Robust Watermarking of Compressed and Encrypted JPEG 2000 Images

M.Veni[*1] , Dr.P.Eswaran[#2],

Department of Computer Science & Engineering
Alagappa University, Karaikudi, INDIA.

***Abstract*— In this paper we present a secure patient medical images and authentication scheme which enhances the security, confidentiality and integrity of medical images transmitted through the Internet. The medical images are secured using the digital image watermarking scheme. If any attacker try to access the secret medical images, that connection is immediately rejected. The proposed approach is used to provide the robustness against the wide variety of attacks and the visible quality of the reconstructed secret image is too clear as the original image.**

***Keywords*— Digital Image Watermarking, Watermark insertion, Compressed and Encrypted, JPEG 2000, DWT.**

I. INTRODUCTION

A. Image Processing

Image Processing is a technique to enhance raw images received from cameras/sensors placed on satellites, space probes and aircrafts or pictures taken in normal day-to-day life for various applications [14].

An image may be defined as a two-dimensional function, f (x, y), where x and y are spatial (plane) coordinates, and the amplitude of f at any pair of coordinates (x, y) is called the intensity or gray level of the image at that point. When x, y and the amplitude values of f are all finite, discrete quantities, we call the image a digital image. The field of digital image processing refers to processing digital images by means of a digital computer. These elements are referred to as picture elements, image elements, pels and pixels. Pixel is the term most widely used to denote the elements of a digital image [13].

B.Digital Watermarking

Digital watermarking is defined as the process of embedding data (watermark) into a multimedia object to protect the owner's right to that object.
Digital watermarks have three major application areas: data monitoring, copyright protection and data authentication. There are several types of watermarking schemes categorized based on their inputs and outputs [4]. Private watermarking and semi-private watermarking. Public watermarking is the most challenging scheme, as it requires neither the source image nor the watermark. These systems extract exactly a set of bits of information (namely the watermark) from the watermarked image. These schemes are also called blind watermarking. [8]

A steganographic system is typically not required to be robust against intentional removal of the hidden message. On the other hand, the watermarking requires that the hidden message should be robust to attempts aimed at removing it [8].

The main advantages of the watermarks over other techniques are:

- They are imperceptible.
- They are not removed when the data are converted to other file formats.
- They undergo the same transformations as the data in which they are embedded [8].

The up to date known watermarking applications considered in the open literature are as follows:

- Copyright Protection
- Fingerprinting
- Copy protection
- Broadcast monitoring
- Data authentication
- Indexing
- Medical safety
- Data Hiding [8].

C. Applications of Image Processing

Digital image processing is used in some applications are:

- Gamma-Ray Imaging

- X-ray Imaging
- Imaging in Ultraviolet Band [13].

D. Image Compression

Image compression addresses the problem of reducing the amount of data required to represent a digital image. The reduction process is the removal of redundant data.

Furthermore, image compression plays a major role in many important and diverse applications, including televideo conferencing, remote sensing, document and medical imaging, facsimile transmission (FAX), and the control of remotely piloted vehicles in military, space, and hazardous waste management applications [13].

E.JPEG 2000

JPEG 2000 is a new digital imaging system that builds on JPEG but differs from it. It utilizes a wavelet transform and an arithmetic coding scheme to achieve scalability in its design and operation. It offers improved compression, better quality for a given file size under most circumstances. This is especially true at very high compression.

Many applications involve the real time coding of image signals, for use in mobile satellite communications, cellular telephony and audio for videophones or video teleconferencing systems [16].

F.Visual Secret Sharing Scheme

The visual secret sharing (VSS) scheme, introduced by Naor and Shamir in 1994, is a type of secret sharing scheme which can split the secret information into n shares and recover them by superimposing the shares. In VSS, the secret to be hidden is a black and white image and each share is comprised of groups of black and white sub pixels used to recover a pixel of the secret image. It is assumed that a white pixel in a share is transparent and a black pixel is opaque so that superimposing shares can result in recovering the secret image. An advantage of VSS is that, unlike other cryptography techniques, this secret recovery does not need difficult computations [9].

