Analysis of Secret Image Sharing using Shared Image

I. Edwin Dayanand
Research scholar, Manonmaniam Sundaranar University, Tirunelveli, India

R.K. Selva Kumar, Ph.D.
Professor, Agni College of Technology, Chennai, India

ABSTRACT
A secret image sharing scheme with steganography lacks to provide the authentication, quality of stego-image and more cheating done by the dishonest participants. So, a secret image sharing using shared image technique is proposed to prevent the participants from the subsidiary stipulation of a false stego-image (an image containing the hidden secret image). A secret image is first processed into n shares which are then hidden in n user-selected suppression images. It is recommended to select these suppression images to contain well-known stuffing to increase the steganographic effect for the security protection.

Additionally, an image watermarking technique is engaged to embed fragile watermark signals into the suppression images by the use of parity-bit checking, thus providing the ability of authenticating the reliability of each processed suppression image. During the secret image recovery process, each stego-image carry by a participant is first verified for its reliability by checking the uniformity of the parity conditions found in the image pixels. This facilitates to avert the participant from subsidiary stipulation of a false stego-image.

Some effective techniques for handling large images as well as for enhancing security protection are employed. As a result, the secret image sharing using shared image scheme offers a high secure and effective mechanism for secret image sharing that is not found in existing secret image sharing methods. High-class experimental results proving the authentication capability, secret hiding effectiveness and quality of the proposed approach are included.

Keywords
Secret image sharing, Steganography, Authentication, suppression image, Data hiding, Stego-image, Fragile watermarking.

1. INTRODUCTION
Due to fast growth of Internet applications, digitized data becomes additionally popular. Since the effortlessness of digital duplication and tinkering, data security becomes a significant concern nowadays. In persuaded application cases, it is jeopardy if a set of secret data is held by only one person with no extra copies since the secret data set may be lost incidentally or customized deliberately. In some other cases, it strength be necessary for a group of persons to share a certain set of secret data. Threshold secret sharing is intended to encode a secret data set into n shares and deal out them to n participants, where any k or more of the shares can be collected to recover the secret data.

However, the resulting methods are suitable only for a few types of digital data, such as text files, passwords, encryption/decryption keys, etc. Because of the radical expansion of network bandwidths, data flow on networks nowadays includes lengthily all types of multimedia, including image, audio, video, etc. In exacting, how to divide a top secret image has attracted wide attention in recent years because of the popular uses of images in network applications.

The Steganography is concept of hiding the information by entrench messages within other, apparently harmless messages. Steganography works by restore bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML) with bits of different, invisible information. This hidden information can be a plain text, cipher text, or even images. Steganography is a kind of data hiding technique that make available another way of security protection for digital image data.

Unlike utilizing a particular cipher algorithm to protect secret data from illicit access, the purpose of steganography is to embed secret data in reselected meaningful images, called conceal images, without creating visually detectable changes to keep an attacker unaware of the survival of the secret. This augments the security protection effect. It necessitates the use of data hiding techniques in the secret sharing process.

Steganography sometimes used when encryption is not allowable. Or, more usually, steganography is used to addition encryption. An encrypted file may still hide information using steganography, so still if the encrypted file is interpret; the hidden communication is not seen. This scheme supplies an easy and fast decryption process that consists of xeroxing the shares onto transparencies and then stacking them to reveal the shared image for visual inspection. The scheme differs from the traditional secret distribution, which does not need difficult cryptographic mechanisms and computation. Instead, it can be make out directly by the individual illustration system. However, the system is suitable for binary images only and the generated noisy share may be distrustful to aggressor.

The advantage of steganography, over cryptography alone, is that messages do not attract concentration to themselves. Plainly noticeable encrypted messages—no matter how indestructible—will stimulate suspicion. Therefore, whereas cryptography guards the contents of a message, steganography is said to protect both messages and communicating parties.

A delicate watermark is a kind of signal, which is designed to be embedded in an image and can be without problems destroyed if the watermarked image is influence in the smallest amount. By scrutinize the continuation of the embedded signal in an inspected image; the aim of authentication is achieved. A technique of fragile image watermarking is accepted for image authentication during the secret sharing process.

2. LITERATURE REVIEW
Secret image is protected by applying threshold scheme. This scheme first divides the pixels in a four pixel block into two groups [1]. The first group contains the pixels whose one bit is used to embed authentication data and the second group consists of the other pixels. Single bit of each pixel in the

second group is customized to decrease the degradation causing from embedding the sharing information. Transform the covert pixels into the m-ary notational system [2]. The information data used to reconstruct original pixels from secret pixels are calculated. Stego-images with good quality and high authentication capability is obtained from the experimental results.

