Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

THE NEW APPROACH OF VISUAL CRYPTOGRAPHY SCHEME FOR PROTECTING THE GRAYSCALE MEDICAL IMAGES

[1]S.MANIMUURGAN, [2]C.NARMATHA, [3]K.PORKUMARAN

[1]Professor and Head, Computer Science and Engineering, *MBC College of Engineering and Technology*

[2]Assistant Professor, Electronics and communication, *MBC College of Engineering and Technology*

[3]Professor Electrical and Electronics Engineering, Dr. NGP College of Engineering and Technology

E-mail: [1]smanimurugan@yahoo.co.in , [2] cmnarmatha@gmail.com, [3]prokumaran@gmail.com

ABSTRACT

Transferring an image from one place to another or storing an image in a particular place in a secure manner has become a challenge. In order to face this challenge, a new Visual Cryptography (VC) scheme for grayscale medical images has been proposed. Generally, the VC method has a few problems or rather, short comings. For instance, when the pixels are expanded, the level of security applied will be high but the quality of reconstructed image will be low. Similarly, if the extent of pixel expansion is reduced, its security is lowered and quality of the image is retain. Hence, to achieve high security as well as to get a good image quality, the proposed Tailored Visual Cryptography Scheme (TVCS) for grayscale medical image is ideal. Some of the VC leads to loss while reconstructing the image but this proposed algorithm which has been developed for medical image, will not provide any loss and the result has been experimented and proved by measuring CC. The main advantage of this proposed method is to provide good quality for the images with reliable security without any pre or post processing. In the proposed algorithm, two types of processes are taking place: Tailored Visual Cryptography Encryption (TVCE) and Tailored Visual Cryptography Decryption (TVCD). The TVCE process provides an encrypted image and in order to get this encrypted image, Splitting Process, Converting Process, Pixel Process and Merging Process are performed. Simultaneously Segregation Process, Inverse Pixel Process, 8-bit into Decimal Conversion Process and Amalgamate Process are involved to retrieve the original medical image from the TVCD process. In the experimental part, many medical images have been tested and the result is also provided. In order to check the security properties like Confidentiality, Integrity and Availability (CIA), the CC has been calculated. From these experimentations, the proposed algorithm provides better result than the existing algorithms.

Keywords:- *Visual Cryptography, Correlation Coefficient, Gray scale medical image*

1. INTRODUCTION

VC is a cryptographic technique which allows visual information to be encrypted in such a way that the decryption is performed to obtain the original image. In VCS, an image is broken up into N shares, so that only an individual with all N shares could decrypt the image, while any N-1 share reveals no information about the original image. Each share is printed on a separate image and decryption is performed by overlaying the shares. When all the N shares are overlaid, the original image would appear. Each pixel of the images is divided into smaller blocks. There will always be the same number of white (transparent) and black blocks [13]. If a pixel is to be divided into two parts, there would be one white and one black block. If the pixel is to be divided into four equal parts, there would be two white and two black blocks. For example: If a pixel on share-1 has a given state, the pixel on share-2 may have one of two states: identical or inverted to the pixel of share-1. If the pixel of share-2 is identical to share-1, the overlaid pixel will be half black and half white. Such overlaid pixel is called grey or empty pixel [1-3]. If the pixels of share-1 and share-2 are inverted or opposite, the overlaid version will be completely black. This is an information pixel. The

Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

two shares can now be created. One transparent image, share-1, has pixels which all have a random state, one of the six possible states. Share-2 is identical to share-1, except for the pixels that should be black (contain information) when overlaid. These pixels have a state that is opposite to the same pixel in share-1. If both images are overlaid, the areas with identical states will look grey, and the areas with opposite states will be black. The system of pixel can be implemented in different ways. For example, each pixel is divided into four blocks. However, pixels divided into two rectangle blocks can be used, or even divided circles. It doesn't matter if the pixel is divided horizontally or vertically. There are many different pixel systems, some with better contrast, higher resolution or even with color pixels (Figure 1). If the pixel states of share-1 are truly (crypto secure) random, both empty and information pixels of share-2 will also have completely random states. One cannot know if a pixel in share-2 is used to create a grey or black pixel. Since, to need the state of that pixel in share-1 (which is random), to know the overlay result. If all requirements for true randomness are fulfilled, VC offers absolute confidentiality according to the information theory [4,6]. This technique is classified into two algorithms namely,

- Share Generation Algorithm
- Stacking Shares Algorithm

The over view of the basic Visual Cryptography Scheme is shown in Figure 1.