II. RELATED WORK

The major contributions of our work are the first solution that addresses the pixel expansion problem of the EVCS for general access structures. So we add cover images to solve pixel expansion problems. Where removing cover images results in repeating the pixel expansion problems and also extends the shares synchronization time. So we are extending visual cryptography without removing cover images. Where it reduces pixel expansion problem [1].The drawback of the proposed method, cannot avoid the pixel expansion problem.

The drawbacks of the proposed method can be applied only on both binary and halftone images. This method cannot be used in grayscale image, color image and still image.

Although the scheme introduces some noise into the recovered image, the recovered image is substantially clearer than in other proposed non-expansion schemes [9].

To hide a binary image into two meaningful shares Chin-Chen Chang et al suggested spatial-domain image hiding schemes. These two secret shares are embedded into two gray level cover images. To decode the hidden messages, embedding images can be superimposed. Balancing the performance between pixel expansion and contrast Liguo Fang recommend a (2, n) scheme based on combination. Threshold visual secret sharing schemes mixed XOR and OR operation with reversing and based on binary linear error-correcting code was suggested by Xiao-qing and Tan.

The disadvantage of the above schemes is that only one set of confidential messages can be embedded, so to share large amounts of confidential messages several shares have to be generated [15].

In this paper I have described about how the secret images or text has been sent to the other party in such a way that if any Third person or hacker gets the message then he/she cannot find out the original message. This method is possible only when I use visual cryptography i.e. in this method I divide the image in different shares such that seeing single piece of share no-one can understand what the secret text is about. I can only get the final image when I stack all the shares or the threshold that I have set for the shares to get the final image. But during dividing the share processes their will be loss of contrast i.e. loss of some pixels due to which the final image will not be as clear as the original image. But this method is useful for many applications such as in Banks, Military etc [10].

The proposed method can withstand various signal processing attacks, including lossy compression, sharpen filtering, blur filtering and image cropping. Especially, it achieves robustness with respect to the image rotation and image rescaling [17].

But the above proposed method does not withstand the other types of attacks, such as additive noise, denoising attacks, watermark removal and interference attacks, statistical averaging, geometrical attacks [8].

We have presented a new scheme for embedding a gray-scale image into a color host image. The proposed system does not need the original host image for recovering the signature at the receiver. Since the system uses embedding in both red and blue components, it can works well for variety of images with different distribution of colors. We evaluate the reconstructed signature image quality when the host undergone various signal processing and geometrical attacks. The results show the system has good robustness. The developed system has low implementation complexity [6]. The drawback of the

proposed method cannot resist the implementation complexity.

The drawback of the proposed watermarking method is highly robust against only the geometrical attacks. The further work will be oriented on the improving of the robustness against the removal attacks, mainly the loss compressions and the exploitation of the human visual system in the watermark embedding process for the better hiding the watermark into the original image [12].

The proposed scheme of watermarking scheme is imperceptible and robust against geometric attacks [11].

The drawback of the above proposed method is robust against only the geometric attack. But it is not robust against the other type of attacks, such as additive noise, filtering, denoising attacks, watermark removal and interference attacks, statistical averaging, geometrical attacks [8].

Visual cryptography technique is used to make the data secure. Here the original data is divided into a number of shares which are sent through different communication channels from sender to receiver. Therefore the intruder has less chance to get the whole information. But still it is not so secured.

The main drawback of the algorithm is in its number of loops. For n=6, k=5 and a 32 bit pixel with 50% '1', number of loop operation required is 32. For n=6, k=4 with other conditions same, number of loop operation required is 48. For n=6, k=3 with other conditions same, number of loop operation required is 64 [20].

The experimental results show that the reconstructed image will not be as clear as the original image [3].

Due to the nature of the traditional VC scheme, the size of the decoded image is unavoidably larger than the original image. In the future, we will introduce a probability-based model to solve this problem [18].

There are some flaws in the stated system. These flaws are as follows:

1. Original image is of size MXN and the share is of size nXn. The size of the share changes at each level. Thus easily identified as shares which requires some more information.
2. The second one is, two share blocks of a white secrete pixel are similar while share blocks of black secret pixel are complementary. If pixels are black then it's ok but in case of white pixel there an overhead of maintain redundant data of white pixels.
3. Original image is divided into number of shares. From figure we see that the outer pixels are having less possible combinations of black and white pixels. Hence this system manipulates pixels partially. Due to this the system may not gives exact output [2].

