Perspectives in Communication, Embedded-Systems and Signal-Processing (PiCES) – An International Journal
ISSN: 2566-932X, Vol. 5, Issue 1, April 2021

Part of the Proceedings of the 1st All India Paper writing Competition on Emerging Research - PaCER 2020

Visual Secret Sharing Scheme Using Encrypting Multiple Images

A Shvetha
Information Technology, Sethu Institute of Technology, Madurai, India. shvethaa05@gmail.com

S Rathnamala
M.Tech.,(Ph.D), Information Technology, Sethu Institute of Technology, Madurai, India. rathnamala@sethu.ac.in

M V Meenumathi
Information Technology, Sethu Institute of Technology, Madurai, India. meenumv1999@gmail.com

Abstract: The new VSS scheme introduces two distinct phases such as Message-oriented Security and Image-based Sensitive Scheme. Through this approach the new framework is improving our privacy and secret sharing security. The main purpose of this work is to hide reversible separable data in the image. In the first step a content provider will use encryption key to encrypt the uncompressed original file. Here we use a data hiding key for the purpose of compressing the least significant bits of the encrypted image in order to generate space for certain additional data. Even if the image content is unknown, the recipient can extract the encrypted image which contains additional data with the data hiding key. The data hiding key and the encryption key can be used to recover additional data and to retrieve the original content without error. The proposed system is to reduce the problems of previous secret sharing. The project's aim is the Multiple Secret Sharing is a cryptosystem that encrypts a secret into multiple shares such that any eligible combination of shares can recreate the secret, whereas any prohibited combination of shares doesn't disclose any secret details.

Keywords: Visual Secret Sharing (VSS); Data Hiding; Data Encryption and Decryption; Embedding; Image Compression; Image Share

I. INTRODUCTION

The processing of signals in the encrypted sector has received significant interest in recent studies. The point of this article is to discuss the efficient method of hiding data in encrypted images from the reference paper on Separable reversible data hiding in encrypted image [6]. According to [6], "*the encryption converts the ordinary signal into unintelligible data as an effective and popular means of privacy protection, so that traditional signal processing usually takes place before encryption or decryption. However, the ability to manipulate the encrypted data when keeping the plain content unrevealed is desired in some scenarios where a content owner does not trust the processing service provider. For example, when the secret data to be transmitted are encrypted a channel provider may tend to compress the encrypted data due to the limited channel resource without any knowledge of the cryptographic key. Although a lossless way of compressing an encrypted binary image by finding the syndromes of low-density parity-check codes, a lossless compression method for encrypted gray image is built using progressive decomposition and rate-compatible punctured turbo codes.*" With the lossy compression process, an encrypted gray image can be effectively compressed by discarding the excessive rough and fine information generated from orthogonal transform coefficients. A receiver can recreate the key content of the original image by retrieving the values of coefficients by having the compressed images. The transform computation has also been studied in the encrypted domain. The discrete Fourier transformation in the encrypted domain may be implemented based on the homomorphic properties of the underlying cryptosystem.

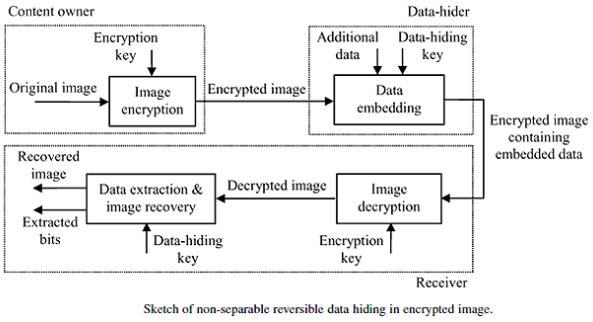

Fig 1. Non-Separable Reversible Data Hiding in Encrypted Image

II. RELATED WORKS

[1] Isha Padiya, Vinod Manure and Ashok Vidhate have proposed the specific approach to color image visual cryptography, the proposed algorithm divides a hidden image into two shares based on three basic color components.

