IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECRET IMAGE SHARING WITH STEGANOGRAPHY SCHEME UTILIZING OAEP AND IDA

[1] Mr. Pranob K Charles, [2]P. Karthik Ram, [3]R. Anil, [4]Y. Seshu Babu, [5]P. Viswa Teja

[1]Assistant professor, [2]Final B.Tech, [3]Final B.Tech, [4] Final B.Tech, [5]Final B.Tech
[1]Department of Electronics and Communication Engineering,
[1] Andhra Loyola Institute of Engineering and Technology, Vijayawada, India.

Abstract- **Secret image sharing schemes are employed to safeguard the confidentiality and availability of critical commercial or military images. In secret image sharing, the image is divided into several stego images, which are managed by corresponding participants. The secret image can be recovered only when the number of authorized participants is no less than the threshold. However, many of the existing image sharing schemes have some security flaws that can reveal key elements of the shared secret image. In this project, to overcome these weaknesses, we will modify a secret image sharing scheme which utilizes Optimal Asymmetric Encryption Padding (OAEP) and Information Dispersal Algorithms (IDA). The proposed scheme provides computational security and better performance in share generation and secret reconstruction. In this project, we use optimal asymmetric encryption padding and information dispersal to analysis a novel computationally secure image sharing scheme and demonstrate that its performance is higher than polynomial based secret image sharing (PBSIS) based method.**

Keywords- **Secret sharing, steganography, OAEP, IDA, PBSIS, Edge-based Steganography method, steganalysis.**

I.INTRODUCTION

With the rapid development of Internet and continuing increase of network bandwidth, images are used more and more often in commercial, military or personal areas. How to tighten image security has become an important problem nowadays. Image encryption is a conventional method to protect an image by making it unreadable without a proper key, but the storage of the noise-like encrypted image in a public cloud, or transmission over an insecure communication channel, may easily arouse attacker's attention, and the encrypted image may thus be destroyed, intercepted or decrypted with brute force. Image steganography is another kind of novel technique developed in recent years for keeping an image safe by embedding it into the innocuous cover media with the use of information hiding techniques. It conceals the existence of a secret image of great importance, as well as protecting its contents. However, an obvious flaws of steganographic methods is that a single misfortune, such as cloud storage breakdown, cover media damage and computer sabotage, can make the protected image inaccessible. The schemes of dealing with such kind of problems are worth the researcher's while to explore.

In order to safely transmission of confidential data, the multimedia object like audio, video, images are used as a cover sources to hide the data. Steganography is defined as the study of invisible communication. Steganography usually deals with the ways of hiding the existence of the communicated data in such a way that it remains confidential. It maintains secrecy between two communicating parties. We also analyse the security of the proposed scheme formally using Random Oracle model and prove that the confidentiality of the secret image is guaranteed in the face of computationally bounded adversaries. Additionally, we will implement a proposed edge-based steganography method to conceal the participant's shares in cover images. We will achieve higher visual quality and better resistance against steganalysis methods.

In this project, we use optimal asymmetric encryption padding and information dispersal to analysis a novel computationally secure image sharing scheme and demonstrate that its performance is higher than polynomial based secret image sharing (PBSIS) based method. And we implement the proposed steganography method to embed the shadows in the edges of cover images.

Steganography is the art and science of hiding information by embedding messages within other, seemingly harmless messages. Steganography means "covered writing" in Greek. As the goal of steganography is to hide the presence of a message and to create a covert channel, it can be seen as the complement of cryptography, whose goal is to hide the content of a message.

The goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second secret message present." By using this proposed algorithm, we can hide our file of any format in an image and audio file. We can then send the image via e-mail attachment or post it on the web site and anyone with knowledge that it contains secret information, and who is in possession of the encryption password, will be able to open the file, extract the secret information and decrypt it. Steganography literally means covered writing. Its goal is to hide the fact that communication is taking place. In the field of Stenography, some terminology has been developed. The term cover is used to describe the original, innocent message, data, audio, still, video and so on. The growing possibilities of modem communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the Internet increases.

