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. 4, Issue 11, November 2016

Visual Cryptography for Image Privacy Protection Using Diverse Image Media

Modhe Nishigandha P[1], Pawar Priti D[2], Sawant Vaibhav L[3], Prof. Sinare P.D[4]

BE. Student, Dept. of Computer Engineering S.C.S.O.E, Rahuri Factory, Maharashtra, India[1,2,3]

Asst. Professor, Dept. of Computer Engineering SCSCOE Rahuri Factory, Maharashtra, India[4]

ABSTRACT: Privacy of Images is very important now a days. There are various methods for privacy protection of images. Visual cryptography can be used for imparting privacy Images. Images could be of different types such as fingerprint, signature Image etc. which is usually used for authentication. The proposed system is used to maintain privacy of images by creating shares of the image using Visual cryptography and securely storing the shares in different databases in the form of QR code. Storing the shares in the form of QR code conceals the share and reduces the risk of information dropping during the transmission phase.

KEYWORDS: Private image, image privacy, Visual Cryptography, Diverse media, QR code

I. INTRODUCTION

A technique that encrypts a secret image into *n* shares, with each participant holding one or more shares is visual cryptography (VC). Secret images can be of different types images, handwritten documents, photographs etc. Sharin gandde ivering secret images is also known as a visual secret sharing (VSS) scheme. The motivation of VC is to securely share secret images in non-computer-aided environments; however, devices with computational powers are ubiquitous (e.g., smart phones).Conventional shares, which consist of many random and meaningless pixels, satisfy the security requirement for protecting secret contents, but they suffer from two drawbacks: a) A high transmission risk because holding noise-like shares will cause attackers' suspicion and the shares may be intercepted. Thus, the risk to both the participants and the shares increases, in turn increasing the probability of transmission failure. b) The meaningless shares are not user friendly. If the number of shares of image increases, it becomes more difficult to maintain the shares, which never give any information for identifying the shares. In the process of encryption plain text will be encrypted to hide secrete message. A key will be provided to encode it and send that encoded text from source to destination. Other side in decryption process received encoded message will be decoded by using the key and original message will be decrypted. The secrete message extracted from encrypted message. The sharedsecrete key plays an important role in whole encryptiondecryption Most of the business organizations need to protect data from disclosure. As the world is more connected by computers, the hackers, power abusers have also increased, and most organizations are afraid to store data in a computer. So there is a need of a method to distribute the data at several places and destroy the original one. When a need of original data arises, it could be reconstructed from the distributed shares. Initially, when it was introduced, its goal was to present its customers a secure information storage media. Secret Sharing can provide confidentiality of the data base. For example, e-voting can be effectively implemented by secret sharing technique. It can ensure confidentiality. It also aims to attain the two goal swhich are somewhat divergent that are data secrecy and data avail ability. If availability was the only goal, then simply duphcatmg the full data in n places would avoid the loss of data up to n-l places from removing the secret. However, this would increase the threats also. Capturing any one of the place can disclose the secret to an enemy. If the single goal were secrecy then the solutions could be splitting of data into n parts and then storing each part at each of the n places. This would result in the need for all n places accessible to retrieve the secret. Though, if there is alteration or destruction of any one part the distributed information would be lost. It ensures secrecy in the face of enemies and thus achieves data integrity and availability with the assistance of its shareholders. General
concept of secret sharing is that, it doesn't want information tobe centralized at one point. For example, in the preparation of plastic cards, such as ATM cards, it can provide good security. Presently, a wide range of its applications have been identified

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. 4, Issue 11, November 2016

II. LITERATURE SURVEY

Visual cryptography concept came into focus to hide the secret text or image behind another image also this concept used by M. Naor and A. Shamir. These can be done by generating the different shares of the image. Then apply the process of encryption to encrypt that image and send to the proper destination. Other side that received shares can be merged to get the original image. But it suffers from the problem of share management, because they generate more than one share to hide the secret image . The problem occurred in the VC scheme that can be overcome by the extended visual cryptography scheme. This VC schemes work on the Share management problem. To get the better solution Kai Hui Lee and Pei-Ling Chiu uses a meaningful cover image concept. This type of VC scheme uses binaryimages. For the purpose of managing shares this technique firstconstruct the meaningful share using an optimization technique.And in the next step it will uses cover images that can beadded in each share directly by a by using the stampingalgorithm. As this VC scheme uses binary image they are notable to maintain the quality of recovered image .
The purpose of such schemes to generate noise-like randompixels on shares to hide secret images which can be done in theconventional visual secret sharing. But it suffers a managementproblem, because of which dealers cannot visually identifyeach share. This management problem is solved by theextended visual cryptography scheme (EVCS), which adds ameaningful cover image in each share. However, the previousapproaches involving the EVCS for general access structuressuffer from a pixel expansion problem A construction of EVCS which is realized by embeddingrandom shares into meaningful covering shares, and we call itthe embedded extended visual cryptography scheme(embedded EVCS). A construction of EVCS which wasrealized by embedding the random shares into the meaningfulcovering shares. A method to improve the visual quality of theshare images. Embedded EVCS has many specific advantagesagainst different well-known schemes, such as can deal withgrey-scale input images, has smaller pixel expansion, alwaysunconditionally secure, does not require complementary shareimages, one participant only needs to carry one share and can

