# Medical Image Watermarking System for Integrity Control With Data Repair Capability

Rakhi.R

**Abstract.** Enforcing protection of medical content becomes a major issue of computer security. Since medical contents are more and more widely distributed, it is necessary to develop security mechanisms to guarantee their confidentiality and integrity. In this context, watermarking and cryptographic hashes has been proposed as a complementary mechanism for medical data protection. The proposed system aims at verifying the integrity of medical images and repairs the data if any tampering occurred in the image. In the proposed method signatures extracted from different pixel blocks of interest are embedded on RONI and are compared with recomputed ones at the verification stage. A set of three signatures are proposed. The first two signatures are based on cryptographic hashes and checksums and are devoted to detection and identification of modification location. The third one is issued from image moment theory that can be used to approximate any local modification by its nearest generalized 2-D Gaussian. For repairing the tampered blocks an authentication method based on the use of (k,n) threshold secret sharing technique is used. An authentication signal is generated for each pixel block, which is transformed into several shares using the (k,n) threshold secret sharing scheme and embedded into the alpha channel plane. The alpha channel plane is then combined with the original image to form a PNG image. In the process of image authentication, an image is marked as tampered if the authentication signal computed from the current block does not match with that extracted from the shares embedded in the alpha channel plane and then data repairing is applied to each tampered block.

**Index Terms—** Cryptographic Hash, Discrete Wavelet Transform, Geometric moments, Integrity control, Medical imaging ,Secret sharing, Watermarking.

---

## 1. INTRODUCTION

Nowadays, protection of healthcare information against unauthorized access becomes a major concern. Due to the advancement in information technology and the wide distribution of medical content, a new security mechanism that guarantee the integrity(ensure image has not been modified by an unauthorized person), authenticity[1](asserts its origin and attachment to one patient) and confidentiality(limits access to information) of the medical content is necessary. Recently, cryptographic signatures and watermarking methods are proposed as a security mechanism for the protection of medical data.

While it is important to keep the medical images secure from any kind of modification, it is as much important to detect when an image has been modified and in which manner it is modified. Medical images can be modified accidently during their transmission or deliberately by the addition or removal of lesions[2].

Medical image integrity verification[3] is an analysis process that focus on three main things: Whether the image identical to its original version? If not, which parts can still be used trustfully for diagnosis purpose? Finally, what is the objective if any of the image tamper? To answer these questions three distinct levels of integrity can be associated :

- Level 1(L1): Modification Detection - Verifies whether the image is modified or not.
- Level 2(L2): Modification Location - Locates untrustworthy parts of the image.
- Level 3(L3): Forensics Analysis - Nature of modification within untrustworthy parts of the image has to be identified.

The proposed system also includes an additional level

- Level 4(L4) : Data Repairing - Repair the original image if any altering is occurred.

———————————————————
• Rakhi R currently pursuing M.Tech Degree in Computer Science and Information technology from FISAT, Angamaly, Kerala, India
• E-mail: rakhirajk20@gmail.com

## 2. LITERATURE SURVEY

For verifying the integrity of medical images different strategies have been proposed, which includes signatures/hashes[4][5], watermarking[6] and blind forensic methods[7].

### 2.1. Signature Based Method

This method verifies the image integrity by comparing the hashes computed over the image under investigation with those extracted from the image. Cryptographic hashes verifies the exact identity of the image under investigation with the

original one and can be used to achieve L1. Also they provide best detection performance and are extremely difficult to counterfeit.

Inorder to localize modification, hashes needs to be computed over independent image areas. H.Yang et al[8] proposed a two layer binary image authentication scheme with tampering localization, by embedding signature and block identifier. In this scheme the first layer targets the overall authentication by hiding the cryptographic signature of the image and second layer identifies the tampering location. For that the image is partitioned into multiple macro-blocks and subsequently they are classified into 8 categories. For each class a block identifier is defined and signatures are embedded in those qualified and self detecting macro-blocks.

### 2.2. Watermarking Based Method

Watermarking is an effective tool proposed to increase medical image security, authenticity and integrity. One common method involves inserting a specific watermark in the image and its non detection at the verification stage informs about the loss of integrity.

Gouenou Coatrieux et al.[9] proposed an approach to image integrity verification using watermarking, where the protection zone is separated from the insertion zone to avoid compromising any diagnostic capability. In this scheme, the medical image to be protected is divided into two zones, ROI and RONI whose integrity need not to be preserved and serves as the watermarking carrier. To achieve strict integrity control, signatures are extracted from ROI and are embedded in the insertion zone. So at the verification stage, any image for which signature extracted from protection zone does not match with that stored in the insertion zone is declared invalid. Thus any change whether due to malicious forging, tampering will give an indication of integrity loss. This scheme uses checksum instead of cryptographic hashes, so they are less efficient in terms of detection.

In some cases, watermarking is combined with image signatures[10]. For eg, a set of signatures are computed from one region of interest and are then watermarked within RONI. Gouenou Coatrieux et al. proposed a reversible watermarking method for knowledge digest embedding and reliability control in medical image. Inorder to improve the medical image sharing in e-learning applications, they have to make the image more usable, by watermarking it with a digest of its associated knowledge. The aim of such a KD is to retrieve similar images with same findings or differential diagnosis. Instead of modifying the image file format by adding some extra header information, watermarking is used to embed the KD in the pixel gray level values of the corresponding image. When it is shared through open networks, watermarking also helps to convey the integrity and authenticity of an image and its KD. This method minimizes image distortion, but message and exact image recovery is possible only if watermarked image has not been modified, since the watermark is fragile.