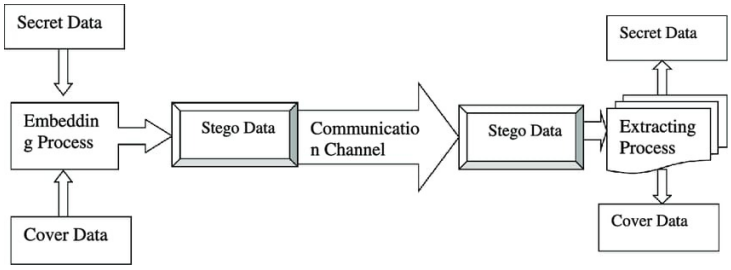

Fig: Block diagram of secret Image transmission using steganography process

II. MOTIVATION

Steganography in ancient Greece, the first book was published in 1499 and it titled as Steganographia. In 1985, Modern steganography is introduced. Steganography is a scheme of hiding information and sharing secret data. The goal of steganography is to hide the data from a third-party people. It is a scheme of hiding data in such a way that no one apart from the sender and receiver even realises that there is hidden data. The hidden data can be in form of an image, text, video. Steganography is used mostly used in military applications to disguise information. In military, sharing of information is highly secured and it is very difficult for a third-party people like hackers, other country forces to decrypt that data.

III. METHODOLOGY

The scheme which we implemented in our research work is briefly explained in following steps
Step 1: Literature survey and a thorough review of the techniques which have been reported is observed.
Step 2: In this scheme, we share a secret image from transmitter to receiver using OAEP and IDA methods. OAEP stands for Optimal asymmetric encryption padding. It is a padding process for encrypting a secret data. IDA is an algorithm which is used for partitioning shares of given secret image.
Step 3: After partitioning secret image into shadows, these shadow images are padded with a cover images of each.
Step 4: Then those secret images which are padded by a cover image will be given as shares to participants.
Step 5: Performance parameters like PSNR and SSIM are simulated and observed. SSIM and PSNR are two parameters that are widely used for image quality assessment.

IV. EXPERIMENT AND SIMULATION

OAEP method

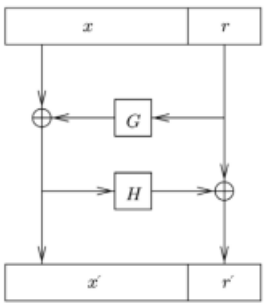

Fig: Diagram of OAEP

For a secret data of length n and a security parameter λ, OAEP uses the following functions:
$G : \{0, 1\}^{\lambda} \rightarrow \{0, 1\}^{n}$
$H : \{0, 1\}^{n} \rightarrow \{0, 1\}^{\lambda}$
where G and H are random oracles. Using these functions,
$OAEP : \{0, 1\}^{n} \times \{0, 1\}^{n} \rightarrow \{0, 1\}^{n+\lambda}$ is defined as:
$OAEP^{G,H}(x, y) = x \oplus G(r) \parallel r \oplus H(x \oplus G(r))$
where $\parallel$ denotes the string concatenation, x is the input message of length n, r is a random string of length λ, and λ is the security parameter of the transform (e.g. $\lambda = 256\ bit$). A diagram of OAEP is depicted in above fig

IDA method

The basic idea of an IDA is to add some redundancy to the data and then partition it among n parties. IDA stands for information dispersal algorithm. It is a code to generate the shares. A non-systematic Reed–Solomon code can be easily converted to a systematic one by modifying its generator matrix.