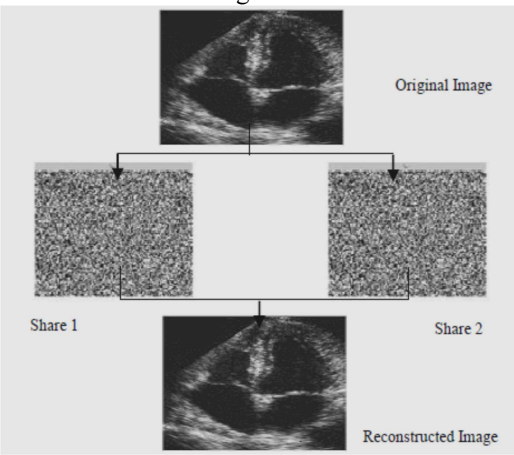

Figure 1 Overview of the Visual Cryptography Scheme

1.1. Share Generation Algorithm

Each share is a collection of m black and white sub-pixels that are printed in close proximity to each other, so that the human visual system averages their individual black/white contributions. This algorithm is used for creating shares for the input image. It takes the input image and divides it into n shares. These shares are created using a set of procedures like processing the white and black pixels. This creates n shares in an unreadable format and any single share cannot reveal the secret image as shown in Figure 1.

1.2. Stacking Share Algorithm

It is a procedure of getting original image by stacking the transparencies. Stacking algorithm merges the shares created using the share generation algorithm. The created shares are overlaid and thus the original image can be retained as shown in Figure 1. In the section II is discussed in detail about overview of the TVCS, the section III is discussed about the results which was generated from the proposed method and the section IV is discussed about the conclusion of the entire work[5,8].

2. THE PROPOSED TAILORED VISUAL CRYPTOGRAPHY SCHEME (TVCS)

The objective of the proposed approach, in this scheme is to obtain a good quality of the output image without any post or preprocessing. Several experiments have been done and have come out with a new approach in VC [5]. This technique is implemented for grayscale medical images. The proposed TVCS is classified into two types of algorithm:

- TVC Encryption algorithm (TVCE)
- TVC Decryption algorithm (TVCD)

Using encryption algorithm the original image can be converted into an encrypted image (figure 6). Finally, that encrypted image will be decrypted by using TVCD algorithm. The overview of the algorithmic functions, how it's going to encrypt and decrypt the grayscale medical image in an efficient manner are discussed in this sections.

2.1. Secret Medical Image Creation Using Proposed TVCE Algorithm

This section deals with the detailed view of the encryption process, how it's going to generate or produce the encrypted secret medical image in an efficient manner by using the following process

i. Splitting Process
ii. Conversion Process
iii. Pixel Process
iv. Merging process

Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.1.1. Splitting Process for producing the Subbands

In this process, the original grayscale medical image $\Theta m(i,j)$ is taken as an input image. This input medical image is splitted into two parts based on the odd and even rows[7]. For example if the input medical image matrix row counting values are 1,2,3,4,5,6,7,8,9, etc., from these rows, odd row values are taken and placed into one new matrix (subband) which is called ΘR_1 in Equation 1. Similarly, the even row values are placed in to the matrix ΘR_2. In the Equation 1 $\Theta m(i,j)$ is represented as the original medical image. The splitted odd rows image $\Theta m(odd,)$ and even rows image $\Theta m(even,)$ from the input grayscale medical image is called as $\Theta R_1(i,j)$ and $\Theta R_2(i,j)$. $\oplus$ denotes the merging symbol.

$$\Theta m(i,j) = \Theta m(odd,) \oplus \Theta m(even,) \quad (1)$$

$$\Theta m(odd,) \prec \Theta R_1(i,j) \quad (2)$$

$$\Theta m(even,) \prec \Theta R_2(i,j) \quad (3)$$

Equation 2 and 3 is derived from Equation 1and both subbands are taken for the next level of Splitting Process. Here the $\Theta R_1(i,j)$ image subband values are splitted based on the columns, the odd columns values which are placed in one matrix and even columns matrix are placed in another matrix, from this process the $\Theta R_1(i,j)$ will produce two levels of subbands, $\Theta R_1C_1(i,j)$ and $\Theta R_1C_2(i,j)$ in Equations 4, 5 and 6.

$$\Theta R_1(i,j) = \Theta R_1(,odd) \oplus \Theta R_1(,even) \quad (4)$$

$$\Theta R_1(,odd) \prec \Theta R_1C_1(i,j) \quad (5)$$

$$\Theta R_1(,even) \prec \Theta R_1C_2(i,j) \quad (6)$$

Same process is carried out to produce the next two subbands from the $\Theta R_2(i,j)$. Those subbands are $\Theta R_2C_1(i,j)$ and $\Theta R_2C_2(i,j)$ in Equation 7, 8 and 9.

$$\Theta R_2(i,j) = \Theta R_2(,odd) \oplus \Theta R_2(,even) \quad (7)$$

$$\Theta R_2(,odd) \prec \Theta R_2C_1(i,j) \quad (8)$$

$$\Theta R_2(,even) \prec \Theta R_2C_2(i,j) \quad (9)$$

$$\Theta m(i,j) = \Theta R_1C_1(i,j) \oplus \Theta R_1C_2(i,j) \oplus \Theta R_2C_1(i,j) \oplus \Theta R_2C_2(i,j) \quad (10)$$

