A Secure Lossless Transmission Scheme for Medical Images

Namitha P., Manoj Ray D.

Abstract— Nowadays security becomes an inseparable issue as information technology is ruling the world. The recent advances in information and communication system have provided new means for transferring valuable health information of patients in order for supporting emerging applications like telemedicine. For the better diagnosis purposes, most of the cases it is necessary to to transfer medical images from one place to another or need to store such datas in particular places in secure manner, and has become a challenge. To achieve high security as well as to get good image quality this paper has framed new efficient Bit level based secret sharing algorithms for medical images. The main advantage of this proposed method is to provide good quality of the image along with security and without any post or pre processing. Similarly for the efficient utilization of available transmission bandwidth and storage space, here framed a better compression scheme in lossless manner, which can provide a compression rate more than that of RLE image compression scheme.

The method proposed here utilizes bit-level decomposition and stacking operations to both encrypt and decrypt B-bit image, preserves all the features of traditional k, n sharing schemes of visual cryptography and allows for the perfect reconstruction of the input B- bit image. The compression scheme can reduce it's output size less than 30 percentage of the encrypted input size. The proposed scheme can be applicable to binary, grayscale and color images.Most importantly; the technique can support the universally accepted format for medical image storage and transfer that is the DICOM (Digital Imaging and Communications in Medicine) format.

Index Terms—bit level secret sharing, EPR, encryption, RLE, telemedicine, vectorization, visualcryptography.

1 INTRODUCTION

Nowadays, major concern throughout the medical field is to make sure that high quality health care available to all. Traditionally, difficulty is that achieving better health care is possible only if provider and recipient are physically present in the same place. Recent advances in information and communication technology have increased the number of ways by which better health care can be delivered to all with reduced effort. Techniques like teledignosis, telesurgery, teleconsultation etc are part of revolution, where medicine, Information and telecommunication technology meet with the aim of better health care delivery through an effortless way.

Telemedicine means " Medicine At Distance ", is achieved by the transfer of Electronic patient Record [EPR] across the public network , so as to provide consultation by specialists located in geographically different locations. In such applications, health informations of patients such as previous examinations' result, lab test results, medical images etc collected in digitized form can be easily transmitted over network.Since such ectronic datas are sensitive, the advanced information and communication techniques should compromise their security due to their ease of manipulation" [1]" .

The security of the health information is compromised by preserving the following things.

- **Authentication:** Ensuring whether the data was transmitted by a properly identified sender, and is not a replay of a previously transmitted data.
- **Confidentiality:** It is the property which ensures that only authorized users have access the information in normal condition.
- **Integrity:** It is the proof that information has not been modified in an unauthorized way.
- **Availability:** It is the ability of the information system to be used under normal working condition.
- **Patient privacy**: It is the right of the patient to determine when, how and to what extent their health information is shared with others "[1], [3], [6]".

In these days of medical advancement, the usage of medical images become necessary for better clinical diagnosis purpose, because by using these types of images an expert can look up inside the body of the patient without having to open up the body surgically. Due to this large volume of medical images are produced and used every day. Such images need to be stored for future references also. Since large generation of medical images become necessary, it is also necessary to undergo the process of compression before storing or transmitting over the network.Lossy compression schemes are not suitable in case of medical images due to the chance of useful clinical information loss. Hence challenges unique to medical images is that preserve the quality of the images together with achieve maximum compression rate for efficient transmission and storage "[1], [2]".

This paper deals with a lossless security scheme for medical image transmission based on share creation. The general outline of the paper is given as follows. Section 2 describes the proposed algorithm; Section 3 describes the Experimental studies followed by section 4 which describes Conclusion.

2 PROPOSED SCHEME

To achieve high security as well as to get good image quality this paper has framed new effcient Bit level based secret shar-