This paper through various visual cryptography schemes analyzing their efficiency in the field of secret sharing. To aggregate the results of various approaches we can see that most of the schemes suffer from the problem of pixel expansion and degraded contrast of recovered images. An imminent work can be a scheme that reduces the above discussed problems in an efficient manner. The drawback of this proposed method is that only reduce the problems. Those problems cannot be completely avoided [7].

This paper presents a system which takes three pictures as an input and generates two images which correspond to two of the three input pictures. The third picture can be recovered through the simple algorithms on two generated images. This scheme achieves lossless recovery and reduces the noise in the cover images [19]. The drawback of the proposed method, the noise can not completely removed.

The method of the joint feature undoubtedly has to pay a higher computational cost, especially when the gBSB neural network needs more times of iteration. Furthermore, there is not a definite criterion to choose the probability P and the threshold T. The percentage of the luminance feature or the texture feature is hard to be determined and to find out such a balance is not easy as well [5].

In existing system the visual secret sharing (VSS) scheme, a slight misalignment between the shares could dramatically degrade the visual quality of the reconstructed image. This alignment or registration problem is worsened if there is some distortion involved in the process of producing transparencies, either by photocopying or laser printing. The heat produced in the printing process may cause the plastic to bend.

III. PROPOSED SCHEME

In (2, n) a VSS scheme that allows a relative shift between the shares in the horizontal direction and vertical direction. When the shares are perfectly aligned, the contrast of the reconstructed image is equal to that of the traditional VSS scheme.

When the secret medical images are transmitted through the internet, that encrypted medical images are not directly transmitted. First that is partitioned into the number of shares for the purpose to secure the medical images. If the attacker finds out the one share of the secret image, he can't view the secret image. Because, when all the shares are perfectly aligned and stacked together, then we can view the secret image clearly. For that purpose the medical images are partitioned into the number of shares to secure the secret medical images.

IV. AES ENCRYPTION & DECRYPTION ALGORITHM

The AES algorithm is used for encrypt & decrypt the images. In 1999, NIST issued a new version of its DES standard that indicated that DES should only be used for legacy systems and that triple DES (3DES) be used.3DES has two attractions, that is first, with its 168-bit key length, it overcomes the vulnerability to brute-force attack of DES.

Second, the underlying encryption algorithm in 3DES is the same as in DES.

1) AES Cipher

- AES cipher was proposed by Rijndael.
- The key length can be 128,192 & 246 bits.
- The Block length is 128 bits.
- A number of AES parameters depend on the key length.

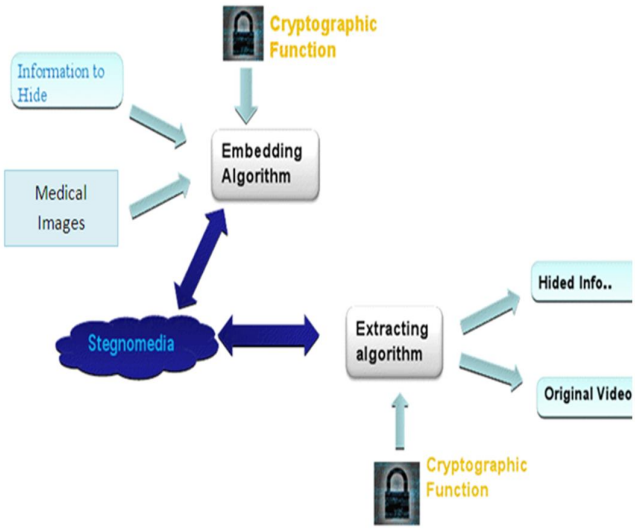
2) The Stages of AES

- Substitute Bytes
- Shift rows
- Mix Columns
- Add Round key

V. EXPERIMENTAL RESULT

The experimental results are discussed in this section. The process of encrypt & decrypt the medical images are performed for step by step by using the following figures.