2.1.2. Creating Binary image using Conversion Process

The above Section deals with the original medical image, which is divided into four subbands through two levels processes. These four subbands are taken as an input for this process. Here, every subband or every matrix pixel values are converted into 8-bit binary format. Suppose, the pixel value is 2, the corresponding binary value 10 is modified into 00000010. The $\Theta R_1C_1(i,j)$ matrix values are converted into 8-bit binary value $\Theta R'_1C'_{18bit}(i,j)$ .Similarly, $\Theta R_1C_2(i,j)$, $\Theta R_2C_1(i,j)$ and $\Theta R_2C_2(i,j)$ also converted into 8-bit binary values in Equations 11, 12, 13 and 14.

$$\Theta R_1C_1(i,j) = \Theta R'_1C'_{18bit}(i,j) \quad (11)$$

$$\Theta R_1C_2(i,j) = \Theta R'_1C'_{28bit}(i,j) \quad (12)$$

$$\Theta R_2C_1(i,j) = \Theta R'_2C'_{18bit}(i,j) \quad (13)$$

$$\Theta R_2C_2(i,j) = \Theta R'_2C'_{28bit}(i,j) \quad (14)$$

From the above Equations 11, 12, 13 and 14, it can derive Equation 15.

$$\Theta m(i,j) = \Theta R'_1C'_{18bit}(i,j) \oplus \Theta R'_1C'_{28bit}(i,j) \oplus \Theta R'_2C'_{18bit}(i,j) \oplus \Theta R'_2C'_{28bit}(i,j) \quad (15)$$

2.1.3. Pixel Process for Converted Binary Medical Image

This pixel process is mainly used for encrypting the binary information. Here, each subband binary information is transformed into a cipher text format. The pixel process provides two level subbands from every subband. So, the N input of the subband information is converted in to 2N

Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

subband information by referring $\prod_{1=[i,j]}^{0=[i,j]} M$. $\prod_{1=[i,j]}^{0=[i,j]} M$ is the reference matrix for '1' and '0' which is given in Figure 2 and 3. Matrix $\Theta R_1' C_{18bit}'(i,j)$ is considered for pixel process, from the input matrix the first binary pixel value will be checked, if the value is '0' it will refer to the corresponding reference matrix for '0', the column value will be placed in A_1 and next column will be placed in A_2. If the value is '1' the same process is followed. Likewise, based on the input matrix pixel value, the output subband will be created by referring to the reference matrix $\prod_{1=[i,j]}^{0=[i,j]} M$. From the pixel process the input subband binary information will be classified into two types of encrypted subbands[9,12]. From the Equations 16, 17, 18 and 19 the following encrypted secret subbands were generated $A_1(;), A_2(;), B_1(;), B_2(;)....D_1(;), D_2(;)$. The ∇ symbol denotes the reference.

$$\Theta R_1' C_{18bit}'(i,j) \nabla \prod_{1=[i,j]}^{0=[i,j]} M = A_1(;) \oplus A_2(;) \quad (16)$$

$$\Theta R_1' C_{28bit}'(i,j) \nabla \prod_{1=[i,j]}^{0=[i,j]} M = B_1(;) \oplus B_2(;) \quad (17)$$

$$\Theta R_2' C_{18bit}'(i,j) \nabla \prod_{1=[i,j]}^{0=[i,j]} M = C_1(;) \oplus C_2(;) \quad (18)$$

$$\Theta R_2' C_{28bit}'(i,j) \nabla \prod_{1=[i,j]}^{0=[i,j]} M = D_1(;) \oplus D_2(;) \quad (19)$$

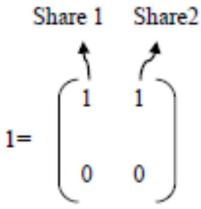

Figure 2 Reference matrix for '1'

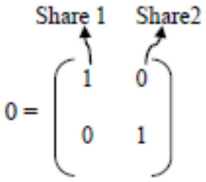

Figure 3 Reference matrix for '0'

2.1.4. Merging the encrypted medical image subbands

Three stages take place to merge the output subbands of the pixel process where in each stage the 2N level of subbands are converted into N level of subbands. The following combination is made in the first level of the merging process $A_1D_1(;), A_2D_2(;), B_1C_1(;), B_2C_2(;)$ as given in Figure 4. For example, in the $A_1D_1(;)$ combination, A_1 is the first subband and D_1 will be another subband, first A_1 subband every row values are placed in the odd position of $A_1D_1(;)$ akin to 1,3,5,7…etc., in Figure 5. Similarly, D_1 subband row values are placed in the even position of $A_1D_1(;)$ reminiscent of 2,4,6,… etc., in Figure 5.