The essence of invertible image sharing approaches is that the revealed content of the secret image must be lossless and the distorted stego-images must be able to be reverted to the original cover image [3]. It achieves the transformation by m-ary notational system and share these transformation by (t,n) threshold scheme. This scheme allows embedding secret data in large capacity. The secret data embedding in a smooth region provides poor visual quality and lower security. To overcome this issue [4], introduces an edge adaptive scheme using the Least-Significant-Bit (LSB) approach by embedding the data in the sharpen edge regions. It increases the embedding rate, provides fault tolerance and trust to group policy during transmission of secret images over networks [7].

The secret data can be in the form of the secret color image. These images are generated with the help of reversible polynomial function and the contributor mathematical key. The secret image and the cover image is embedded together to construct a stego-image [5]. Quantization process applied to improve the quality of cover image and secret and cover are reconstructed without loss. Gradual search algorithm for a single bitmap BTC (GSBTC) and threshold concept generates smaller shadows in the secret color image sharing scheme [9]. It prevents the leakage information and reduces the shadow size successfully.

An image sharing method applied to the integer single or multiple Wavelet transform [10] and threshold scheme for highly compact and easily manageable shadows. Secret Image Embedded Authentication of Song Signal through Wavelet Transform helps to secure the image by embedding its coefficient without changing its audible quality [11]. The embedded hidden secure image as well as authenticating code is used to detect and identify the original content from similar available content. Secret Image identification is done losslessly by reversible color transformation [12]. It handles huge data volume and provides feasibility.

Iteratively searches proper modifications of pixels to enhance a base steganographic scheme with optimized picture quality and higher anti-steganalysis capability using closed-loop computing framework. To achieve this goal, an anti-steganalysis tester and an embedding controller-based on the simulated annealing (SA) algorithm [6] with a proper cost function-are incorporated into the processing loop to conduct the junction of investigation. It shows the improved performance and file-size variation.

Wavelet-domain statistical quantity histogram shifting and clustering (WSQH-SC) constructs new watermark embedding and extraction procedures by histogram shifting and clustering, which are vital for humanizing sturdiness and reducing run-time complexity [8]. Experiments are performed over a natural, medical and synthetic aperture radar images to show the effectiveness of WSQH-SC.

3. METHODOLOGIES

The different work involved in "Secret Image Sharing using shared image" is:

3.1 A Color Secret Image Sharing Scheme using Shadow Images

Secret image sharing technique is an attempt to avoid secret images from snooping in addition to traditional cryptography. A Gradual search algorithm for a Single bitmap BTC (GSBTC) and threshold notion is combined to speed up the transmission of a secret color image in a secret image sharing scheme using shadow images. It productively reduces shadow size and that each shadow behaves as a random-like image that averts leakage of information about the secret color image.

Furthermore, the correlation between two vertically or horizontally adjacent pixels in each shadow is considerably less than those in a color secret image. Security is established in a proposed scheme and one-pixel difference could cause a considerable difference in the corresponding shadows.

3.2 Secret-Fragment-Visible Mosaic Images by Nearly - Reversible Color Transformation

A new image steganography technique produces mechanically from an arbitrarily-selected target image called secret-fragment-visible mosaic image as conceal of a given secret image. The mosaic image is surrender by dividing the secret image into fragments and transforming their color characteristics to be those of the blocks of the intention image. Skilled techniques are designed for use in the color transformation process so that the secret image may be enhanced almost losslessly. The scheme not only produce a steganographic effect helpful for safe keeping of secret images, but also supplies a new way to resolve the difficulty of hiding secret images with huge data volumes into target images.

3.3 Visual Cryptography by Image Filtering and Resizing

In visual cryptographic scheme (VCS), each secret pixel is prolonged to m sub pixels in shadow images to encrypt a secret image. In fact, it put these m sub pixels as a rectangle such that the blocks can be agreed efficiently with each other. Though, if the aspect ratio is outlook as important information of the secret image, the distortion take place at the case that m is not a square. An aspect ratio invariant VCS (ARIVCS) is according to address the arrangement of sub pixels.

Furthermore, the dummy pixels are condensed and an easy solution for the image filtering and resizing.