We present the Information Dispersal Algorithm (IDA) which breaks a file F of length L = |F| into n pieces F i , $1 \leq i \leq n$, each of length |F i | = L/m, so that every m pieces suffice for reconstructing F. Dispersal and reconstruction are computationally efficient. The sum of lengths |F i | is (n/m) L. Since n/m can be chosen to be close to 1, the IDA is space efficient. IDA has numerous applications to secure and reliable storage of information in computer networks and even on single disks, to fault-tolerant and efficient transmission of information in networks, and to communications between processors in parallel computers. Here we also give applications to the problem of data consistency and availability in distributed systems, and to a distributed pattern matching algorithm.

Steganalysis method

Steganalysis is the study of detecting hidden data using steganography. Steganalysis will identify suspected packages, determine whether they have a payload encoded into them and if possible, recover that payload.

GUI In MATLAB:

In our project we used GUI in MATLAB software for demonstrating our project. Graphical user interfaces (GUIs), also known as apps, provide point-and-click control of your software applications, eliminating the need for others to learn a language or type commands in order to run the application. You can share apps both for use within MATLAB and also as standalone desktop or web apps.

You can choose from the following three ways to create an app in MATLAB:

- **Convert a script into a simple app:** Choose this option when you want to share a script with students or colleagues and allow them to modify variables using interactive controls.
- **Create an app interactively**: Choose this option when you want to create a more sophisticated app using a drag-and-drop environment to build the user interface.
- **Create an app programmatically:** Choose this option when you want to create an app's user interface by writing the code yourself.

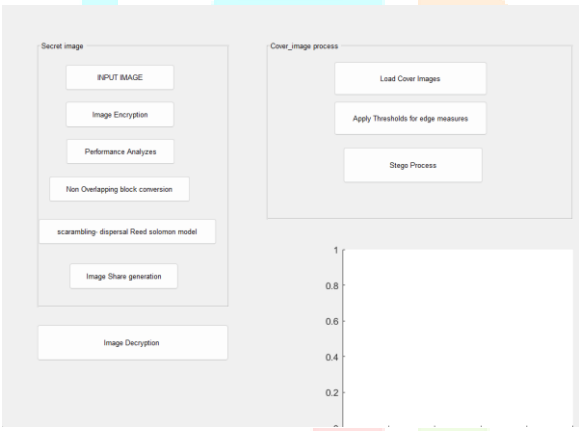

Fig. GUI in MATLAB

V. RESULTS

In this project, we used OAEP and IDA methods for secret image sharing. The below shown figures are the results that has been simulated in MATLAB software for the proposed method. The results are secret image, cover image, threshold applied cover image, OAEP output, Image share generation, Stego images, performance parameters, decrypted image.