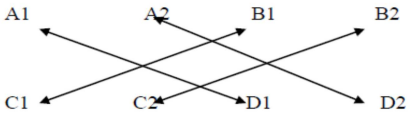

Figure 4 First level of the merging process

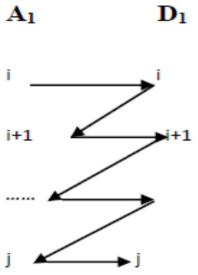

Figure 5 Merging process of A_1 and D_1

Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In the same way, both A_1 and D_1 subbands values are merged and same process is also followed for the remaining subbands in Equations 20, 21 and 22. In this merging process N/2 level of subbands are produced from N subbands in every stage as shown in Figure 4. Remaining two merging process works the same way as the first stage (level)[10]. The different levels of merging process have been derived from Equations 20-23 in every stage; the combination of the merging process is given in detailed manner as represented in the Equations 20, 21 and 22. Finally, the output of the merging process is one single encrypted image as shown in Figure 6.

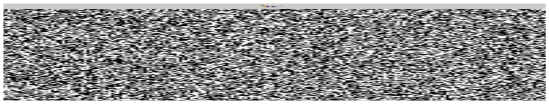

Figure 6 Encrypted Secret Medical Image after the merging process.

- Merge Level-1

$$\left.\begin{aligned} A_1(;) \oplus D_1(;) &= A(;) \\ A_2(;) \oplus D_2(;) &= B(;) \\ B_1(;) \oplus C_1(;) &= C(;) \\ B_2(;) \oplus C_2(;) &= D(;) \end{aligned}\right\} \quad (20)$$

- Merge level-2

$$\left.\begin{aligned} A(;) \oplus C(;) &= A_1(;) \\ B(;) \oplus D(;) &= A_2(;) \end{aligned}\right\} \quad (21)$$

- Merge Level-3

$$A_1(;) \oplus A_2(;) = A_{12}(;) \quad (22)$$

$$A_{12}(;) \prec E_{12}(;) \quad (23)$$

The first level of the merging process is working based on the Figure 4, following the same procedure; the output of the first merging process will be merged once again in the second level. Here, the four subbands will be transformed into two subbands $A_1(;)$ and $A_2(;)$. In the same way, the output of the second level that merged two subbands will be merged in the third level of merging process. In the Equation 22, two subbands will be converted into a single subband $A_{12}(;)$, this subband is called highly encrypted secret medical image $E_{12}(;)$ given in Equation 23.

2.2. Reconstruction of the Original Medical Image from Encrypted Secret Image Using TVCD

In this section, is going to be discussed in a detailed about decryption process. To encrypt the image is uncomplicated but to reconstruct the image in an accurate manner is a challenge. To achieve these challenges some of the efficient process have been proposed. Those processes are

i. Segregation process,
ii. Inverse pixel process,
iii. 8-Bit into decimal conversion process,
iv. Amalgamate process.

2.2.1. Split the Encrypted Image Using Segregation Process

In this process the encrypted medical image is taken as an input image $E_{12}(i, j)$. This is the reverse of merging process which was discussed in the above section. The segregation process has been classified into three processing levels. In every level, the N input subbands are divided into 2N subbands. In first level the encrypted image odd rows $E_{12}(odd; j)$ and even rows $E_{12}(even; j)$ are splitted in a separate manner. In detail, the odd rows are placed in one matrix $A_1'(i, j)$ which is taken from the encrypted medical image, in the same way the remaining even rows are placed into another matrix or subband $A_2'(i, j)$. So, the N subband or image will be converted 2N subband in the first level. Equations 24-26 are clearly defines, how the first level of the segregation process is working for splitting the subband from encrypted image.

Segregation process level-1

Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$E_{12}(i,j) = E_{12}(odd,j) \oplus E_{12}(even,j) \quad (24)$$

$$E_{12}(odd,) = A_1^{'}(i,j) \quad (25)$$

$$E_{12}(even,) = A_2^{'}(i,j) \quad (26)$$

Segregation process level-2

$$A_1^{'}(i,j) = A_1^{'}(odd,j) \oplus A_1^{'}(even,j) \quad (27)$$

$$A_2^{'}(i,j) = A_2^{'}(odd,j) \oplus A_2^{'}(even,j) \quad (28)$$

$$A_1^{'}(odd,j) = A^{'}(i,j) \quad (29)$$

$$A_1^{'}(even,j) = C^{'}(i,j) \quad (30)$$

$$A_2^{'}(odd,j) = B^{'}(i,j) \quad (31)$$

$$A_2^{'}(even,j) = D^{'}(i,j) \quad (32)$$

The first level output $A_1^{'}(i,j)$ and $A_2^{'}(i,j)$ will be considered for the next level of segregation process. Same way is followed here, by taking up the $A_1^{'}(i,j)$. $A_1^{'}(i,j)$ will be classified into the two parts based on the odd row and even row [3], from this process two subbands are created. The remaining processes are based on the same concept and everything has been defined in a detailed manner from Equations 33 to 45.

