Securing Data through Steganography & Secret Sharing Schemes

K.Chandra Sekhar[1], A.Manju[2], Ch.Manuja Varma[3], B.Niranjan Naidu[4], D.Kiran Chandu[5], E.Durga Vara Prasad[6]

[1]*Assistant Professor, Department of ECE, Raghu Institute of Technology, Dakamarri, Vizag*

[2,3,4,5,6]*Student, Department of ECE, Raghu Institute of Technology, Dakamarri, Vizag*

Abstract-Data hiding is a technique of hiding recognizable virtual facts into an unrecognizable form, i.e. imperceptible to the human eye. Secret sharing with steganography is a hot topic of debate. As the method is similar to a secret sharing scheme, it tricks the attacker into falling into our trap. He may think that n restores the images to be output and follow his lead, which ends up going in the wrong direction. But to recover the secret image, the output data from level one must pass through level two. In the second level, we used the concept of steganography. The input to the second step is n recovered envelope images and one stego image. The experimental final result shows that the proposed scheme is clearly secured in both ranges, the change with arbitrary n proportions does not reveal any sub-statistics.

Keywords: **Steganography, Stego, Visual Cryptography**

I.INTRODUCTION

Ancient people used various techniques to send secret messages during times of war. Safe and secure massage delivery is a top priority for any organization dealing with confidential data. Information hiding techniques are essential for military, intelligence, internet banking, privacy, etc., so it is currently an area of research. Increased use of the internet, information is available on the internet, a person who has the internet can easily get data from the internet for the information he wants. As more and more information hiding techniques are developed and improved, more and more different information detection techniques are also being developed.[1][3] This created a strong need to create new techniques to protect confidential information from hackers. There are a number of data hiding techniques available for different purposes and applications, such as steganography, cryptography, and watermarking. Steganography means hidden writing. Cryptography means encoding data in such a way that it becomes meaningless to eavesdroppers. Watermarking means embedding a watermark signal into data to create a watermark object . So that it is most used in copyright protection and media authentication. In the method of steganography, confidential data is embedded in such a way that the existence of secret data is invisible. Steganographic approaches are mainly organized into approaches based on spatial domain and frequency domain.[2][5] The Spatial domain techniques operate on a pixel-by-pixel basis, embedding messages directly into the least significant bits (LSBs) of the data [10]. In the frequency domain, the host files are first transformed into the frequency domain, eg by FFT, DCT, or DWT, and then the messages are embedded in some or all of the transformed coefficients. Steganography methods can also be classified based on the cover medium as text, image, video, audio and protocol steganography.

II. DIGITAL STEGANOGRAPHY

In digital steganography, the message is converted into a binary message and hidden in overlapping objects, there are many types of digital steganography; audio characters can be hidden in images or videos, text can be hidden in digital images, it can be text. hidden in audio files etc. The hiding process takes advantage of the sensitivity of human systems, for example, each pixel in grayscale images is represented by 8 bits, which means there are 2^8=256 different color levels, the human visual system normally cannot distinguish between two following colors. this "flaw" can be exploited to hide data in the least significant bit of each pixel. It is likely that in audio files, some of the less important data may be replaced by the data to be

hidden without being able to perceive the noise generated by the hiding process.[3][6]

III. LEAST SIGNIFICANT BIT ALGORITHM

24-bit color images are used in this system. So the shared image is a 24-bit color image and has the same dimension as the secret image. A 24-bit color image has 3 layers namely red, green and blue. First, both the secret and shared images are converted to a binary matrix and divided into red, green, and blue layers. An XOR operation is then performed on each of the corresponding layers between the secret image and the shared image. It is a pixel-by-pixel XOR operation and a new image is created using the resulting matrix called share2. This share2 has the same dimension as the secret and shared image. share2_pixel(p, q) = © [secret_pixel (p, q), sharel_pixel (p, q)].[7][8]