III. PROPOSED ALGORITHM

In the proposed system the trusted third party receives the private image. It generates shares using Visual Cryptography Before transmitting the shares to different servers the shares are converted to QR code by using Diverse Image Media.After converting the shares to QR codes the QR codes are stored at different database at different location or on cloud At the time of retrieval of private image, the QR code is collected from the database, converted to shares. There is no loss of data during conversion of QR code to share. After recovering the shares, both the shares are overlapped i.e. XOR to get the original private image. In cryptography, the one-time pad (OTP), which was proven to be impossible to break if used correctly, was developed by Gilbert Vernam in 1917. Each bit or character from the plaintext is encrypted by a modular addition (or a logical XOR operation) with a bit or character from a secret random key of the same length as the plaintext resulting in a ciphertext. The cipher rtext was sent to a receiver; then, the original plaintext can be decrypted in the receiver side by applying the same operation and the same secret key as the sender used for encrypting the ciphertext. As pointed out by Naor and Shamir, the visual secret sharing scheme is similar to the OTP encryption system. In a (2, 2)-VSS scheme, the secret random key and the ciphertext that can be treated as two shares in the scheme were distributed to two participants who involve in the scheme. Instead of generating a secret random key, we extract the secret key from an arbitrarily picked natural image in the (2, 2)-NVSS scheme. The natural image and the generated share (i.e., ciphertext) were distributed to two participants. In decryption process, the secret key will be extracted again from the natural image and then the secret key as well as the generated share can recover the original secret image.

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. 4, Issue 11, November 2016