$$A^{'}(i,j) = A^{'}(odd,j) \oplus A^{'}(even,j) \quad (33)$$

$$A^{'}(odd,j) = A_1^{'}(i,j) \quad (34)$$

$$A^{'}(even,j) = D_1^{'}(i,j) \quad (35)$$

$$B^{'}(i,j) = B^{'}(odd,j) \oplus B^{'}(even,j) \quad (36)$$

$$B^{'}(odd,j) = A_2^{'}(i,j) \quad (37)$$

$$B^{'}(even,j) = D_2^{'}(i,j) \quad (38)$$

$$C^{'}(i,j) = C^{'}(odd,j) \oplus C^{'}(even,j) \quad (39)$$

$$C^{'}(odd,j) = B_1^{'}(i,j) \quad (40)$$

$$C^{'}(even,j) = C_1^{'}(i,j) \quad (41)$$

$$D^{'}(i,j) = D^{'}(odd,j) \oplus D^{'}(even,j) \quad (42)$$

$$D^{'}(odd,j) = B_2^{'}(i,j) \quad (43)$$

$$D^{'}(even,j) = C_2^{'}(i,j) \quad (44)$$

$$E_{12}(i,j) = A_1^{'}(i,j) \oplus A_2^{'}(i,j) \oplus B_1^{'}(i,j) \oplus B_2^{'}(i,j) \oplus C_1^{'}(i,j) \oplus C_2^{'}(i,j) \oplus D_1^{'}(i,j) \oplus D_2^{'}(i,j) \quad (45)$$

2.2.2. Inverse Pixel Process for Reconstructing the Binary Input Image

Here, reference matrix Figures 2 and 3 are considered and a single pixel value from main matrix is not taken instead of taking two input matrixes. From every input matrix, two column values are compared with Figure 2 and 3 matrixes. If those pixel values are equal, then the relevant pixel value will be placed in one matrix. The combination of the input matrix is given in the Equations 46-49. Here, the output of the segregation process is the input and also the N subbands are converted in to N/2. For example, the eight subbands which are produced by the segregation process is converted into the four subbands.

$$[A_1^{'}(i,j) \oplus A_2^{'}(i,j)] \nabla \prod_{1=[i,j]}^{0=[i,j]} M = \Theta R^{'}1C^{'}18bit(i,j) \quad (46)$$

$$[B_1^{'}(i,j) \oplus B_2^{'}(i,j)] \nabla \prod_{1=[i,j]}^{0=[i,j]} M = \Theta R^{'}1C^{'}28bit(i,j) \quad (47)$$

$$[C_1^{'}(i,j) \oplus C_2^{'}(i,j)] \nabla \prod_{1=[i,j]}^{0=[i,j]} M = \Theta R^{'}2C^{'}18bit(i,j) \quad (48)$$

$$[D_1^{'}(i,j) \oplus D_2^{'}(i,j)] \nabla \prod_{1=[i,j]}^{0=[i,j]} M = \Theta R^{'}2C^{'}28bit(i,j) \quad (49)$$

2.2.3. Converting into decimal value from 8-bit binary value

In this conversion process, the 8-bit value is converted into corresponding decimal value. The inverse pixel process output is the input for converting this process and in this process the input matrix each 8 bit value is taken for processing and it will be converted into the relevant decimal value. Due to this process, the image size is reduced automatically [16-18] .The combination of this process has been declared in the Equations 50 to 54.

$$R^{'}1C^{'}18bit(i,j) = R^{'}1C^{'}1Dec(i,j) \quad (50)$$

$$R^{'}1C^{'}28bit(i,j) = R^{'}1C^{'}2Dec(i,j) \quad (51)$$

Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$R'2C'18bit(i,j) = R'2C'1Dec(i,j) \quad (52)$$

$$R'2C'28bit(i,j) = R'2C'2Dec(i,j) \quad (53)$$

$$E_{12}(i;j) = R'1C'1Dec(i,j) \oplus R'1C'2Dec(i,j) \oplus R'2C'1Dec(i,j) \oplus R'2C'2Dec(i,j) \quad (54)$$

This output subbands are input for the next level of Amalgamate Process. These four subbands are merged based on the combinations [8-9].

2.2.4. Generating the Original Image by Amalgamate Process

In this section, the reverse of the splitting process is followed and is discussed in the above section. The amalgamate process is based on the Equation 55. Both $R'1C'1, R'1C'2$ subbands are taken as the first combination [14], the column values are placed in odd column basis in the matrix of $R'1(i,j)$. In detail, the first column of $R'1C'1$ are placed in first column of output matrix $R'1(i,j)$. Similarly, the second column of the $R'1C'1$ is placed in third position (column) of output matrix $R'1(i,j)$, remaining columns of $R'1C'1$ are placed in odd position of output matrix $R'1(i,j)$. In the same way, $R'1C'2$ columns are placed in the even