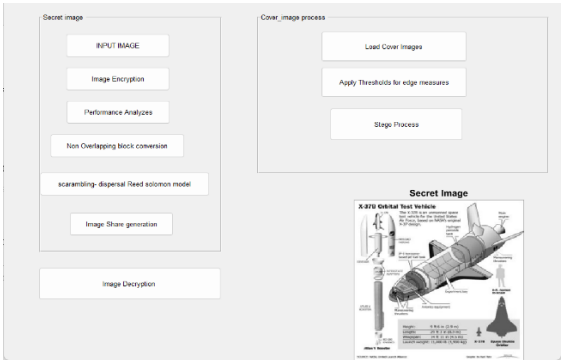

Fig: secret Image

Fig: Cover Image

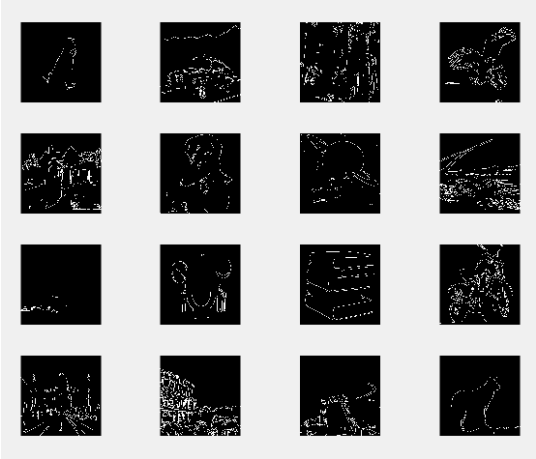

Fig: Threshold applied cover images

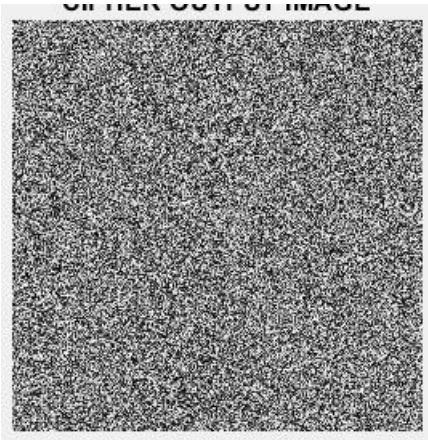

Fig. OAEP output

Fig:Stego imhages

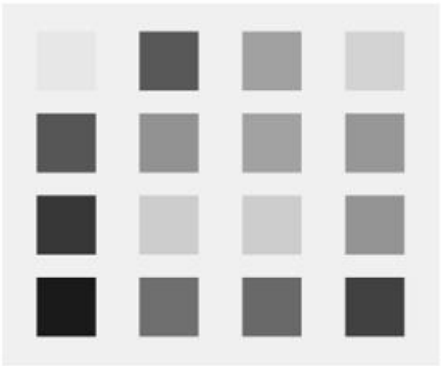

Fig: Shares generated using IDA algorithm

```
PSNR measure

psnr =

   31.3808

mse =

   1.5327e+04

SSIM measure

mssim =

    0.0079

>>
```

Fig: Performance parameters obtained in MATLAB

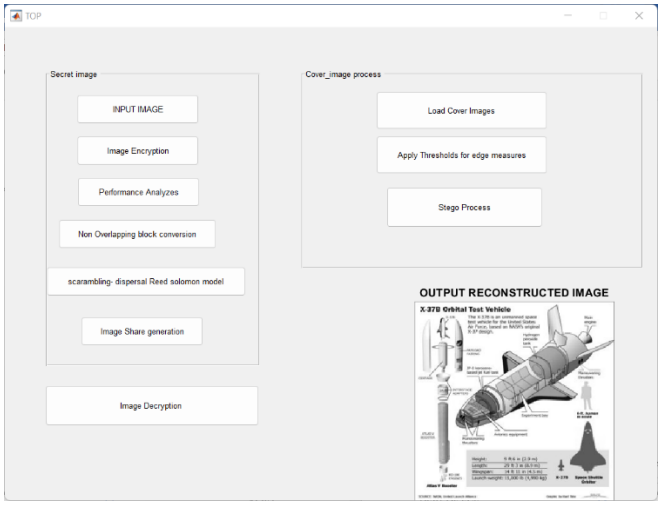

Fig: Decrypted image

VI. CONCLUSION AND FUTURE SCOPE

In this paper, we introduce polynomial-based secret image sharing (PBSIS) scheme which includes optimal asymmetric encryption padding (OAEP) based image encryption and improved information dispersal algorithms (IDA) for a novel computationally secure secret image sharing scheme. The proposed image sharing models offered the benefits of computational security and small shadow size. Experimental results proved the computational efficiency and validate that the performance of the proposed scheme superior than existing PBSIS methods. The image steganography embed the shadows only in the edges of cover images which makes the proposed steganography resistance against steganalysis algorithms.

REFERENCES

[1] G.R. Blakley, Safeguarding cryptographic keys, in: Proc. of the National Computer Conference1979, Vol. 48, 1979, pp. 313–317.

[2] A. Shamir, How to share a secret, Commun. ACM 22 (11) (1979) 612–613.

