOPE

Maintaining the secrecy and confidentiality of images is a vibrant area of research. Divide the image into random shares to maintain the images secrecy. The random shares so generated individually convey no information about the secret of that image, however to recover the imaginative image all the random shares would be required. It is implemented with the SDS algorithm.

Representation of colors, additive and the subtractive color models are the most preferred models. In the RGB or the additive model, there are three primary colors (i.e.) Red, Green, Blue are mixed to generate the desired colors. The colors as visible on the monitor are an example of the additive model. Likewise when using the CMY or the subtractive model, the colors are represented by the degree of the light. Cyan (C), (M), and Yellow (Y) pigments are used to produce the preferred range of colors and extensively used in printers. Since the shares were printed on transparencies, hence subtractive model is using this technique improving the image encryption.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

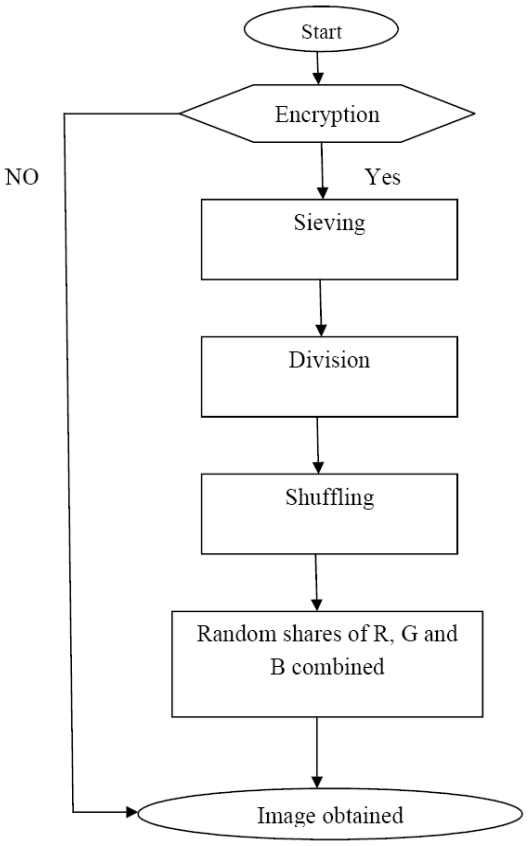
Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

## IV. APPROACH

The proposed technique can be implementing using SDS algorithm and involves three steps. In step one (Sieving) the secret image with data is split into primary colors. In step two (Division) these split images are randomly divided. In step three (Shuffling) divided shares are then shuffled each within itself. Final step is combining these shuffled shares to generate the desired random shares.

4.1 ALGORITHM FLOWCHART




## V. MODULES

- 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, and Sieving.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

5.1 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

5.1.1 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.

5.1.2 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)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

- 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.

5.1.3 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

5.1.4 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.

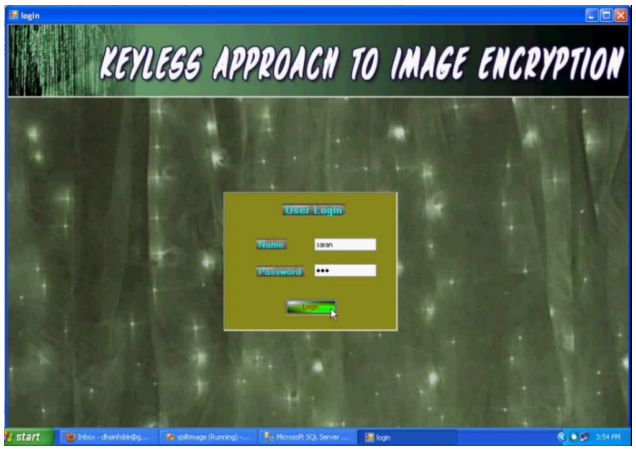
- Uncombined: Get the two encrypted shares
- Unshuffle: these uncombined shares are then unshuffled each within itself to get original image.
- Color Share Creation: the unshuffled image is split into primary colors.
- Merge: To merge the primary colors, we will get the original secret image without any loss of pixels.

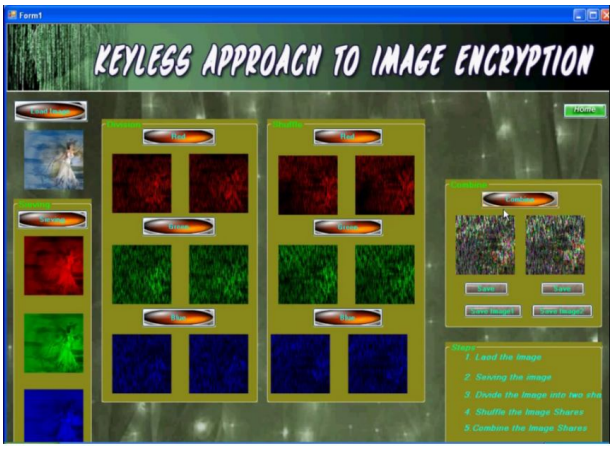
## VI. EXPERIMENTAL RESULTS

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).