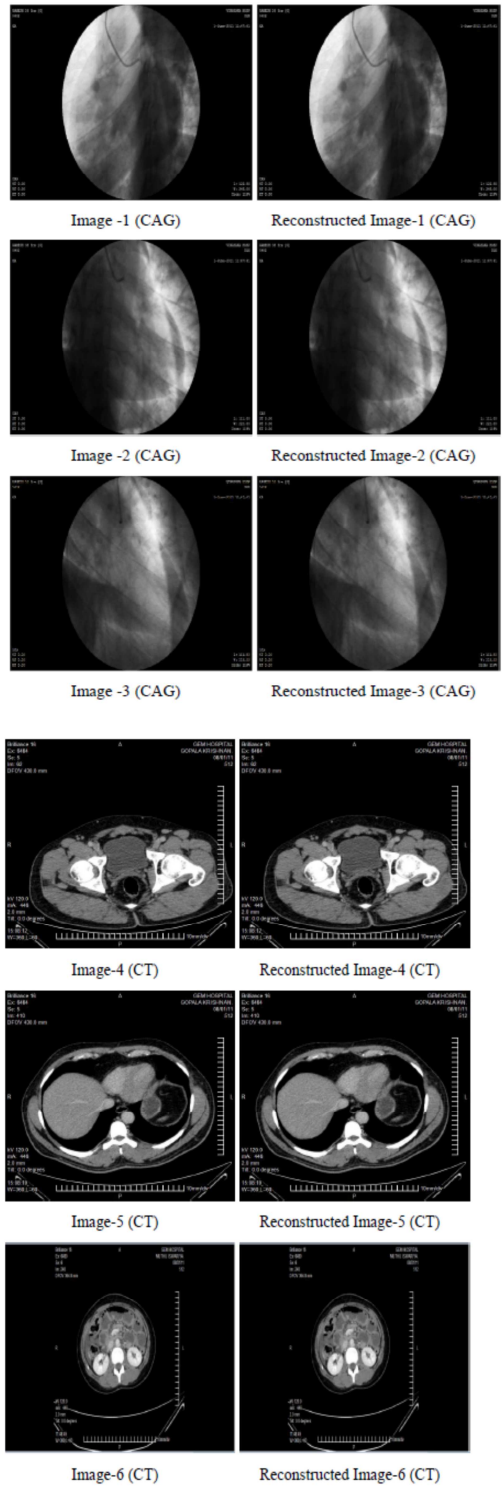

Figure 7 (a) Input and reconstructed grayscale medical images

Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

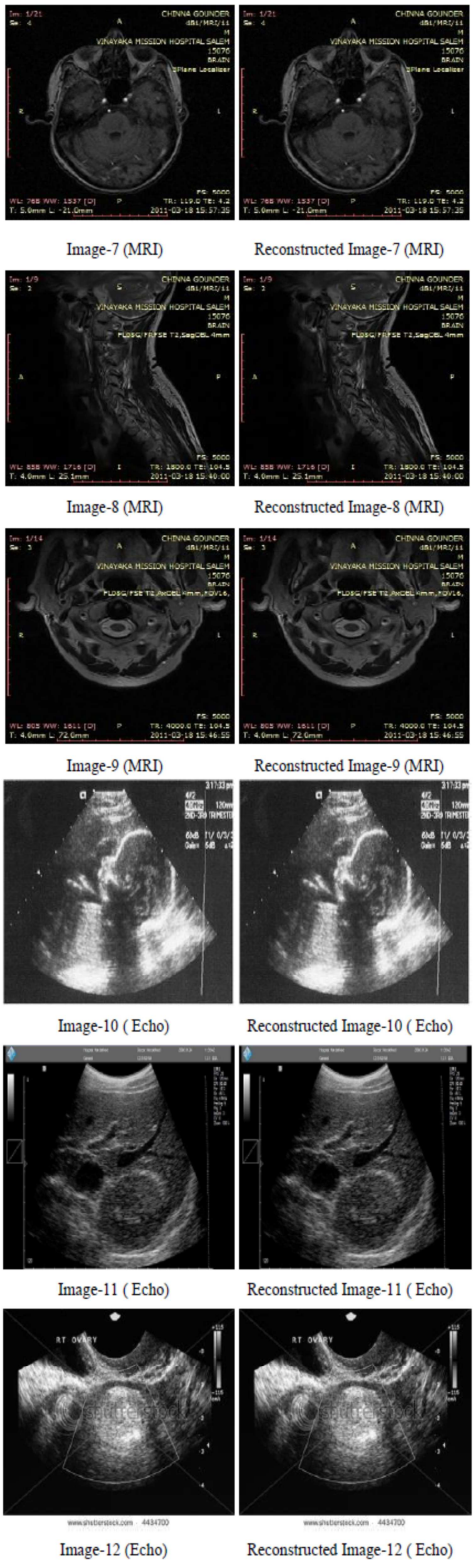

Figure 7 (b) Input and reconstructed grayscale medical images

position of output matrix $R'1(i,j)$. The next level combination [15] is $R'2C'1$ and $R'2C'2$, here the same procedure has been followed as illustrated in the Equation 56. $R'2C'1$ subband columns values are placed in the odd position of output matrix $R'2(i,j)$. Similarly, $R'2C'2$ subband columns values are placed in the even position of output matrix $R'2(i,j)$. Finally, the $R'1(i,j)$ and $R'2(i,j)$ subbands are considered, the $R'1(i,j)$ rows values are placed in the odd position of final output subband $\Theta m'(i,j)$, in the continuous manner