ing algorithms for gray scale image. The main advantage of

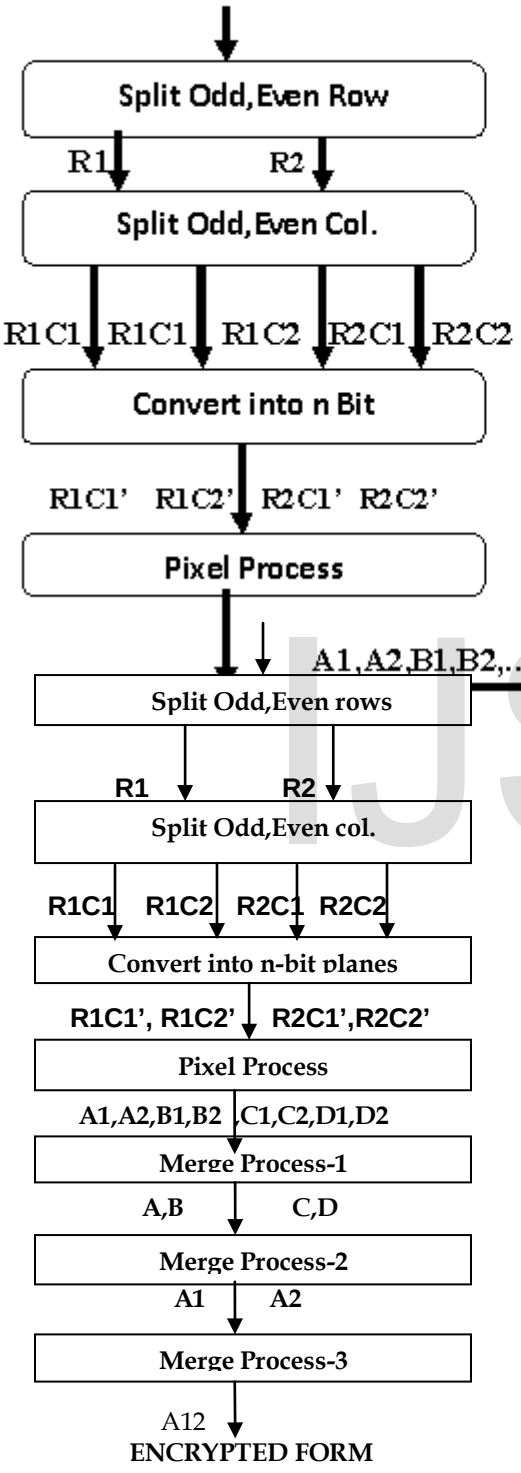


Fig 1: Steps in Bit Level Based Secret Sharing Scheme

Splitting Process : First level splitting is based on row informations,in which extract odd rows together form one subband (R1) and even rows together form other one (R2).In the second level splitting take the 2 previously created subbands as inputs.For R1 extract all odd columns together form new subband (R1C1),and even column together form other one(R1C2).Simillarly for R2 generate 2 subbands R2C1 and R2C2.

Conversion Process: It is actually a preprocessing step for following pixel process.In which generates **n**-bit planes for an n-bit image.For each of the n-planes performs the pixel expansion as explained below.

Pixel Process: For each of the n-planes perform the following,

i) Declare the matrix for 2 shares as

Share1=zeros (2*rows,(2*columns))

Share2=zeros (2*rows,(2*columns))

ii) For each rows and columns

If($plane_k$ (i,j)==1)

Set share1(i , 2*(j-1):2*j)=s1 and

Set share2(i, 2*(j-1):2*j)=s1

Else

Set share1(1,2*(j-1):2*j)=s1 and

Set share2(1,2*(j-1):2*j)=s2

End If

End For

Where **s1=[1 1; 0 0;]**

s2=[0 0; 1 1;]

iii) compose S1(u, v, 0-(n-1)) and S2(u, v, 0 (n-1)) using equations:

$S1(u,v)= share1(u,v,(n-1))*2^{(n-1)}+share1(u,v,(n-2))*2^{(n-2)}+ \ldots .+ share1(u,v,0)*2^{0} \ldots \ldots$

$S2(u,v)= share2(u,v,(n-1))*2^{(n-1)} +share2(u,v,(n-2))*2^{(n-2)} + \ldots .+ share2(u,v,0)*2^{0} \ldots \ldots$

Where u = 2*image height and

v= 2*image width

now we get 2*n different shares for an n-bit image.

Merging Process: Three stages will be taking place to merge the output subbands of the pixel process A1(;), A2(;) ,B1(;) ,B2(;) ,C1(;) ,C2(;) ,D1(;) ,D2(;).

where in each stage the 2xN level of subbands are converted in to N level of subbands. The following combination is made in the first level of the merging process A1D1(;), A2D2 (;),

B1C1(;), B2C2 (;) . For example, let us consider the A1D1(;) combination. A1 is the first subband and D1will be the another subband, first A1subband row values are placed in A1D1(;) in the position of odd(1,3,5,7…) Fig-3. Similarly D1subband row values are placed in the even position of A1D1(;) (2,4,6,…) Likewise both *A*1and *D*1subbands values are merging. Similarly both remaining merging process are done as shown in the figure below,

level - 1 merging:
A1(;)+D1(;)=A(;)
A2(;)+D2(;)=B(;)
B1(;)+C1(;)=C(;)
B2(;)+C2(;)=D(;)
level - 2 merging:
A(;)+C(;)=A1(;)
B(;)+D(;)=A2(;)
level - 3 merging:
A1(;)+A2(;)=A12(;)-**Encrypted Form**