6.1 SCREEN SHOTS



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

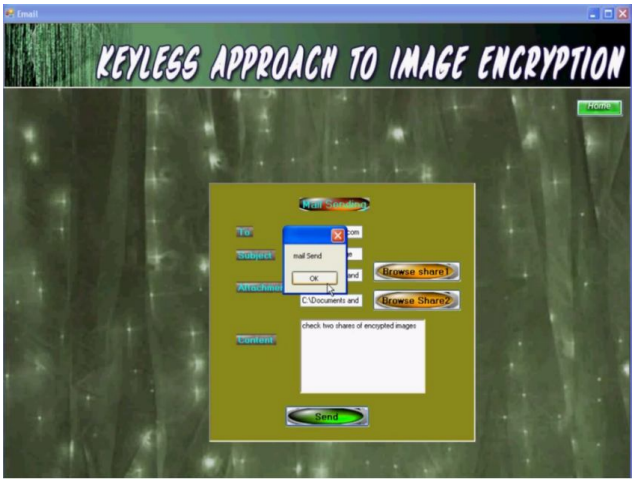
International Journal of Innovative Research in Computer and Communication Engineering

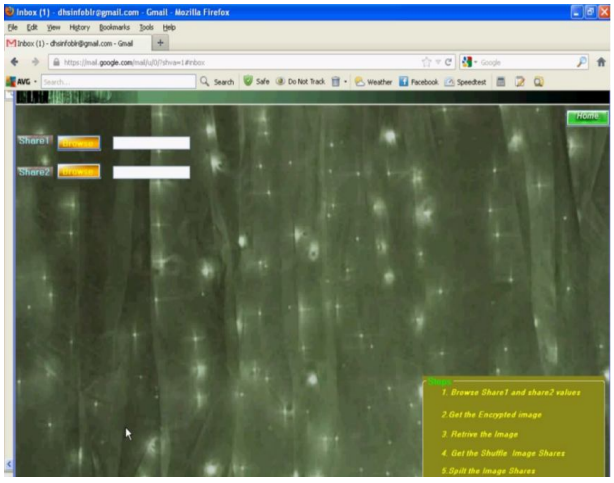
(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

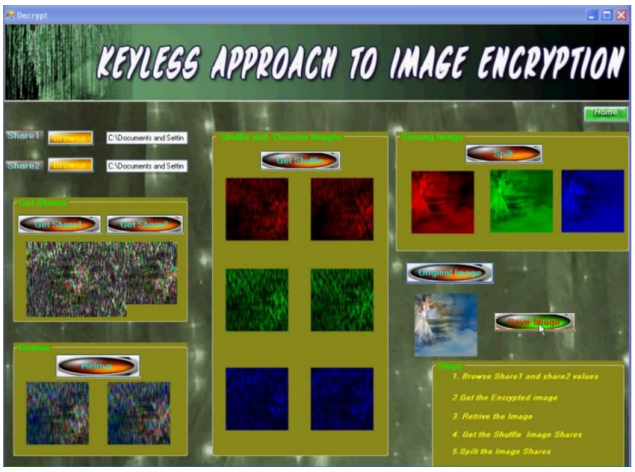
Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

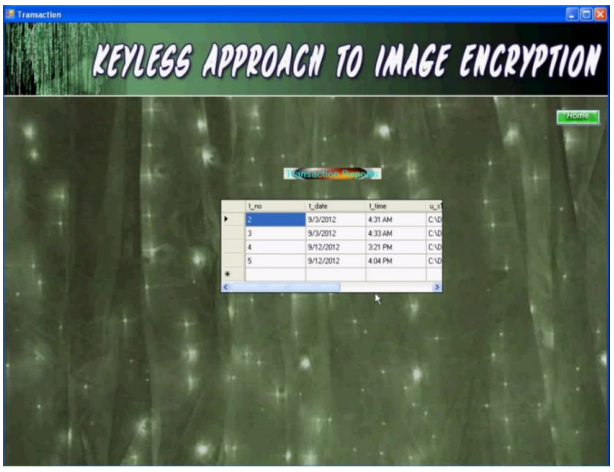
Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014




## VII. CONCLUSION and FUTURE ENHANCEMENT

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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

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. Quantization", International Journal Of Circuits, Systems And Signal Processing, Issue 3, Volume 3, 2009.
2. Xin Zhang and Weibin Chen (2008), A new chaotic algorithm for image encryption, International Conference on Audio, *Language and Image Processing*, (ICALIP 2008), Intelligent systems Design and Applications Of Computer Society, Ieee2008.
3. Aloka Sinha and Kehar Singh (2003), A technique for image encryption using digital signature, Optics Communications, 218(4-6), pp 229-234.
4. S.S.Maniccam, N.G. Bourbakis (2001), Lossless image compression and encryption using SCAN, *Pattern Recognition* 34 (2001), pp 1229-1245.
5. 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.
6. F.Liu,C.K.Wu,X.J.Lin," Colour Visual Cryptography Schemes", Eighth International Conference On