A NEOTERIC COLOR IMAGE SHARING BASED ON COMPRESSED SENSING

(G.Lakshmikala)[1], (S.Fayaz Basha)[2]
[1](M.TECH STUDENT, DEPT OF ECE, BHARATH COLLEGE OF ENGINEERING AND TECHNOLOGY FOR WOMEN, KADAPA)

[2](ASSISTANT PROFESSOR, DEPT OF ECE, BHARATH COLLEGE OF ENGINEERING AND TECHNOLOGY FOR WOMEN, KADAPA)

ABSTRACT

Secret image sharing has been attracting considerable research attention in recent years as images become ubiquitous on the Internet and mobile applications. The rising need of secret image sharing with high security has led to much advancement in lucrative exchange of important images which contain vital and confidential information. The purpose of secret sharing methods is to reinforce the cryptographic approach from different points of failure as a single information-container. Conventional methods based on compressed sensing has some limitations. An image is taken as input then DWT and SVD are applied to the input image. Again a message image is taken and the methods, DWT and SVD are applied such that we will get a converted image. Image sharing is don furtherly. Inverse DWT is applied to the obtained image and finally a secter image is obtained.The proposed method based on DWT and SVD shows better results when compared to other state-of-art methods.

Keywords: Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), Secret Image Sharing etc.

I. INTRODUCTION

Because of the fast growth of internet technology development, our daily lives cannot be separated from the internet. We can get lots of information we want by powerful search engine, share the articles or photos in blogs, and contact friends by social network. Therefore, information security becomes more and more important nowadays. If we do not process or hide our secret information, the information might be stolen by the hackers easily. The image hiding and watermarking are techniques that can increase the security of the secret information. However, there is a drawback that the information is kept in a single information-carrier. If the information-carrier is lost or destroyed by an attacker, the secret information might disappear. Thus motivated, the secret sharing method might be the better technique that not only increases the security but also has an extremely high opportunity of recovering the secret information completely. It aims to distribute the secret information to several shadow information holders, and we can completely recover the desired information by collecting an enough number of multiple carriers. That is, we can recover the secret based on only some portion of shadow information.

To safeguard cryptographic keys, Shamir and Blakley presented a novel method for constructing secure and robust key management schemes, called secret sharing (SS), which can overcome many vulnerabilities when one possesses a single master key for a certain cryptosystem.

From a cryptographic perspective, SS scheme refers to some methods for distributing a secret among a group of participants and each one in the group is allocated a share or shadow of the secret. The secret can be reconstructed only when a sufficient number of shadows are combined together and individual shadow serves no useful purpose for obtaining it. As a secure and fault-tolerant technique, SS has been widely used in many fields, such as distributed storage system, secure multiparty computation, and electronic voting. In Shamir's $(k, n)(2 \leq k \leq n)$ threshold SS scheme, the secret is divided into n shadows and any k of them can reconstruct the whole original secret. However, any less than k shadows cannot obtain any information about the secret. Although this construction method is information theoretically secure, each participant requires relatively large storage space because the size of each shadow is equal to that of the secret data. Therefore, using Shamir's SS scheme will result in huge communication burden when we share image or video data at the pixel level. In fact, the topic of designing SS scheme for image data has attracted wide attention in the past fifteen years.

The secret sharing scheme was first proposed by Shamir and Blakley in late 1980s. It is also called (k, n) threshold scheme which should meet the following three requirements, where a secret is represented by a positive integer S. (1) The secret value S is used to generate n shadows (positive integers): D1, D2, … , Dn. (2) Any k or more shadows can be used to reconstruct the secret value S. (3) Any k-1 shadows or fewer cannot get sufficient information to reveal the secret value S. Some (k, n) threshold schemes proposed by Shamir, Blakley, and Asmuth, which are applied for image sharing can be found in, respectively.

II. RELATED WORK

Compressive Sensing (CS) has been proposed more than a decade ago as a method for dimensionality reduction of signals which are known to be sparse or compressible in a specific basis representation. By "sparse" we mean that only a relatively small number of the coefficients of the representation are non-zero, whereas "compressible" indicates that the magnitude of the coefficients decays quickly, according to a power law, hence the signal can be well approximated by a sparse signal. In the CS paradigm, the signal is projected onto a low-dimension space, resulting in a measurements vector. If the signal is sparse, it is possible to exactly reconstruct it from the measurements vector.

A compression scheme based on CS enjoys the following unique properties which are primarily different from those of any conventional signal compression scheme.

• The encoder is of much lower complexity than the decoder. In fact, a significant part of the encoder processing, namely the measurements generation, can be done in the analog domain, e.g. by a single-pixel camera or a lensless camera.