2. 2 Compression Scheme:

The compression of the encrypted image is done by extended version of RLE. When we apply the RLE coding for compression, during the case of non-repetitive bit value, the size of image will be lessthan that of size of RLE coded form. Similar issues can occur while we compress the image in secure manner. The Proposed algorithm is adopted to solve these kinds of problems. The encrypted image is the input for the compression algorithm .The basic principle is that, the encrypted form consists of large number of repeted pixel values as well as repeted paired combinations of pixel values.This is happend because of pixel expansion process during encryption.So compression can be completed into two distinct steps. In the initial stage perform the vectorization of encrypted input,from which continuous occurance of a particular pixel value can be coded as" pixel value,followed by ending location" which are seperated by a '.' symbol.In the second level of compression the coded sequence is of the form paired pixel value followed by ending location which is separated by a '-' symbol."[4],[7]"
The proposed scheme can be explained with an example,
Input Sequence: 1 2 2 2 2 2 2 1 2 1 2 1 2 1 2 1 2 3 1 1 1 1 1 1 1 1 5 4 5 4 5 4 5 4 5 4 5 4 5 4 7;
After level-1 compression:
Compressed Sequence: 1 2.7 1 2 1 2 1 2 1 2 1 2 1 2 3 1.28 5 4 5 4 5 4 5 4 5 4 5 4 5 4 7 ;
After level-2 compression: 1 2.7 1 2-15 3 1.28 5 4 -33 7;

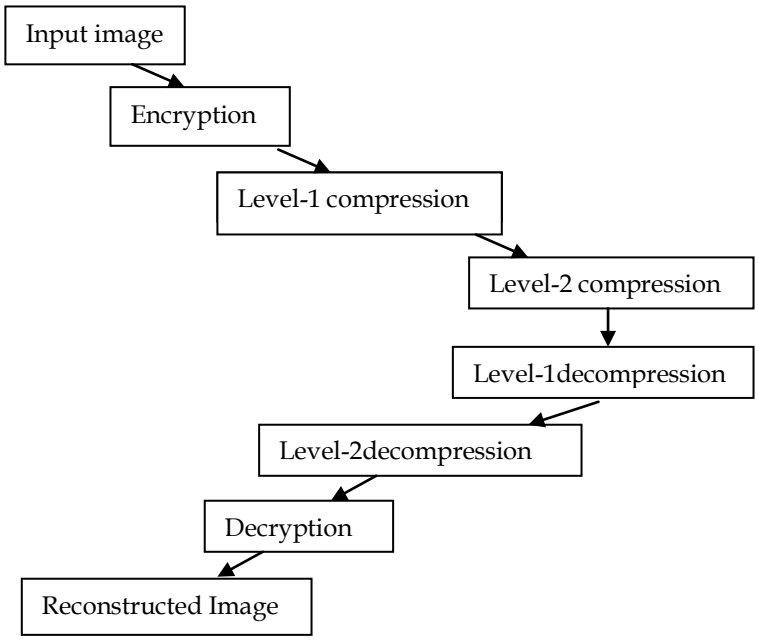


Fig 2: Block digram of compression and decompression

2. 3 Decryption Scheme:

Step 1: Reversing of three levels merging

Step 2. Decoding Algorithm
2.1: Decompose each input share1 and share2 to n-bit binary images (2k1 x 2k2),ranging from (0) for the least significant bit (LSB) to (n)for the most significant bit(MSB).
2.2 : implement the following procedure:

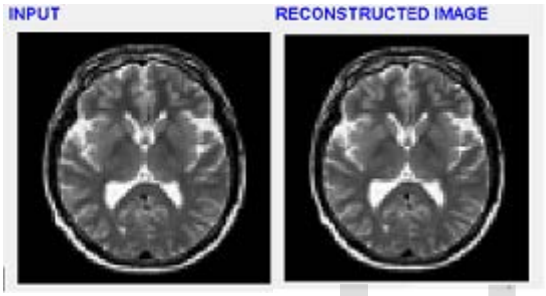
```
for plane = 0 to n
    i from 1 : k1
        j from 1 : k2
            if Share1(i,j,plane)=Share2(i, j,  plane) then
                    bP(i, j, plane) =1
            else
                    bP(i, j, plane) =0
            End If
        j=j+2;
    i=i+2;
End For
```