The secret color image is decomposed into three planes namely red, green, blue displays the three primitive color components of the secret color image, where each picture has 256 levels of the corresponding primitive color, and each pixel represents 24 bits. Encrypting the color space,

half tone the image and divide the image into two shares. Two shares will be generated by the following method.

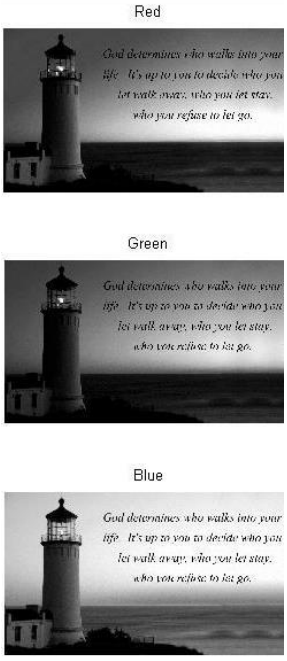

Fig 2. Primitive color (R, G, and B) component

1) Read the pixel value concerning ii (number of rows of secret image) and jj (number of columns of secret image).

   sij = I(ii,jj);

2) Invert pixels.

   sij1 = 255-sij;

3) Read and convert to shares each pixel.

4) Reduce sij.

5) Invert pixels.

6) Take the difference of two original pixel random generators.

7) Invert pixels.

After we have mixed share1 and share 2 with three RGB planes we get decrypted image. The decrypted image size is similar to that of the secret image.

[2] Manami Sasaki and Yodai Watanabe proposed the paper to optimize the range of visual secret sharing (VSS) access control schemes which encrypt multiple images. First, to those for multiple secrets, the formulation of access mechanisms for a single secret is generalized. This generalization is maximal in the sense that there are no restrictions on access structures in the generalized formulation in particular it includes the existing ones as special cases. Next, a sufficient condition is introduced to satisfy the encryption of VSS schemes that realize an access structure for the most general form of multiple secrets, and two constructions of VSS schemes are provided with encryption that meets that condition. Each of the two constructions has its advantage over the other, the one is more general and can generate VSS schemes with a strictly better contrast and pixel expansion compared to the other. Additionally, the pixel extensions of the VSS schemes generated by the latter construction are estimated for threshold access structures and turn out to be the same as those of the existing schemes called the multiple threshold secret visual cryptographic schemes. Finally, the optimality of the previous construction is tested, allowing the existence of access structures for which no optimal VSS schemes are created.

[3] Haiping Lu, Alex C. Kot and Jun Cheng have proposed a paper entitled “Secure Data Hiding in Binary Document Images for Authentication”. This paper presents an algorithm for data hiding for binary documents images. This algorithm is based on the calculation of distance reciprocal distortion used in binary images of documents to determine the distortion caused by the flipping of a certain pixel. Pixels which will produce less distortion after turning are the preferred flip candidates. They integrate the system by enforcing the uniform characteristics of blocks that are uniform and use a 2-D shift to ensure tamper proofing and authentication security. Experiments show that the watermark image has good quality, and it is possible to successfully detect content manipulation. This paper, for the authentication of digital documents in binary image format, proposes a secure data hiding algorithm based on the DRDM test. They combine a 2-D shifting technique with an odd-even embedding scheme and select the appropriate pixels to flip using the DRDM scheme. Experiments demonstrate the imperceptibility of the algorithm and can be used for authentication and tamper proofing. The key downside of this proposed scheme is the variability that is found in the hiding images.

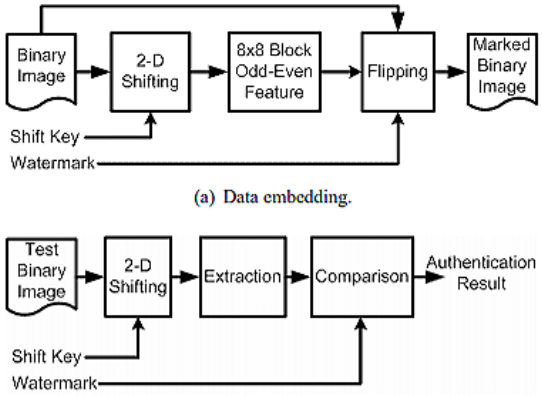

Fig 3. Data hiding algorithm for binary document image.