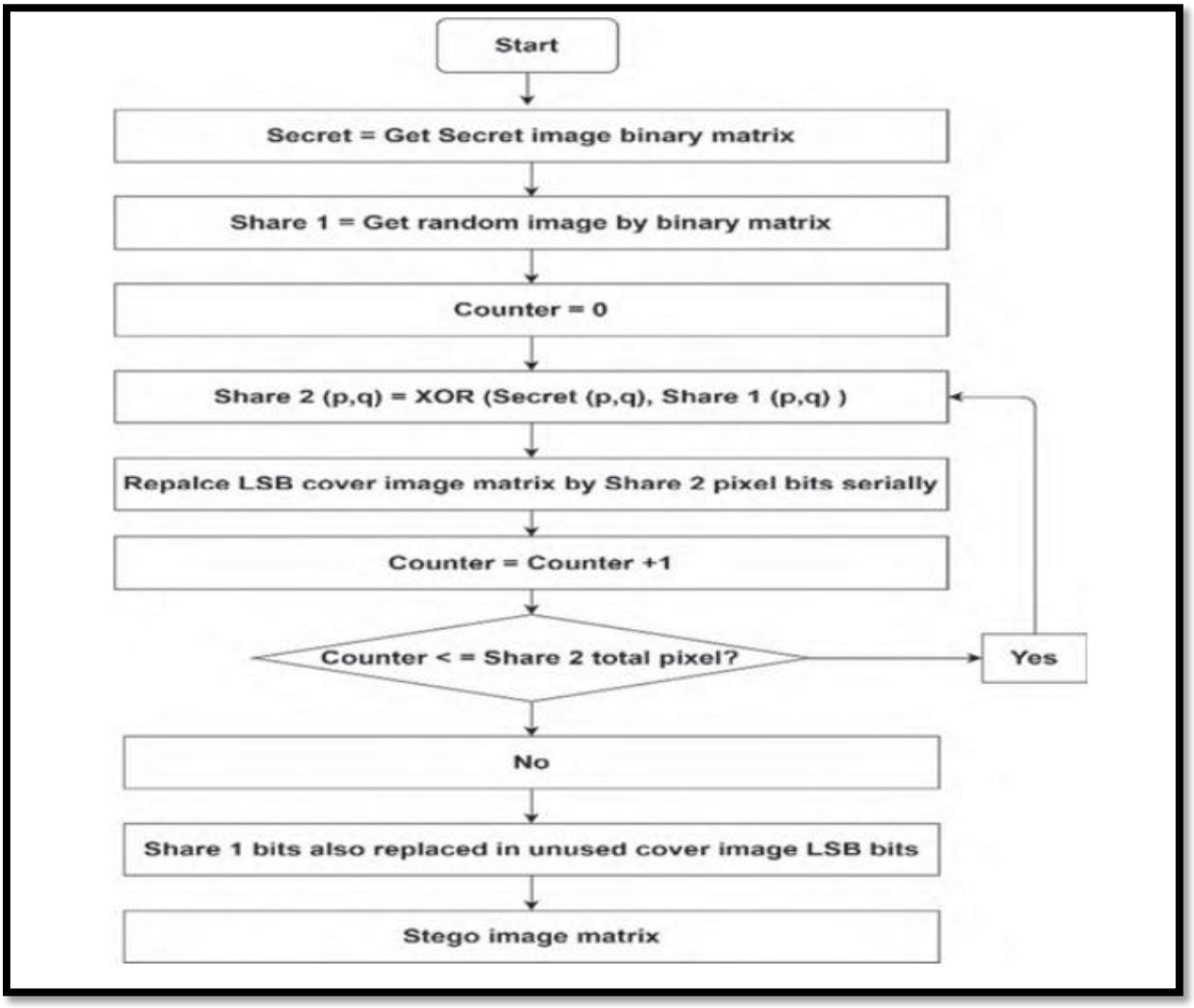

Fig 1: Flowchart of Encoding Technique

From each layer of the stego image, the LSB bits of each pixel are extracted and sequentially inserted into the new image matrix array.[4] For example, the extracted bits from the red layer of the stego image are inserted into the empty image matrix for the red layer of the share2 image. 8 LSB bits are taken from the 1st 8 pixels of the stego image and these bits are inserted into the 1st pixel of the empty matrix. This process continues until the share2 red layer is complete. [9][11]The green and blue layers are generated in the same way. This process is described in the following Fig. 2. After obtaining 3 layers of the share2 image, the share2 image is reconstructed by combining all layers. Now bit by bit XOR operation is applied to each image layer share1 and share2. As a result, the R, G, B layers of the secret image are

generated. By stacking all the layers together, the desired secret image is decoded. The entire search method is demonstrated in the following flowchart.