3.4 Robust Reversible Watermarking via Clustering and Enhanced Pixel-Wise Masking

Robust Reversible Watermarking (RRW) methods are accepted in multimedia for defensive patent, while conserve intactness of host images and on condition that robustness against accidental attacks. Conventional RRW methods are not willingly applicable in practice. It is mainly because: 1) they fail to offer satisfactory reversibility on large-scale image datasets; 2) they have incomplete robustness in extracting watermarks from the watermarked images shattered by different unintentional attacks; and 3) some of them suffer from extremely poor invisibility for watermarked images.

Therefore, it is essential to have a framework to address these three problems, and supplementary improve its performance. To conquer this obstacle, the Wavelet-domain Statistical

Quantity Histogram Shifting and Clustering (WSQH-SC) is developed. WSQH-SC ingeniously constructs new watermark embedding and extraction measures by histogram shifting and clustering, which are important for civilizing robustness and reducing run-time complication. In addition, WSQH-SC contains the property-inspired pixel alteration to professionally knob overflow and underflow of pixels. This outcome is acceptable reversibility and invisibility.

Moreover, to increase its practical applicability, WSQH-SC designs an improved pixel-wise masking to balance robustness and invisibility.

3.5 Reversible Data Hiding Scheme via Optimal Codes for Binary Covers

In Reversible Data Hiding (RDH), the unique cover can be lossless re-establish after the embedded information is extracted. A rate-distortion model for RDH, in which they confirm out the rate-distortion bound and proposed a recursive code construction. The generalized method using a decompression algorithm as the coding scheme for embedding data and establish that the generalized codes can reach the rate-distortion bound as long as the compression algorithm reaches entropy. The proposed binary codes perk up three RDH schemes such as binary feature sequence as covers, second scheme for JPEG images and a pattern substitution scheme for binary images.

The novel codes can considerably reduce the embedding distortion. In addition, by modifying the histogram shift (HS) manner, coding method practical to one scheme that uses HS, showing that the proposed codes can be also subjugated to recover integer-operation-based schemes.

3.6 Sharing Secret Images using Integer Single or Multiple Wavelet Transform

Integer single and multiple wavelet transform is originate widely in image and video applications where its scaling functions afford higher energy compaction in smooth sub band. It merge the image sharing method relating the integer single or multiple wavelet transform and threshold scheme that offer highly compact and effortlessly manageable shadows for real time progressive transmission.

3.7 Secret Image Embedded Authentication through Wavelet Transform

Security provide for the digital songs through wavelet transform with the help of a protected image embedded with coefficients of it with no altering the audible quality. Sampling the hidden image with the help of amplitude coding for generating lower magnitude values is the first phase of technique go behind by fabrication of authenticating code by inserting into lower magnitude values with selected coefficients of song signal generated via wavelet transform. The embedded hidden sheltered image as well as authenticating code is used to detect and identify the original content from similar available content.

4. PERFORMANCE RESULT

General experimental studies are conducted to inspect the proposed Secret Image Sharing using shared image (SSIS) with Steganography. The performance result of the proposed SSIS technique for prevents the participants from the subsidiary stipulation of a false stego-image. It is measured in terms of

i) Feasibility Level

ii) Data hiding Effectiveness

iii) Authentication Capability

iv) Stero-Image Quality

4.1 Feasibility Level

Experimental results are shown to prove the feasibility level of the proposed scheme.

Table 4.1 No. of pixels Vs Feasibility Level

No. of pixels	Feasibility level (%)			
	Proposed (SSIS) system	Enhanced pixel wise masking	Through optimal code	Reversible Color Transform
10	85	80	50	60
50	87	75	40	65
100	90	73	30	50
150	91	70	28	45
200	95	60	15	52

The above table (Table 4.1) described the feasibility level of proposed method with the various existing system. The feasibility level of the secret Image sharing using shared Image (SSIS) technique is compared with an existing enhanced pixel wise masking, through optimal code, Reversible color transform.

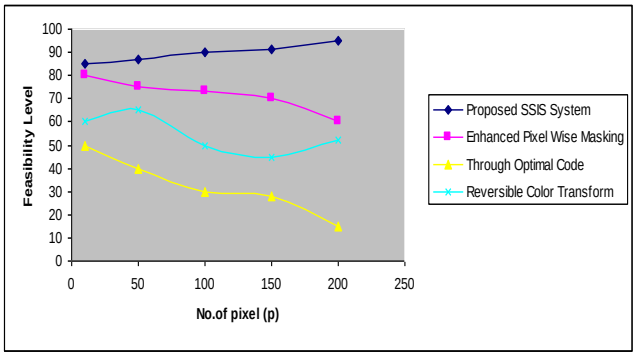

Fig 4.1 No. of pixels Vs Feasibility Level

Fig 4.1, described the Feasibility level of pixels in Steganography. In the proposed SSIS technique the variance in the feasibility level would be 20-25% high in the proposed technique.