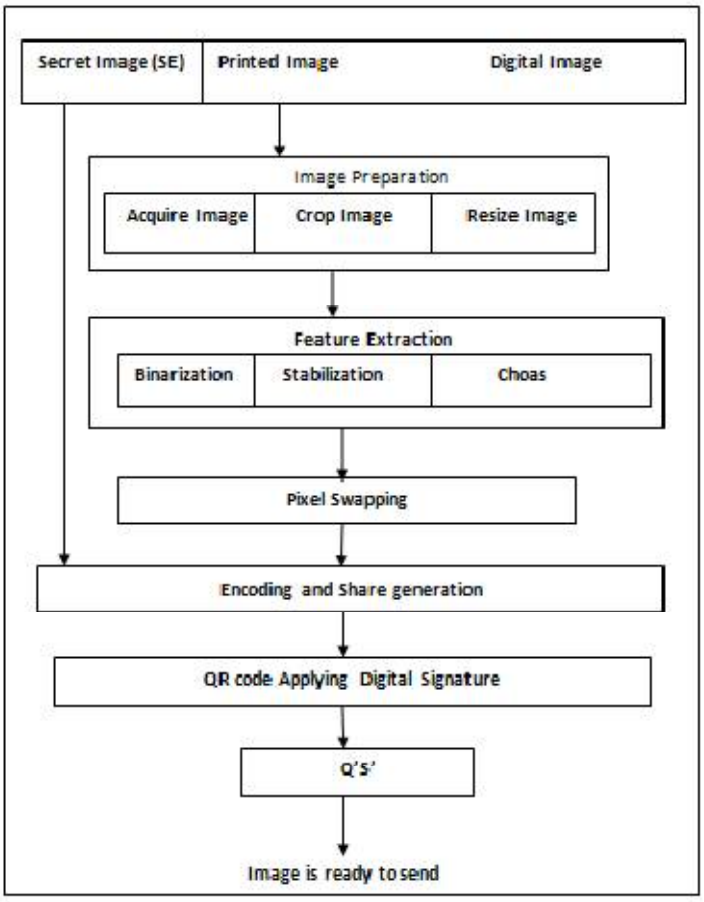

Fig. 1 System Architecture

The feature extraction process is used to extract feature from the natural image by doing the three operations namelyBinarization, stabilization, chaos. Binarization process used to extract feature matrix from natural image. Balancing theoccurrence frequency of values 1 and 0 in the obtained feature matrix can be done in the process of stabilization. The process named chaos is used to eliminate the texture of the extracted feature images and the generated share. In this process, the original feature matrix will be disordered by adding noise in thematrix. Image distortion caused by the image preparation process can be tolerated in the pixel swapping process. The image distortions were introduced in the image preparation process was spread in a feature matrix, and the noise also is distributed in the recovered image without clustering together. Lots of the mage distortions result in noise that appears in the recovered images and if there is large amount of noise clusters together, then the image is severely disrupted which may cause a bad effect on recovered image that it makes impossible task for the naked eye to identify it. The pixel swapping process is the solution for this problem. XOR operation used to do the encryption process. Before applying the XOR operation the stacking process of input image S and feature images FI1,…, FI*n*--1 can be done after that the XOR operation can be apply on in each color plane. Then the resultant image S is the share image ready to send to the destination place. This generated share is secure because the share was generated by stacking a secret image and *n*-1 feature images as well as the pixel values in each feature image are distributed randomly and uniformly. These feature images (FI) can be used as *n*-1 one-time pads (OTP). An important OTP system used which is difficult to break. The length of each

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. 4, Issue 11, November 2016

Methodologies

Feature Extraction Process

1. The Feature Extraction Module The feature extraction module consists of three processes Binarization, stabilization, and chaos processes. First, task is a binary feature matrix is extracted from natural image N via the Binarization process. Then, the stabilization balances the occurrence frequency of values 1 and 0 in the matrix. At last, the chaos process scatters the clustered feature values in the matrix.

2. **The Image Preparation and Pixel Swapping Processes** : The image preparation and pixel swapping processes are used for preprocessing printed images and for post processing the feature matrices that are extracted from the printed images. The printed images were selected for sharing secret images, but the contents of the printed images must be acquired by computational devices and then be transformed into digital data .

Encryption: Input images include *n* -1 natural shares and onesecret image. The output image is look like a noise-like shareimage. Decryption: Input images include *n* -1 natural shares and one noise-like share. The output image is a recovered image i.e. image with secrete message .

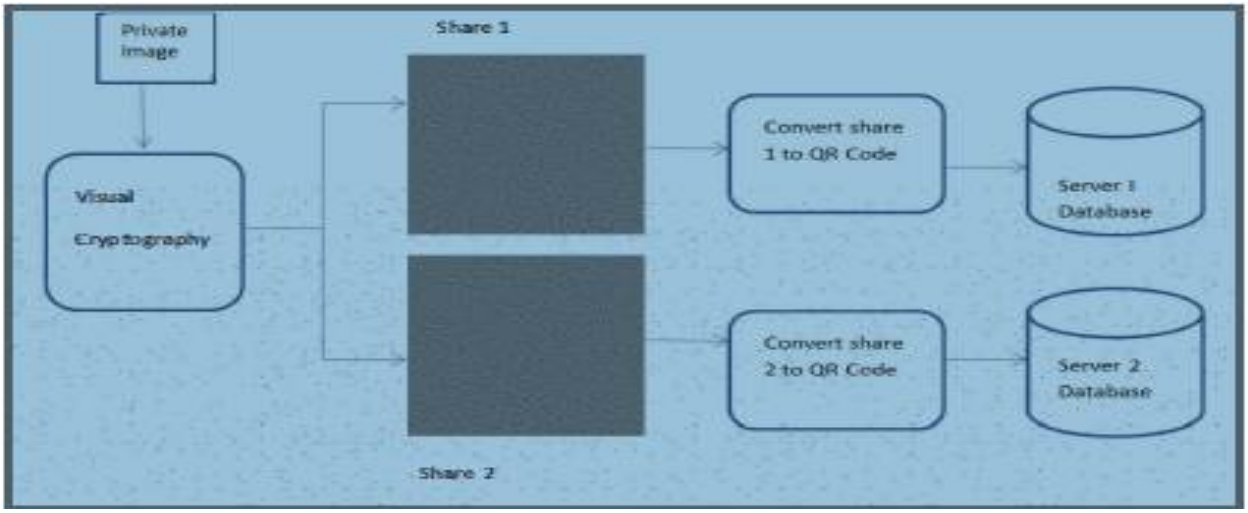

Fig. 2 -Conversion of private image to QR code and storing it on different databases