[3] M. Naor, A. Shamir, Visual cryptography, in: Workshop on the Theory and Application of of Cryptographic Techniques, Springer, 1994, pp. 1–12. [4] C.-C. Thien, J.-C. Lin, Secret image sharing, Comput. Graph. 26

(5) (2002) 765–770. [5] Y.-S. Wu, C.-C. Thien, J.-C. Lin, Sharing and hiding secret images with size constraint, Pattern Recognit. 37 (7) (2004) 1377–1385.

[6] C.-C. Chang, Y.-P. Hsieh, C.-H. Lin, Sharing secrets in stego images with authentication, Pattern Recognit. 41 (10) (2008) 3130–3137.

[7] Y.-Y. Lin, R.-Z. Wang, Scalable secret image sharing with smaller shadow images, IEEE Signal Process. Lett. 17 (3) (2010) 316–319.

[8] C.-C. Wu, S.-J. Kao, M.-S. Hwang, A high quality image sharing with steganography and adaptive authentication scheme, J. Syst. Softw. 84 (12) (2011) 2196–2207.

[9] Z. Eslami, J.Z. Ahmadabadi, Secret image sharing with authentication-chaining and dynamic embedding, J. Syst. Softw. 84 (5) (2011) 803–809. [10] G. Ulutas, M. Ulutas, V.V. Nabiyev, Secret image sharing scheme with adaptive authentication strength, Pattern Recognit. Lett. 34 (3) (2013) 283–291.

[11] M.J. Khosravi, A.R. Naghsh-Nilchi, A novel joint secret image sharing and robust steganography method using wavelet, Multimedia Syst 20 (2) (2014) 215–226.

[12] J. He, W. Lan, S. Tang, A secure image sharing scheme with high quality stegoimages based on steganography, Multimedia Tools Appl. (2016) 1–22.

[13] P. Li, Q. Kong, Y. Ma, Image secret sharing and hiding with authentication based on psnr estimation, J. Inf. Hiding Multimedia Signal Process. 5 (2) (2014) 353–366.

[14] G. Ulutas, M. Ulutas, V. Nabiyev, Distortion free geometry based secret image sharing, Procedia Comput. Sci. 3 (2011) 721–726.

[15] C. Asmuth, J. Bloom, A modular approach to key safeguarding, IEEE Trans. Inf. Theory 29 (2) (1983) 208–210.

[16] M. Ulutas, V.V. Nabiyev, G. Ulutas, A new secret image sharing technique based on asmuth bloom's scheme, in: Application of Information and Communication Technologies,

2009. AICT 2009. International Conference on, IEEE, 2009, pp. 1–5.

[17] G. Alvarez, A.H. Encinas, L.H. Encinas, A.M. del Rey, A secure scheme to share secret color images, Comput. Phys. Commun. 173 (1) (2005) 9–16.

[18] Z. Eslami, S. Razzaghi, J.Z. Ahmadabadi, Secret image sharing based on cellular automata and steganography, Pattern Recognit. 43 (1) (2010) 397–404.

[19] J. Zarepour-Ahmadabadi, M.S. Ahmadabadi, A. Latif, An adaptive secret image sharing with a new bitwise steganographic property, Inform. Sci. 369 (2016) 467– 480.

[20] C.-C. Lin, W.-H. Tsai, Secret image sharing with steganography and authentication, J. Syst. Software 73 (3) (2004) 405–414.

[21] C.-N. Yang, T.-S. Chen, K.H. Yu, C.-C. Wang, Improvements of image sharing with steganography and authentication, J. Syst. Software 80 (7) (2007) 1070–1076.

[22] P.-Y. Lin, J.-S. Lee, C.-C. Chang, Distortion-free secret image sharing mechanism using modulus operator, Pattern Recognit. 42 (5) (2009) 886–895.

[23] A.M. Ahmadian, M. Amirmazlaghani, Computationally secure secret image sharing, in: Electrical Engineering (ICEE), 2017 Iranian Conference on, IEEE, 2017, pp. 2217–2222.