4.2 Secret Data Hiding Effectiveness

Table 4.2 Data Hiding Effectiveness

Methods	Effectiveness (%)
Proposed Secret image sharing using shared Image (SSIS)	95
Secret image embedded through wavelet transform	70
Data Hiding Scheme through optimal code	65
Secret-Fragment-Visible Mosaic Images by Nearly-Reversible Color Transformation (NRCT)	50

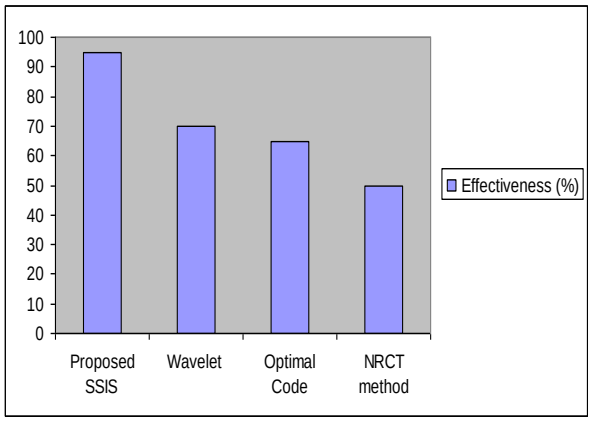

Fig 4.2 Data Hiding Effectiveness

Fig 4.2, described the Secret data hiding effectiveness in the proposed Secret Image Sharing using shared Image (SSIS) technique. The images are hidden very effectively in the stego-image using steganography concept. The proposed method attains the 95 % effectiveness.

4.3 Authentication Capability

Table 4.3 No. of pixels Vs Authentication Capability

No. of pixels (p)	Authentication Capability (%)			
	Proposed (SSIS) system	Through optimal code	Secret Color Image sharing	Through Wavelet Transform
10	95	70	60	45
50	97	65	62	46
100	94	67	63	50
150	96	68	61	35
200	93	72	54	42

Table 4.3 illustrates the authentication capability of the proposed technique. Comparison result of the proposed with an existing method in steganography is measured.When number of pixel increases the authenication capability also increases drastically.

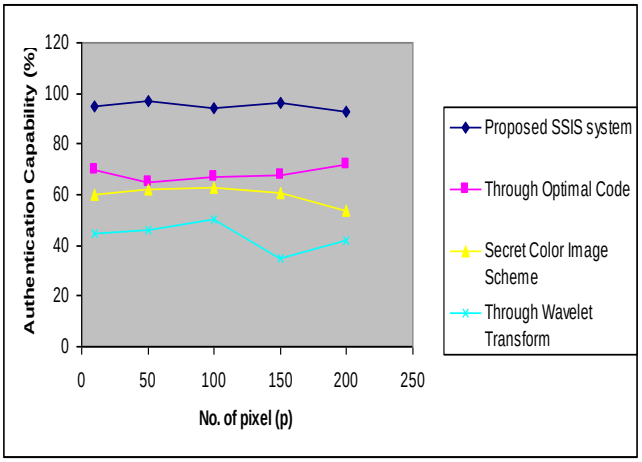

Fig 4.3 No. of pixels Vs Authentication Capability

4.4 Stego-Image Quality

Table 4.4 Image Size Vs Quality

Image Size	Quality (%)			
	Proposed (SSIS) system	Secret Color Image sharing	Reversible Color Transform	Enhanced pixel wise masking
Original Size	98	78	85	50
Four times larger than original size	98	48	53	35