$R'2(i,j)$ rows values are placed in even position of $\Theta m'(i,j)$. This $\Theta m'(i,j)$ subband is called as the reconstructed medical image. The process combination has been given in the Equations 3.55-3.57.

$$R'1C'1Dec(i,j) \oplus R'1C'2Dec(i,j) = R'1(i,j) \quad (55)$$

$$R'2C'1Dec(i,j) \oplus R'2C'2Dec(i,j) = R'2(i,j) \quad (56)$$

$$R'1(i,j) \oplus R'2(i,j) = \Theta m'(i,j) \quad (57)$$

The reconstructed original grayscale medical image $\Theta m'(i,j)$ comparable with existing algorithm is more efficient and accurate. In order to find the error from reconstructed information plenty of error matrixes will be availed [14]. Among all, in this experimentation CC is chosen for checking the CIA properties. The next section discusses about the result analysis for the proposed system.

3. EXPERIMENTED RESULTS

Whenever the security issue is considered, mainly three things have to be concentrated on Confidentiality, Integrity and Availability. What important roles do these properties play in the security side? This is an important question one has to think about. While transmitting data or any kinds of information from one user to another, whether or not it has reached successfully to the right person, such things are defined by the confidentiality and

Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

availability. To check whether the particular user received the correct information which was sent by the sender, to measure these kinds of details integrity plays a vital role. In this case, while transferring the medical image in secure manners there are many crypto systems that are available in this hi-tech world. Among the existing crypto systems, the proposed system TVC is one of the most powerful systems [6]. With respect to the drawbacks of the existing systems, the proposed system has been enhanced to reduce these problems and comply with the CIA properties. To achieve the confidentiality, the original image is encrypted, viewing the encrypted image, the actual medical image cannot be predicted, as represented in Figure 6. Also, to achieve the authentication and integrity, the receiver, the one who is going to reconstruct the original grayscale medical image, that person will only be able to retrieve the actual information whereas rest of the people or unauthorized persons cannot do so.

In the proposed scheme, authentication is highly achieved. To check the integrity of the received file, one of the powerful error matrix correlation coefficient has been measured. Nearly, 1000 grayscale medical images have been tested for experimental results, but for this documentation, only 18 various grayscale medical images have been provided. In Figure 7, the 18 grayscale medical images and reconstructed images have been shown [18].

3.1. Testing

After the input grayscale medical image has been received, it has been tested for CIA properties using correlation coefficient. Using these kinds of tests, the fake image can be identified easily. Thus in order to authenticate the reconstructed image, the reconstructed image is compared with the original image using correlation coefficient method.

Correlation is a method of identifying the degree of relationship between two sets of values. The correlation coefficient is calculated using the formula given in Equation 58.

$$\ell_{xy} = \frac{E(XY) - \mu_{xy}}{\sigma_x \sigma_y} \quad (58)$$

Here, E is the expected value operator, X is the mean and Y is the standard deviation. The value of correlation coefficient ranges from -1 to +1 and if the value obtained is -1, then the images are inversely related. If it is 0, then they are independent. So, if the value is more or less +1, it can be concluded that the input image and the output image are same and CIA can be granted.

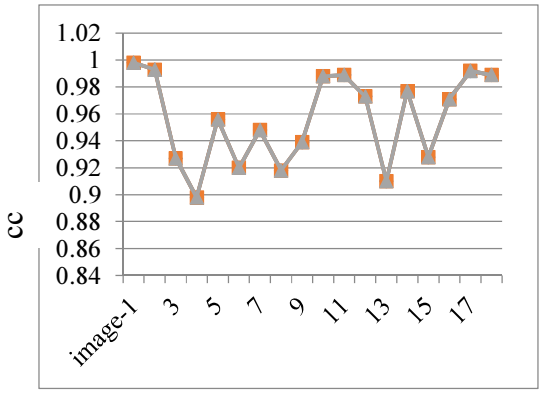

Figure 8 CC Measurements

From the Figure 8 and Table 1 it is clearly stated that, the proposed TVCS gives the better performance in terms of measuring the CC. When the CC values are near to 1, the reconstructed information is perfect original replica. Based on this point, in Table 3.2 information given by the TVCS are from 0.9 to 1. While reconstructing the original information from the encrypted information by VCS, the original secret information can be able to understand but unable to reconstruct the exact information, but TVCS provides the exact information after the decryption process. Image-1 correlation coefficient value is 0.998, which is given in the Table 1 is the evidence of the algorithm performance, not only one images for all

Table 1 CC result analysis for the proposed system

Images	CC	Images	CC
Image-1(CAG)	0.998	Image-10(Echo)	0.988
Image-2(CAG)	0.993	Image-11(Echo)	0.989
Image-3(CAG)	0.927	Image-12(Echo)	0.973
Image-4(CT)	0.898	Image-13(US)	0.910
Image-5(CT)	0.956	Image-14(US)	0.977
Image-6(CT)	0.920	Image-15(US)	0.928
Image-7(MRI)	0.948	Image-16(X-Ray)	0.971
Image-8(MRI)	0.918	Image-17(X-Ray)	0.992
Image-9(MRI)	0.939	Image-18(X-Ray)	0.989

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

image the proposed TVCS has provided the enhanced results.