• The decoder is not fully defined by the encoder. Different reconstruction algorithms can be applied to the same measurements vector at different situations, and as more prior information becomes available the reconstruction algorithm can be improved to take it into account.

• The loss of a small fraction of the measurements generally results in only a minor degradation in reconstruction quality. This may be used to achieve robustness to channel impairments without the usual overhead of error protection.

According to theory of CS, if the signal can be represented by a small number of non-zero coefficients, it can be converted into a limited number of incoherent random measurements by constructing a suitable measurement matrix. These random measurements maintain the information of the reconstructed signal, so the original signal can be accurately reconstructed from a

small number of measurements by solving the sparse optimization problem.

Assume that a real-valued signal, x $\in R^N$, is a k-sparse vector on an orthonormal basis $\Psi \in R^{N\times N}$, i.e., only k(k $\ll$ N) out of the N elements of x have non-zero values. Then

$$x = \psi\theta \qquad (1)$$

where the coefficient θ can be well approximated by k non-zero values. So, a small number of linear random measurements y $\in R^m$, k < m $\ll$ N obtained as

$$y = \phi x \qquad (2)$$

where $\Phi \in R^{m\times N}$ is a measurement matrix that is incoherent with Ψ and satisfies the restricted isometric property (RIP).

Then, according to the given y, we can reconstruct signal x by solving the following optimization problem.

$$\min_{\theta} \|\theta\|_1 s.t. \quad y = \phi\psi\theta = \phi x \qquad (3)$$

III.METHODOLOGY

Input Image

An image is taken as input in this stage for further processing.

Discrete Wavelet Transform (DWT)

Discrete wavelet transform is being used widely in 1D and 2D signal processing due to its advantages in signal and image processing applications like compression, de-noising, texture analysis and etc. Later on, its usage is carried into high pass filter and together can be termed as filter banks. In this work, Haar Wavelets are selected due to its simplicity in-terms of operations and it decomposes the signal into four sub band signals. Hungarian mathematician Alfred Haar introduced the Haar wavelets, which is similar to step function. Original signal can be computed by inverse operation of the decomposition filter and is symmetry of the decomposition filter. Instead of down sampling where up-sampling will be used on the given four sub band inputs. All though DWT is old transform domain, still it has been being used in image or video watermarking due to its advantages

DWT gives the relation between time and frequency domain of signal. Applying DWT to an image gives four different bands among which three are high frequency bands and one is low frequency band. Most of the information is carried by low frequency band. so any operation/ processing on image is carried by taking the low frequency band.

Two Dimensional Wavelet Transform

In two dimensions Wavelet transformation, the wavelet representation can be computed with a pyramidal algorithm. The two-dimensional wavelet transform that we describe can be seen as a one dimensional wavelet transform along the x and y axes. Mathematically the wavelet transform is convolution operation, which is equivalent to pass the pixel values of an image through a lowpass and highpass filters.

Singular Value Decomposition (SVD)

Singular value decomposition (SVD) is generally used for decomposing the image into sub matrices for removing redundant data in compression applications and also used for watermarking. As name suggests the Decomposition results in three matrices and they are left, right singular vector matrix and diagonal matrix. The diagonal Matrix consists of singular values along its

diagonal in decreasing order, where singular value represents the energy of the given signal. These singular values plays an important role in compression and as well as watermarking. One peculiar property of the singular values is small perturbation over signal, these values are not effected much and vice versa. Hence, these are used for watermarking

SVD is compression technique, SVD of an image gives three matrices among these two matrices are ortho-normal matrices and one matrix is diagonal matrix. Diagonal elements are called as singular values. The equation for SVD is as

$$X = P \sum Q^T$$

Not all the singular values are used to reconstruct the original information; few singular values are reconstruct the information, there by compression is achieved.

Image sharing

The secret image sharing is a technique based on secret message sharing. Each pixel value of a secret image is a secret message. We use the secret image to generate shadow images and only require part of these shadow images to reconstruct the secret image. The shadow images should not reveal any information about the image itself such as silhouette and smooth regions. Ideally, each shadow image should look like random noise so that anyone without the permission won't be able to get any information about a secret image.

Inverse DWT (IDWT)

In inverse DWT (IDWT) step we are applying inverse DWT to the output image obtained after merging the K shares.