Fig. 1 System Architecture



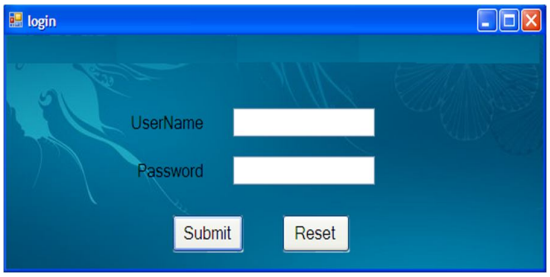
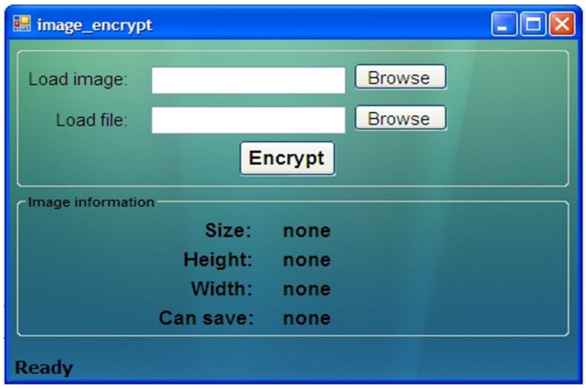


Fig. 2 Login

This form shows Login procedure.

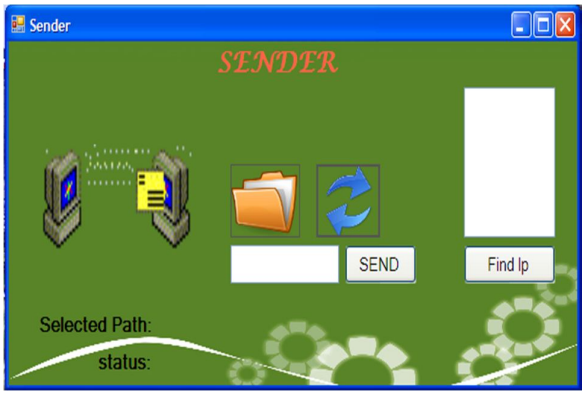
Registration

Fig. 3 Image encrypt



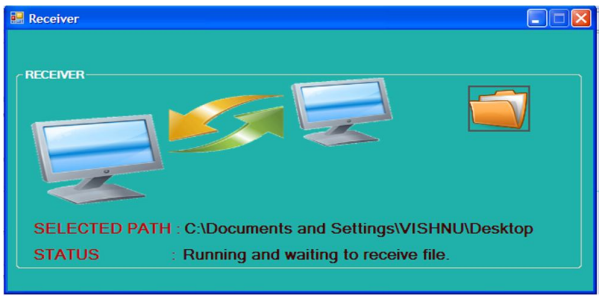
This form shows the image encryption.

Fig. 4 Sender



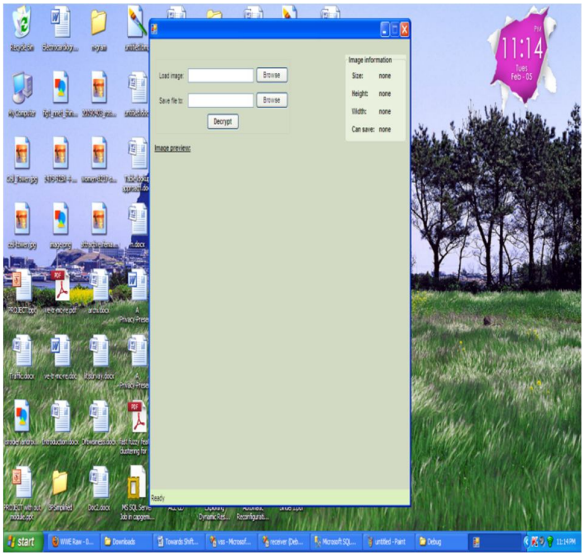
This form shows the sending of encrypted file.

Fig. 5 Receiver



This form is used to receive the file.

Fig. 6 Image decryption



This form is used to decrypt the file.

VI. CONCLUSION

We have proposed a (2, n)-VSS scheme, in this scheme, the secret medical images are divided into the number of the shares. This partition method is used to secure the secret medical images. If any attacker tries to access the secret medical images, at that time, the attacker find out one secret share method, he can't view the secret image. When all shared images are perfectly aligned and stacked together, we can view the reconstructed secret images. The share process is used for this purpose. All shares contain the watermarked images, which ensures the security, confidentiality and authentication scheme. Our proposed method present a secure patient medical images and authentication scheme which enhances the security, confidentiality and integrity of medical images transmitted through the Internet. The medical images are secured using the digital image watermarking scheme. If any unauthorized attacker try to access the medical images, that connection is immediately rejected. The proposed approach is used to provide the robustness against the wide variety of attacks and the visible quality of the reconstructed secret image is very clear as the original image.