4. CONCLUSION

Eventually, for every encryption or decryption process to perform better, the existing algorithm depends on post processing or preprocessing methods. But the proposed algorithm here gives a solution where post and pre processing methods need not be used. The result obtained by using the proposed algorithm while calculating the Correlation and Coefficient (CC) is extraordinary. The brief discussion of the proposed system results has been adopted in the result analysis chapter. In Figure 8, the correlation coefficient result of the proposed system has been represented by means of a graph. The formula of CC states that, if the value is more or less to one, then the output of the image which the system has reconstructed is as equal to the input image. From the experiment, proposed system results are between 0.89 and 0.99. Therefore, it is concluded that the proposed system has achieved confidentiality, integrity and authentication.

REFERENCES

[1] Fang .W.P and Lin .J.C , "Visual cryptography with extra ability of hiding confidential data", Journal of Electronic Imaging, Vol.15, pp.0230201-0230207, 2006.

[2] Feng Liu and Chuankun Wu, "Embedded Extended Visual Cryptography Schemes", IEEE Trans. Information Forensics and Security, Vol.6, pp.307-322, 2011.

[3] Feng Liu., *et. al.*, "Step Construction of Visual Cryptography Schemes", IEEE Trans. Information Forensics and Security, Vol.5, pp.27-38, 2010.

[4] InKoo Kang., *et. al.*, "Color Extended Visual Cryptography Using Error Diffusion", IEEE Trans. Image rocessing, Vol.20, pp.132-145, 2011.

[5] Jong-Yun Kim., *et. al.*, "Optical image encryption using interferometry-based phase masks", IEEE Electronics Letters, Vol.36, pp.874-875, 2000.

[6] Liu .F., *et. al.*, "Cheating immune visual cryptography scheme", IEEE Trans. Information Security, Vol.5, pp.51-59, 2011.

[7] Lukac .R and Plataniotis .K.N , "Colour image secret sharing", IEEE Electronics Letters, Vol.40, pp.529-531, 2004.

[8] Lukac .R and Plataniotis .K.N , "Digital image indexing using secret sharing schemes: a unified framework for single-sensor consumer electronics", IEEE Trans. Consumer Electronics, Vol.51, pp.908-916, 2005.

[9] Martin .K., *et. al.* , "A Biometric Encryption System for the Self-Exclusion Scenario of Face Recognition", IEEE Systems Journal, Vol.8, pp.440- 450, 2009.

[10] Naor .M and Shamir .A , "Visual Cryptography, Advances in Cryptology: Eurpocrypt'94", Lecture Notes in Computer Science,Springer Verlag, Germany, Vol.950, pp.1-12,1995.

[11] O'Gorman .L and Rabinovich .I, "Secure identification documents via pattern recognition and public-key cryptography", IEEE Trans. Pattern Analysis and Machine Intelligence, Vol.20, pp.1097-1102, 1998.

[12] Qiu-Hua Lin and Fu-Liang Yin , "Blind source separation applied to image cryptosystems with dual encryption", IEEE Electronics Letters, Vol.38, pp.1092-1094, 2002.

[13] Stinson .D (1999), "Visual cryptography and threshold schemes", IEEE Trans. Potentials, Vol.18, pp.13-16.

[14] Manimurugan, S., Porkumaran, K.,"A New Fast and Efficient Visual Cryptography Scheme for Medical Image with Forgery Detection", Proceedings of 2011 International Conference on Emerging Trends In Electrical And Computer Technology (ICETECT 2011),pp 594-599,23rd&24th March 2011.

[15] S.Manimurugan, Dr.K.Porkumaran," Tailored Visual Cryptography Scheme for Gray Scale Image", IEEE International Conferences on ICSAP 2011, February 26-28, 2011, Singapore.

[16] S.Manimurugan, Dr.K.Porkumaran," A New Visual Cryptography Scheme for GrayScale Medical Image", 2011 International Conference on Communication and Electronics Information (ICCEI 2011), Vol-1 ,pp 336-340,February 22-24, 2011, Haikou, China.

[17] S.Manimurugan, and Porkumaran,K.,"Secure Medical Image Compression Using Block Pixel Sort Algorithm", European Jour. Scientific Research, Vol. 56, pp.129-138, Jul. 2011.

[18] S.Manimurugan, and Porkumaran,K., "Fast and Efficient Secure Medical Image Compression Schemes", European Jour. Scientific Research, Vol. 56, No.2, pp.139-150, Jul. 2011.