III. PROPOSED SYSTEM

In the earlier process the dealer (or) user shares only one secret among the participants in every secret sharing process. The dealer and participants are deemed to be honest absolutely. The existing process has more complex stages. The proposed system is to minimize the previous Multi-Secret sharing scheme and reconstruction issues. The new scheme introducing two different phases such as Message oriented Security and Image based Sensitive Scheme. Here, we introduce message based privacy by using RDH Algorithm to reverse the multi secret sharing scheme and encrypt the reversed message via the AES Algorithm. The second stage is privacy based image. The image based privacy is applied by internal water marking Techniques, image compression, encryption and wrapping Techniques also. The image based privacy approach having separate algorithm.

In authentication based on VSS schemes that encrypt a single secret image, an adversary's way of detecting tampering is to divide the secret image into two disjoint areas: one for one message and the other for detection (see e.g. the first method “content areas and black areas”). On the other hand, VSS schemes encrypting multiple images allow the authentication that can be identical with the above two areas; for instance, the authentication in which Shares 1 and 3 are distributed to a human recipient, Share 2 is generated by an informant, and the two secrets v1 and v2 are taken to be an all-black image for the detection and an image for a message, respectively.

Modules:

A) System initialization

B) Secret share generation

C) Secret construction and distribution

D) Verification and secret reconstruction

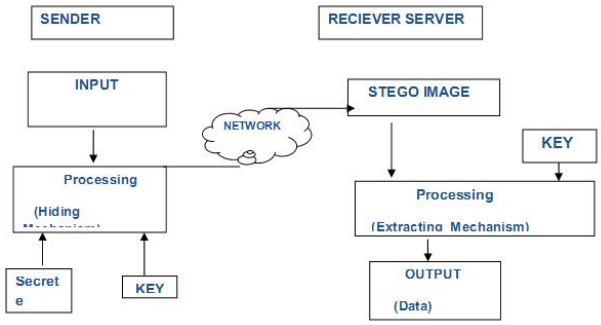

Fig 4. Proposed Architecture Diagram

A. System Initialization

This module allows the user to register with the administrator as a valid user by submitting their profile. Upon registration of the User, the User may share secret communication via local mail. The sent and received mail will receive as per registered account. The remaining modules will be used to approach the multi-stage secret sharing system.

B. Secret Share Generation

The Secret Sharing Generation having 2 stages like communication based preprocessing and multimedia object reconstruction through multi-stages. This module maintains communication based preprocessing like Reversing the original content, Algorithm based Encrypt the reversed content and keep security key based multimedia object embedding of secret message.

C. Secret Construction and Distribution

The complete process of Secret share generation, construction process started. This module is multi-based construction with secret share generation result. The Secret Construction using embedding encrypted message into multi-media object, continue to apply lossy compression, file encryption and File wrapper approach also. The segmented original identity will distribute single or multiple secret key recipients.

D. Verification and secret reconstruction

The verification and reconstruction module consists valid receiver will be reconstructing the sender produced secret sharing. The reviewed multi-segmented identity will download and continue to merge, decrypting, and decompressing. The reviewed original identity having security key with encrypted message. The encrypted message will apply reconstruction stage-1. The message oriented reconstruction used to identify secret message and also get original object.

IV. WORKING PRINCIPLE

A. User Module

This module allows the user to register with the administrator as a valid user by submitting their profile. Once the user is registered, the user may send mail and view the received mail. The item Sent can store the users' mail. User can also add or modify or view the address book maintain by the application.