REFERENCES

[1] Dr.V.R.Anitha and Dilip Kumar," Extending the visual cryptography algorithm without removing cover images", *International Journal of Engineering Trends & Technology*, Vol.4, Issue 4, April 2013.
[2] Arindam Dasgupta and Amit Kute,"A robust blind watermarking using fractional fourier rework and visual cryptography", *IJETAE*, Vol.3, Issue 3, March 2013.
[3] Ayan Banerjee and Sreya Banerjee,"A robust visual cryptography technique for photographic grayscale images using block optimization and blind invisible watermarking", *International Journal of Computer Theory and Engineering*,Vol.4,No.2,April 2012.
[4] Latha Parameswaran, and K. Anbumani, "A Robust Image Watermarking Scheme using Image Moment Normalization", World Academy of Science, Engineering and Technology 19 2006.
[5] Li Fan,Tiegang Gao and Qunting Yang, "A novel watermarking scheme for copyright protection based on adaptive joint image feature and visual secret sharing", *International Journal of Innovative Computing, Information and Control*,Vol.7,Number 7(A), July 2011.
[6] Mohsen Ashourian, Peyman Moallem and Yo-Sung Ho," A Robust Method for Data Hiding in Color Images", LNCS 3768, pp. 258 – 269, 2005.
[7] M.Monish and S.Iwin Thanakumar,"Visual secret sharing-A Pandect", *International Journal of Computer Science and Management Research*, Vol.2, Issue 2, February 2013.
[8] Natasa Terzija, "Robust digital image watermarking algorithms for copyright protection".
[9] Nazanin Askari, Cecilia Moloney and H.M.Heys,"A novel visual secret sharing scheme without image size expansion".
[10] Neelam Yadav,Dhiraj Kumar and Ravi Yadav,"Key sharing schemes using visual cryptography", *International Journal of New Innovations in Engineering and Technology*,Vol.1,Issue 4,April 2013.
[11] Pankaj U.Lande Sanjay, N.Talbar and G.N.Shinde,"FPGA prototype of robust watermarking JPEG 2000 encoder", *International Journal of Circuits, Systems and Signal Processing*, Vol.4, Issue 3, 2010.
[12] Radovan Ridzon and Dusan Levicky,"Robust digital watermarking based on the log-polar mapping", *Radio engineering*, Vol.16, No.4, Dec 2007.
[13] Rafael C.Gonzalez and Richard E. Woods, "Digital image processing".
[14] K.M.M. Rao*, Deputy Director, NRSA, Hyderabad-500 037, "Overview of image processing".
[15] P.S.Revenkar, Anisa Anjum and W.Z.Gandhare, "Survey of visual cryptography schemes", *International Journal of Security and its Applications*, Vol.4, No.2, April 2010.
[16] Shaik.Mahaboob Basha, Dr. B.C.Jinaga, "A Novel Optimum Technique for JPEG 2000 Post Compression Rate Distortion Algorithm", ACEEE *Int.J.on Information Technology*, Vol.1, No.2, Sep 2011.
[17] Shen-Chuan Tai, Chuen-Ching Wang and Chong-Shou Yu,"Visual Secret Sharing Watermarking for Digital Image", Informatica 26(2002) 381-388.
[18] Shu-Fen Tu and Ching-Sheng Hsu,"A Joint Ownership Protection Scheme for Digital Images Based on Visual Cryptography", *The International Arab Journal of Information Technology*, Vol.9, No.3, May 2012.
[19] V.Srinivas, Dr.E.V.Krishna Rao, Ch.Madhava Rao and K.Anitha,"A (2, 2) Effective Secret Sharing Scheme", *IJECT*, Vol.3, Issue 1, Jan-March 2012.
[20] R.Yadagiri Rao,"Secure Visual Cryptography", *International Journal of Engineering and Computer Science*, Volume 2, Issue 1, Jan 2013.