Step3: the n binary images b (k1 x k2) are constituted by bit-level stacking using equation:
$Share1(u,v)= b_{(n)}(u,v,7)*2^{(n-1)} +b_{(n-1)}(u,v,6)*2^{(n-2)} \ldots + b_1(u,v,0)*2^0$
Get the output shares of splitting process (R1C1,R1C2,R2C1,R2C2).
Step4: Reversing of splittingprocess:
Take the 4 shares (R1C1, R1C2, R2C1, R2C2) as inputs and place each share in proper row and column order to get the original input image.''[5]"

The decryption can be performed in a reversible manner.Since the decompression process is lossless,the resultent output is exact copy of the encrypted image.so decryption process can generate a copy of the input image which has no loss from input image.So it can be applicable to medical images with no doubt.

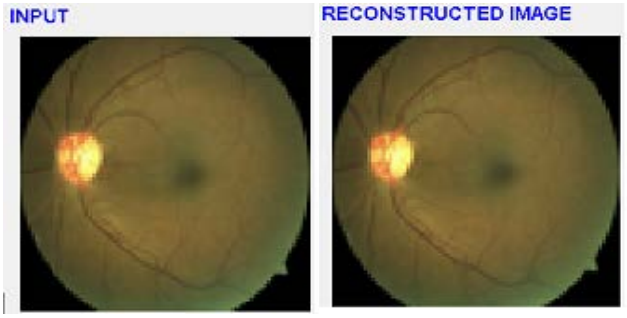
3 Experimental Results

The performance of the application implemented for the secure medical image transmission scheme using the proposed method has been evaluated using several images. Some examples are given below:



a

b



c

Fig 3: Input and reconstructed images for (a) Gray (b) Dicom (c) Color

Table given below shows the size reduction information

Input Image Type	Size before Compression	Size after Compression	Rate of Compression
Gray	51200	11083	21.64 %
DICOM	80000	18476	23.09 %
Color	153600	41345	26.92 %

Table 1: size reduction information

Conclusion

We can conclude that the proposed compression algrithm helps to achieve the lossless compression and at the same time we can reduce less than 30 percentages from encrypted size. Also the bit level secret sharing scheme for encryption is best suited for the medical images. The decompressed image has same size and clarity of the original image which provides the Integrity and Availability of the algorithm. The Confidentiality criterion is going to achieve with the accurate compression technique. Similarly the secret sharing scheme has been developed for sending a data (image) in a secured and compressed manner. It is applicable for medical data or military data.This method can be implemented further for military images to further study the efficiency.
From experience it is clear that many of the medical images having least significant bitplanes having no specific info mation contents, so as a future work we can neglect such planes before encryption leads to reduction of image size to a large extent,which helps to increase the compression ratio without lossing any valueable image information.

Acknowledgment

During the paper preparation, many reviews provided many valuable consecutive comments. I thank all.

References

[1] Rohini, VinayakBairagi," Lossless Medical Image Security, "International Journal Of Applied Engineering Research, Dindigul Volume 1, No 3, 2010.
[2] F. Caoa, H.K. Huang, X.Q. Zhou," Medical Image Security In A Hipaa Mandated Pacs Environment", Computerized Medical Imaging And Graphics 27 (2003) 185–196.
[3] Joint NEMA/COCIR/JIRA, Security and Privacy Committee (SPC) , "Identification and Allocation of Basic Security Rules in Healthcare Imaging Systems "In September 2002, www.nema.org/medical.
[4] Fast and Efficient Secure Medical Image Compression Schemes, S. Manimurugan CSE Department, Karunya University, Coimbatore, and India,E-mail:smanimurugan@yahoo.co.in-621.
[5] "Visual Cryptography Vs Bit Level Secret Sharing For Image Encryp-

tion*", Musaab R.Abdulrazzaq,Eng.&Tech.Journal,Vol.28,No.7,2010.*

[6] Hui Huang," PhD thesis-Contribution to the control of integrity of medical images-under the seal of the European University of Brittany".

[7] David Salmon,"Book -Data Compression, The Complete Reference, Fourth Edition.

[8] Moni Naor and Adi Shamir," visual cryptography", Department of Applied Math and Computer Science, Weizmann Institute, Rehovot 76100, Israel.

[9] Chandramathi S., Ramesh Kumar R., Suresh R. and Harish S.,"An overview of visual cryptography ", *International Journal of Computational Intelligence Techniques*, ISSN: 0976–0466 & E-ISSN: 0976–0474 Volume 1, Issue 1, 2010.

[10] Rupinder Kaur, Nisha Kaushal," Comparative Analysis of Various Compression Methods for Medical Images ".