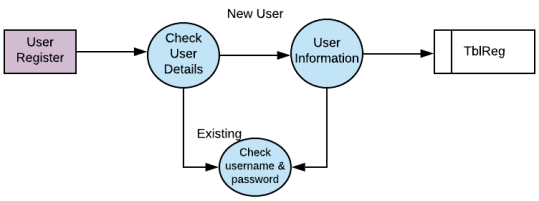

Fig 5. User Registration

B. Admin Module

Only admin can able to validate the user data and activate the user account. There is a separate mailbox for

the administrator who would like to send mail, review mail.

C. Data Hiding

Also, a data-hider can hide reversible data by using the histogram modifying mechanism. The host image is split into block size and a circle is mapped with gray values. Once the histogram of the two sub regions in this circle is pseudo-randomly segmented into two subsets, rotation is used to embed a bit in each of the blocks. The original block could be recovered from a marked image on the receiving side in the inverse process.

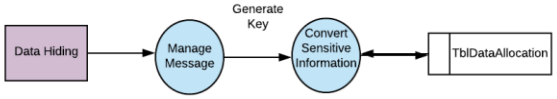

Fig 6. Data Hiding

D. Reversible Data Hiding

The secret and auxiliary data used to recover the content are conveyed by the difference between the pixel value and the corresponding estimates of the neighbor, and the estimate errors are altered by an optimal value transfer matrix. The optimal value transfer matrix is generated to maximize the amount of secret data. The embedded secret data can be retrieved successfully by a receiver and the original content can be recovered in the subgroups in inverse order. Reverse user message with RDH Algorithm is the state of data hiding process. The reversed original message will be converted into encrypt with the help of MD5 Algorithm. In the Image, the encrypted message is embedded. The encrypted message will encrypt the image through the AES algorithm. Finally, we split into the encrypted file using unique key with file wrapper algorithm.

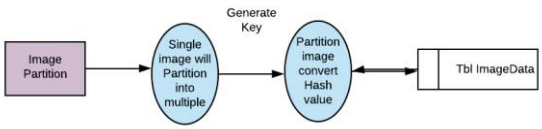

Fig 7. Image Partition

E. Data Extraction and Content Recovery

First, the receiver divides the image into Sets A and B when it has an image that contains embedded data, since Sets A and B are divided into several subsets using the same method.

V. PERFORMANCE ANALYSIS

In the experiment the test image Lena size 512 x 512 shown in Fig.8 was used as the original image. After the image has been encrypted, the eight encrypted bits of each pixel are converted to a gray value to generate an encrypted image. Then, we let M = 3, L = 128 and S = 2 to embed 4.4 X 10^3 additional bits into the encrypted image. The encrypted image contains the embedded data and the R embedded rate is 0.017 bit per pixel (bpp). We could use the data-hiding key to extract additional data with an encrypted image containing embedded data. If we decrypted the encrypted image directly using the embedded data encryption key, the PSNR value in the decrypted image was 39.0 dB which verifies the calculated theoretical value of 39.1dB. Using the keys of encryption and hidden data, the data which was embedded could be extracted successfully. Recovery of the original image could be performed from the data encompassed encrypted image.

1) Tables II and III list the rates of embedding, PSNR in directly decrypted images, and PSNR in recovered images when using the Lena and Man images with different M, L and S. The embedding rate depends on S and L as analyzed, and a higher embedding rate corresponds to the higher and lower S. On the other hand, the smaller the values of M and S, the better the quality of the directly decrypted image, since more data will not be changed in encrypted image by embedding the data. The "+" in Tables II and III indicates the recovery of the original images without any error. Here, the large M, L and the small S are helpful for the perfect recovery of content since the recovery process involves more cover data and fewer possible solutions.

2) Here, three quality metrics were used to measure distortions in directly decrypted images: PSNR, Watson metric and a Q universal quality index. While PSNR simply indicates the energy distortion caused by data hiding, the Watson metric is designed using characteristics of the human visual system and measures the total perceptual error based on DCT, taking into account three factors: contrast sensitivity and masking and luminance masking. Additionally, in the spatial domain the quality index Q works as a combination of loss of correlation, distortion of luminance, and distortion of contrast. Higher PSNR, lower metric Watson or greater Q means better quality.