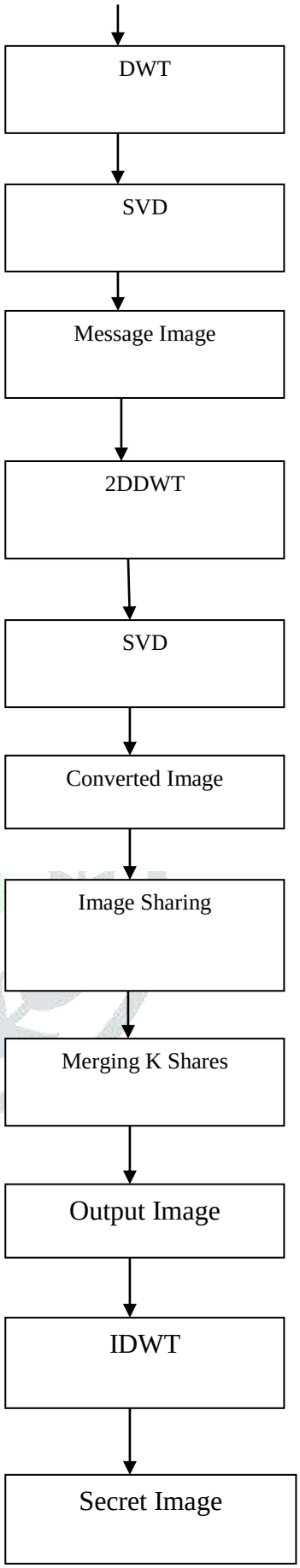

Figure 1 : Block Diagram of Proposed Method

IV. RESULTS

Figure 1: Input Image

Figure 2: Message Image

Figure 3: Restored Image

Figure 4: Converted Image

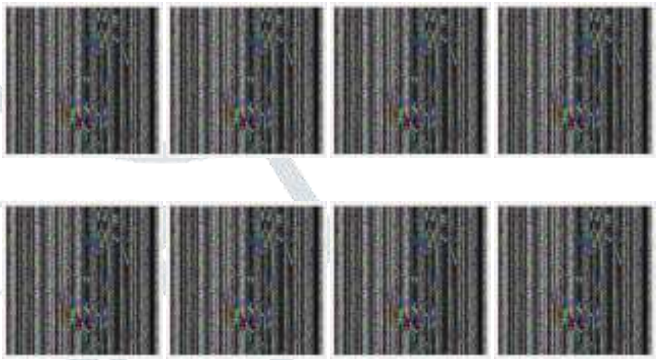

Figure 5: Generation of eight Shares

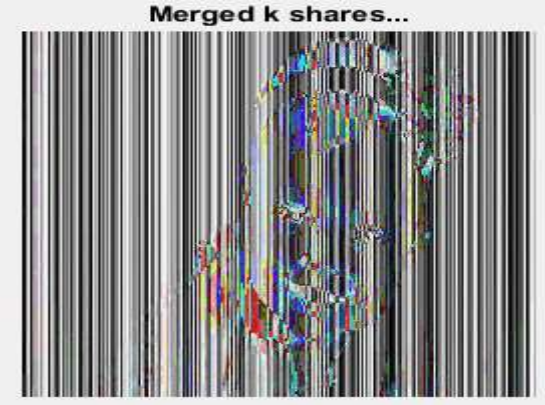

Figure 6: Merged K Shares

Figure 7: output Image

Figure 8: Retrieved secret image

V. CONCLUSION

This paper reviews and implements three secret image sharing algorithms. By applying the existing schemes directly on a secret image, the silhouette and smooth regions of an image may appear in a shadow image.In the proposed scheme, it was extended to secret image sharing scheme with DWT and SVD concept. The experimental results and security analysis indicate the potential superiority of our scheme. The performance is measured using metrics which says that our proposed scheme is better compared to other state-of-art methods.

VI.REFERENCES

[1] Shamir A. How to share a secret [J].Communication of the Association for Computing Machinery, 1979,22(11):612-613.

[2] Blakley G R. Safeguarding cryptography keys[C] Proceeding of AFIPS 1979 National Computer Conference, New York, 1979:313-317.327

[3] Emmanuel Candes. Compressive sampling [A]. In: Proceedings of the International Congress of Mathematicians[C]. Madrid, Spain, 2006, 3, 1433-1452.

[4] Emmanuel Candes, Justin Romberg, Terence Tao. Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information [J]. IEEE Transaction on Information Theory, 2006, 52(2):489-509.

[5] David L.Donoho, Compressed sensing[J]. IEEE Transaction on Information Theory, 2006, 52(4):1289-1306.

[6] Thien CC, Lin JC. An image-sharing method with user-friendly shadow images. IEEE Transactions on Circuits and Systems for Video Technology 2003; 13(12): 1161 -1169.

[7] Lin CC, Tsai WHo Secret image sharing with steganography and authentication. Journal of Systems and Software 2004; 73(3):405-414.

[8] Yang CN, Chen TS, Yu KH, Wang Cc. Improvements of image sharing with steganography and authentication. Journal of Systems and Software 2007; 80(7): I 070-1 076.

[9] Lin PY, Lee JS, Chang Cc. Distortion-free secret image sharing mechanism using modulus operator. Pattern Recognition 2009;42(5):886-895.