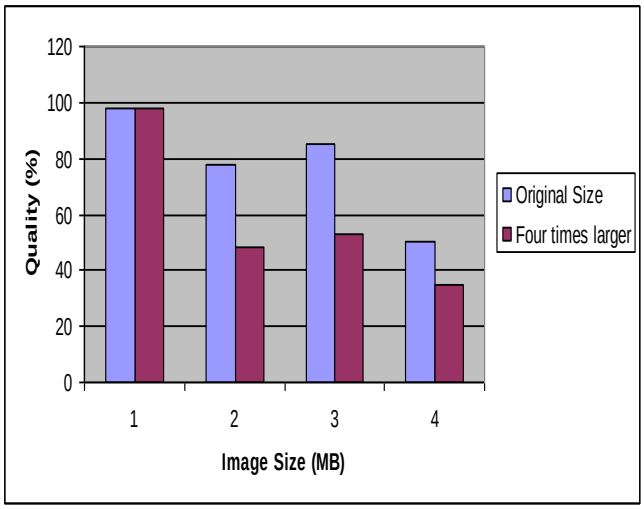

Fig 4.4 Image Size Vs Quality

Fig 4.4, described the quality level of the image even when it image is four times larger than the original size. The proposed SSIS technique produces same quality whereas the various existing system outfits lesser quality. The Size is measured in Mega Bytes. The higher the quality produces the better outcome.

5. CONCLUSION

In this paper a secret image sharing using shared image with steganography is proposed. The main objective is to avoid the participants from cheating. More in detail, the paper build the following contributions. First, it illustrate that the authentication can be really enhanced by hashing the pixel block. The proposed scheme is outfitted with the capability of authentication, which can sense false participants' shares before the recovery process is executed. At this time, even the dishonest participant could not influence the fake stego-image from his own stego-image.

Second, it takes into account the improvement of both the qualities for stego-images and secret image. Even the development of the suppression image size to four times that of the secret image, the quality of stego image does not vary. Moreover, the proposed scheme can also handle full color images, and the quality of the recovery result is nearly lossless. This system is thus suitable for the applications where high security and efficiency is required.

6. REFERENCES

[1] Chi-Shiang Chan., Ping-En Sung., "Secret Image Sharing with Steganography and Authentication Using Dynamic Programming Strategy," International Conference on Pervasive Computing Signal Processing and Applications, 2010.

[2] Chin-Chen Chang., Pei-Yu Lin., Chi-Shiang Chan., "Secret Image Sharing with Reversible Steganography," International Conference on Computational Intelligence and Natural Computing, 2009.

[3] Pei-Yu Lin., Chi-Shiang Chan., "Invertible secret image sharing with steganography," Elsevier Science Inc, Volume 31 Issue 13, 2010.

[4] Weiqi Luo., Fangjun Huang., Jiwu Huang., "Edge Adaptive Image Steganography Based on LSB Matching Revisited," IEEE Transactions on Information Forensics and Security, Volume: 5, Issue: 2, 2010.

[5] Anbarasi, L.J., Kannan, S., "Secured secret color image sharing with steganography," International Conference on Recent Trends in Information Technology, 2012.

[6] Guo-Shiang Lin., Yi-Ting Chang., Wen-Nung Lie.," A Framework of Enhancing Image Steganography With Picture Quality Optimization and Anti-Steganalysis Based on Simulated Annealing Algorithm," IEEE Transactions on Multimedia, Volume:12, Issue:5, 2010.

[7] Ulutas, G.,Ulutas, M., Nabiyev, V.V., "A new casccaded secret image sharing scheme," IEEE Conference on Signal Processing and Communications Applications, 2012.

[8] An, L., Gao, X., Li, X., Tao, D., Deng, C., Li, J., "Robust Reversible Watermarking via Clustering and Enhanced Pixel-Wise Masking," IEEE Transactions on Image Processing, Volume :21, Issue: 8, 2012.

[9] Chin-Chen Chang., Chia-Chen Lin., Chia-Hsuan Lin., Yi-Hui Chen., "A novel secret image sharing scheme in color images using small shadow images," Elsevier Science Inc., Volume:178, Issue:11, 2008.

[10] Chin-Pan Huang., "Sharing secret images using integer single or multiple wavelets transform," Journal of Communications Technology and Electronics, Volume: 56, Issue: 1, pp 43-51, 2011.

[11] Uttam Kr. Mondal., Jyotsna Kumar Mandal.," Secret Image Embedded Authentication of Song Signal through Wavelet Transform (IAWT)," IEEE Transaction on Advances in Computing and Information Technology, Volume: 176, pp 199-208, 2012.

[12] Ya-Lin Li.,Wen-Hsiang Tsai," New Image Steganography via Secret-Fragment-Visible Mosaic Images by Nearly-Reversible Color Transformation," IEEE transaction on Advances in Visual Computing, Volume: 6939, 2011.