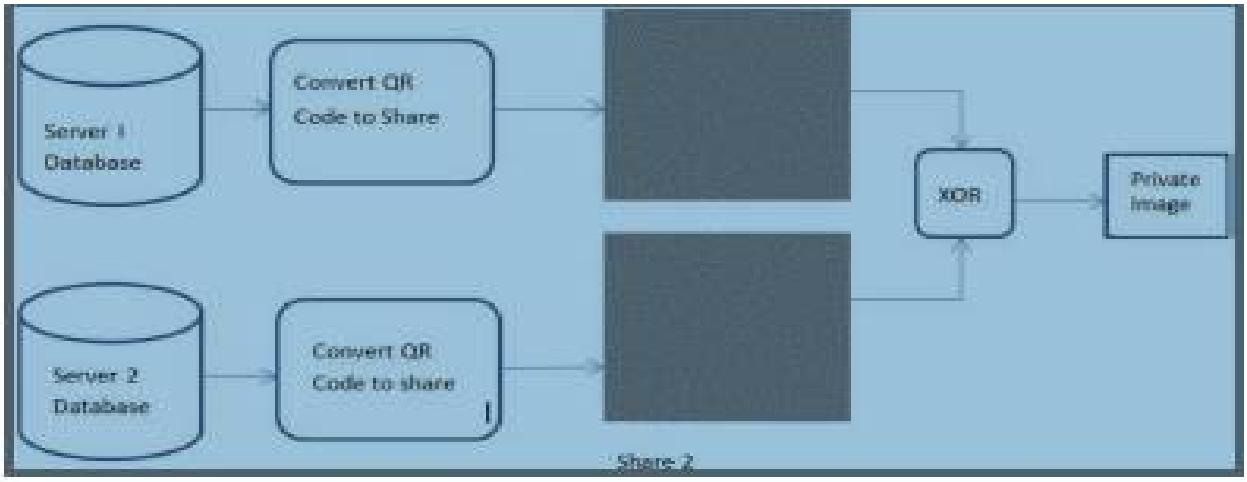

Fig- 3 Recovery of Original Private Image

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. 4, Issue 11, November 2016

Advantages:
1 To reduce the transmission risk, the dealer can choose an image that is not easily suspected as the content of the media (e.g., landscape, portrait photographs, hand-painted pictures, and flysheets). The digital shares can be stored in a participant's digital devices (e.g., digital cameras or smart phones) to reduce the risk of being suspected. The printed media (e.g., flysheets or hand-painted pictures) can be sent via postal or direct mail marketing services. In such a way, the transmission channels are also diverse, further reducing the transmission risk.
2 ransmission is highly secure due to QR code
3Cost for transmission is reduced.
4 Recovered image is almost the same as that of the input image

Algorithm
1>Share Hiding Algorithm
Step 1. Initialize the parameters code.

Step 2. Reduce the amount of information in the feature matrix F to fit within the capacity of the hiding media.

Step 3. Decides the value of stego bit Sb by majority. Function H(S) represents the Hamming weight of bit string S. Then, the stego-bit is appended to bit string FQR .

Step 4. Convert FQR to the numeric string SQR' And finally the SQR is output share image with QR code.

2>Share Extraction Algorithm

Step l. Retrieves the related parameters from SQR.

Step 2. Transform 5 numeric characters into binary form, then removes 5 consecutive numeric characters from the front of number string SQR by calling procedure remov O.

Step 3. Converts string S to its integer value by procedure str2int O.

Step 4. Transforms the value to a corresponding binary bit string and appends it to bit string FQR.

Step 5. Converts FQR to the resultant feature matrix F.

Step 6. Outputs feature matrix F.

Applications:
1 Secure Web Browsing Using Secure Socket Layer (SSL) Or Transport Layer Security (TLS) Proto Cols, The Use Of Encryption May Be Transparent To Users.
2 Encrypting entity needs to share the key with a separate decrypting entity, the key must be transported to the decrypting entity in a secure manner.
3 It also applied in the field of ecology, biometrics and medical applications.

IV. CONCLUSION

QR code used to store the shares on different servers. The Natural Image used to encode the share into QR code is known only to the trusted third party. So only the trusted third party can encode the share to QR code and decode QR code to share image.

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. 4, Issue 11, November 2016

REFERENCES

1. Visual Secrete Sharing by Diverse Image Media, Jyoti Rao, IJECS Volume 4 Issue 4 April, 2015
2. Digital Image Sharing By Diverse Image Media Using Nvss Technique , R.H. Adekar1, N.M. Jadhav2, N.D. Pergad3,Vol-2 Issue-1 2016 Ijariie-Issn(O)-2395-4396
3. Visual Cryptography for Image Privacy protection using Diverse Image media Aparna Bhosale , Jyoti Rao,978-1-4673-7910-6/15/$31.00 ©2015 IEEE