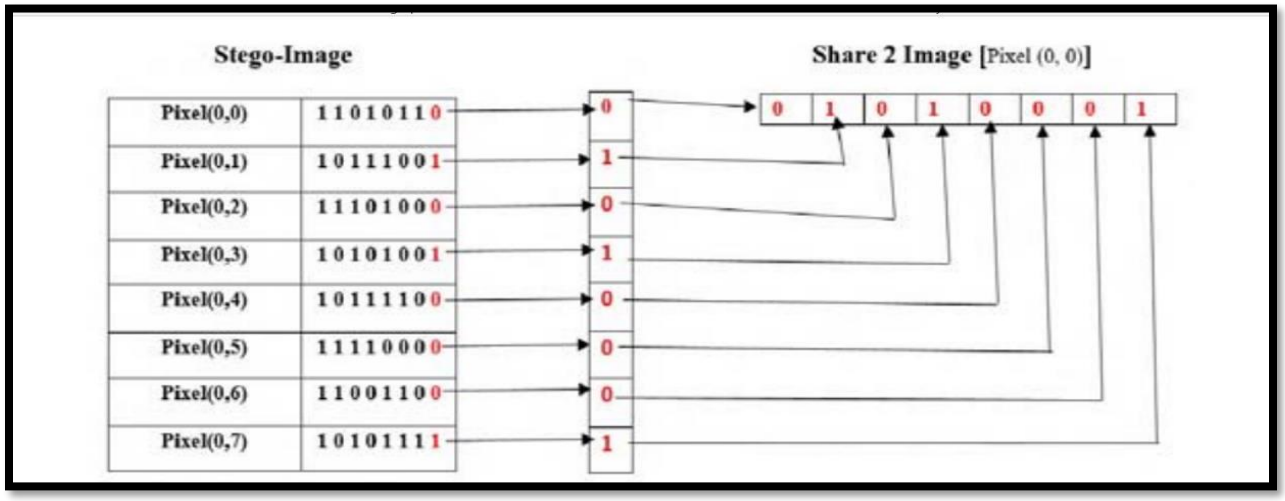

Fig 2: Decoding of 1-Pixel Secret data from 8 -pixels of Stego image

IV. PROPOSED METHOD

In this paper, dual text steganography for secure communication was proposed. Here in dual steganography image steganography is used.

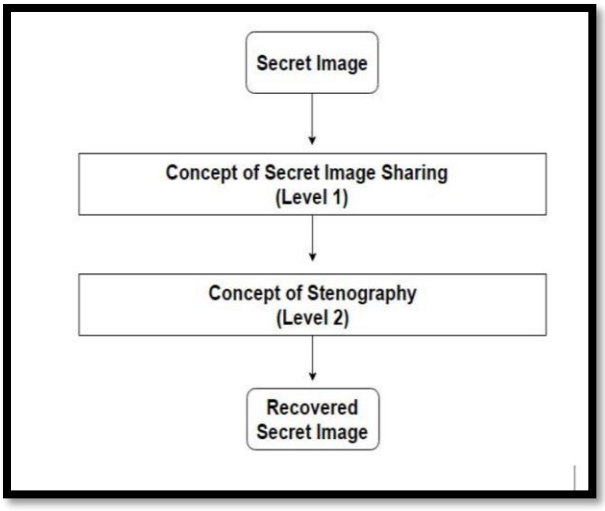

Fig 3:General idea of proposed scheme

New ways are always needed to overcome the shortcomings of the previous ones. A lot of efforts are being made to achieve this goal. Many new schemes came into play, some related to shorthand and some concerned with secret sharing. These schemes are less secure because only one technique is used. This allows an intruder to repeatedly try to reveal the secret by constantly tempering the shared information. The scheme we proposed addresses this problem by using both secret sharing and shorthand. The proposed scheme initially uses the concept of a secret sharing scheme to encrypt a secret image SI with n cover images Ci, i = 1, 2, ⋯ , n, to form n + 1 shared images Sj j = 1, 2, ⋯ , n, n + 1. The same concept is used to decrypt n+1 shared images Sj j = 1, 2, ⋯ , n, n + 1 to obtain n recovered wrapper images Ri i = 1, 2, ⋯ , n and stego image ST. This entire process of encryption and decryption using the concept of secret sharing is denoted under level 1. In level 2, the concept of shorthand is used to obtain the recovered secret image G.

V. ENCRYPTION & DECRYPTION

The Encryption process involves the following

Secret message encoding: The secret message is first converted into a binary format.

Encryption: The binary message is encrypted using a cryptographic algorithm, such as AES (Advanced Encryption Standard), to ensure the security of the message.

Splitting: The encrypted message is then split into two equal parts, each with the same length.

Embedding: The two parts of the encrypted message are then embedded in the cover texts, such that each cover text carries one part of the message.

The Decryption process involves the following

Extraction: The two cover texts are first extracted.