TABLE II
EMBEDDING RATE R, PSNR IN DIRECTLY DECRYPTED IMAGES (DB) AND PSNR IN RECOVERED IMAGES (DB) WITH DIFFERENT PARAMETERS FOR TEST IMAGE LENA

		$S=1$	$S=2$	$S=3$	$S=4$	$S=5$
$M=1$	$L=2000$	0.0005, 54.6, +∞	0.0010, 52.3, +∞	0.0015, 51.6, +∞	0.0020, 51.4, +∞	0.0025, 51.3, +∞
	$L=1500$	0.0067, 54.3, +∞	0.0013, 52.2, +∞	0.0020, 51.7, +∞	0.0027, 51.4, +∞	0.0033, 51.3, 73.8
	$L=1000$	0.0010, 54.3, +∞	0.0020, 52.2, +∞	0.0030, 51.5, 70.4	0.0040, 51.3, 68.2	0.0050, 51.2, 70.6
$M=2$	$L=400$	0.0025, 47.7, +∞	0.0050, 45.3, +∞	0.0075, 44.7, +∞	0.010, 44.3, +∞	0.013, 44.2, 72.6
	$L=300$	0.0033, 47.5, +∞	0.0067, 45.3, +∞	0.010, 44.6, +∞	0.013, 44.4, 73.6	0.017, 44.2, 70.2
	$L=200$	0.005, 47.6, +∞	0.010, 45.2, +∞	0.015, 44.7, 68.3	0.020, 44.4, 62.6	0.025, 44.2, 61.9
$M=3$	$L=150$	0.007, 41.4, +∞	0.013, 39.0, +∞	0.020, 38.4, +∞	0.027, 38.1, +∞	0.033, 38.0, +∞
	$L=125$	0.008, 41.4, +∞	0.016, 39.0, +∞	0.024, 38.5, +∞	0.032, 38.1, +∞	0.040, 38.0, 71.5
	$L=100$	0.010, 41.0, +∞	0.020, 39.0, +∞	0.030, 38.5, 67.8	0.040, 38.1, 67.9	0.050, 38.0, 65.3

Fig 8. Performance Analysis

VI. CONCLUSION

The objective of this paper is therefore to create user-friendly software with the required modules to support the

hiding of data and the extraction of data. Strong need to develop the secure secret scheme for sharing images over network, as per survey. We proposed a work for that purpose, which consists of hiding data and extracting data. This is a new LSB based digital watermarking system that combines LSB with reverse bit. The test result shows that the proposed algorithm maintains the watermark quality of the image. This work proposes a compressing scheme of encrypted images with auxiliary information. The channel provider uses ideal parameters derived from the first part of the auxiliary information to quantize encrypted data and then transmit an encrypted image when the content owner produces encrypted images and supporting information. The main image contents can be reconstructed on the recipient side with the compressed encrypted data and the secret key.

REFERENCES

[1] Isha Padiya, Vinod Manure, Ashok Vidhate, "Visual Secret Sharing Scheme Using Encrypting Multiple Images", IJAREEIE, Vol.4, Issue 1, January 2015.

[2] H. Yang and A. C. Kot, "Pattern-based data hiding for binary image authentication by connectivity-preserving," IEEE Trans. Multimedia, vol. 9, no. 3, pp. 475–486, Apr. 2007.

[3] Q. G. Mei, E. K. Wong, and N. D. Memon, "Data hiding in binary text documents," Proc. SPIE, vol. 4314, pp. 369–375, Aug. 2001.

[4] Manami Sasaki and Yodai Watanabe, "Visual Secret Sharing Scheme Encrypting Multiple Images", IEEE Transactions on Information Forensics and Security, Vol.13, No.2, February 2018.

[5] "Secure Data Hiding In Binary Document Images For Authentication", Haiping Lu, Alex C. Kot and Jun Cheng.

[6] Zhang, Xinpeng, "Separable Reversible Data Hiding in Encrypted Image", IEEE Transactions on Information Forensics and Security, Vol 7, Issue 2, April 2012.