Detection: The existence of a hidden message is detected by comparing the two cover texts, and looking for any

differences or patterns that suggest the presence of hidden information.

Extraction of embedded data: Once the hidden message is detected, the two parts of the encrypted message are extracted from the cover texts.

Decryption: The two parts of the encrypted message are then decrypted using the same cryptographic algorithm used during encryption.

Reassembling: The two decrypted parts are combined to reveal the original secret message

V. RESULTS

This section deals with the experimental result and analysis of the proposed method. The proposed method works effectively on both color and grayscale images. We use 512 × 512 pixel grayscale images for experimentation. For binary images, we need to make some changes in the algorithm, such as removing the multiplication and division operator and updating the modulo value to 2. All experiments are performed on an 8GB RAM, Intel(R) Core (TM) i7- 4710HQ 2.50 GHz processor, machine using MATLAB 13.

Fig 4 : Data Hiding

Fig 5 : Results for recovered cover image

VI. CONCLUSION & FUTURE SCOPE

In this paper, we proposed a new scheme using the concept of secret sharing and shorthand with visual cryptography. The secret sharing concept is used to provide better security and to deceive an attacker by providing pseudo-images. Stenography is used to hide a secret image into a stego image. The proposed scheme used n cover images to provide randomness to n + 1 shared images, so less than n + 1 shares cannot reveal any information about the cover images and the secret image. Stacking less than n recovered envelope images with a stego image will not reveal the secret image. RMSE, PSNR and correlation techniques are used to check the similarity between 1. Secret image and Shared images 2. Stego image and Shared images 3. Stego image

and Recovered images 4. Secret image and combination of Stego image and Recovered images.

The proposed scheme uses a division operator that reduces the pixel size, which makes the proposed scheme not valid for more than 255 images. The Stego image is random, which can ring bells for attackers. In future work, we may use another alternative for the division operator. We can make the stego image more systematic, so it will undoubtedly be on the mind of attackers and easily fooled. The designed image does not accommodate images of different sizes. This can be achieved in the future.

REFERENCE

[1] Shamir, Adi. "How to share a secret." Communications of the ACM 22.11 (1979): 612-613.

[2] Blakley, George Robert. "Cryptographic Key Protection." Why. National Computer Conference 1979 48 (1979): 313-317.

[3] Naor, Moni and Adi Shamir. "Visual Cryptography." Advances in Cryptology EUROCRYPT'94. Springer Berlin/Heidelberg, 1995.

[4] Karim, SM Masud, Md Saifur Rahman and Md Ismail Hossain. "A New Approach for LSB-Based Image Steganography Using a Secret Key." Computer and Information Technology (ICCIT), 2011 14th International Conference on IEEE, 2011.

[5] Anbarasi, L. Jani, and S. Kannan. "Secure Secret Sharing of Color Images with Steganography." Recent Trends in Information Technology (ICRTIT), 2012 International Conference on IEEE, 2012.

[6] Marvel, Lisa M., Charles G. Boncelet, and Charles T. Retter. "Spread Spectrum Steganography." IEEE Transactions on image processing 8.8 (1999): 1075-1083.

[7] Fridrich, Jessica, Miroslav Goljan and Rui Du. "Reliable detection of LSB steganography in color and grayscale images." Proceedings of the 2001 Workshop on Multimedia and Security: New Challenges. ACM, 2001.

[8] Cheddad, Abbas et al. "Digital Image Steganography: A Survey and Analysis of Current Methods." Signal Processing 90.3 (2010): 727-752.

[9] Provos, Niels and Peter Honeyman. "Hide and Seek: An Introduction to Steganography." IEEE Security & Privacy 1.3 (2003): 32-44.

[10] Chen, Tzung-Her and Chang-Sian Wu. "Efficient Multi-Secret Image Sharing Based on Boolean Operations." Signal Processing 91.1 (2011): 90-97.

[11] Johnson, Neil F. and Sushil Jajodia. "Exploring Steganography: Seeing the Invisible." Computer 31.2 (1998): 26-34.

[12] Blundo, Carlo, Alfredo De Santis, and Moni Naor. "Visual cryptography for grayscale images." Information Processing Letters 75.6 (2000): 255-259.

[13] Kuwakado, Hidenori, and Hatsukazu Tanaka. "Image Size Invariant Visual Cryptography." IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science 82.10 (1999): 2172-2177.

[14] Iwamoto, Mitsugu, and Hirosuke Yamamoto. "An optimal n-out-of-n visual secret sharing scheme for grayscale images." IEEE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 85.10 (2002): 2238-2247.