Jasni Mohammed Zain et al.[11] proposed a watermarking scheme that can recover original image from the watermarked one. This scheme is used to verify the integrity and authenticity of DICOM images. For that, the image pixels are arranged as string, then hash function is applied. SHA-256 of the whole image is embedded in the LSB of the RONI. If the image has not been modified watermark will be extracted and the original image will be recovered. SHA-256 of the recovered image will be compared with the extracted watermark for authentication. This scheme is only possible for images that has an area of known constant, ie, for an ultrasound image, the embedding region is normally a dark region with pixel value '0'.

### 2.3. Blind Forensics Method

These techniques do not require any image prior. They aim at identifying the evidences that are left by most image modifications. Blind forensic methods are based on classifier based mechanism, which uses image features that reveal the statistical nature of image modifications as input. Most of these solutions discriminates non modified images from those that have been processed.

Ismail Avcibas et al.[12] proposed a framework for digital image forensics. They aim at designing a feature based classifier that can discriminate original and doctored images. These measurements are used as features in the classifier based design. Using these classifiers they test whether a suspicious part of a given image has been processed with a particular method or not.

## 3. PROPOSED SYSTEM

The basic system structure is depicted in Fig.3.1 and Fig.3.2. At the protection stage, a signature is extracted from the ROI of the image and is embedded into the RONI. At the verification stage, differences between extracted and recomputed signatures are compared, inorder to achieve the three integrity levels: L1, L2 and L3. For each integrity level there will be one specific and independent signature. More clearly, Li is based on one signature $H_i$, which means the ROI signature H will be the concatenation of the signature $H_i$, i=1,2,3. So at the verification stage if both the extracted and recomputed signatures are matched(means no tampering occurred), then the image is authentic, otherwise data repairing(L4) is performed. For embedding the signatures, the proposed method decompose the image to be watermarked using discrete wavelet transform(Haar). A discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. The decomposition process will produce an approximation image and a sequence of detail

images, which corresponds to horizontal, vertical and diagonal details. Then the watermark bits are embedded into the detail coefficients and the watermarked image is produced by the corresponding inverse wavelet transform.

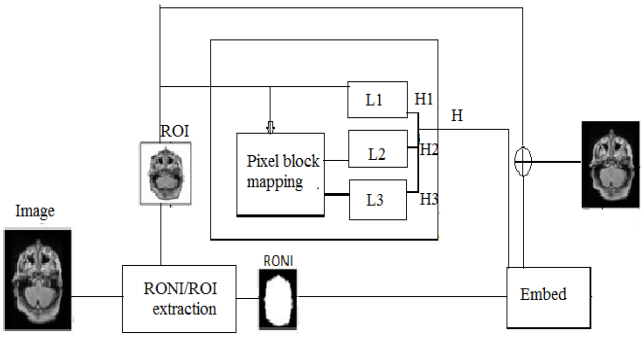


Fig.3.1 Protection Stage

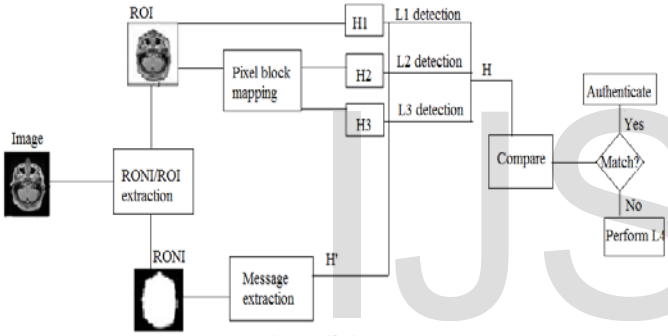


Fig. 3.2 Verification Stage

### 3.1. Detecting(L1) and Localizing(L2) Image Modifications

To achieve L1, ROI is considered as a binary message. Then SHA-1 is applied which yields a 160 bit signature $H_1$ .The cryptographic hash functions provide best detection performance and have specific properties like dispersion property which ensures that two slightly different ROIs have very different signatures[4].

Inorder to identify which parts of the image can still be interpreted without the risk of misdiagnosis, a set of signatures from different parts of the ROI is computed; ie, ROI is divided into several sub-blocks and each block is independently protected by one signature. At the verification stage, one block $B_i$ is said to be tampered if its recomputed signature differs from the extracted one. Here hamming codes[9] are used for the purpose of computing signatures. Thus based on $H_1$ and $H_2$, it is possible to know if the image has been altered and which pixel blocks cannot be used trustingly.

### 3.2. L3 Signature

L3 signature corresponds to digital forensics analysis, the purpose of which is to identify the nature of modification. Similar to L2 analysis, L3 analysis is also conducted independently on each pixel block. Two kinds of modification are there: local and global image modifications, ie, if at the output of L2, only some blocks are non authentic then it is local modification, otherwise the modification is global. If the image is modified locally, then it aims to identify some insights regarding the modification(its position within the block that is claimed as non authentic at the output of L2 and its dimension). For that purpose, the modification model is approximated by its nearest generalized 2-D Guassian defined as

$$G_{r0,c0}^{A,\sigma_1,\sigma_2}(c',r') = Ae^{-\left(\frac{(c'-c_0')^2}{2\sigma_1^2}+\frac{(r'-r_0')^2}{2\sigma_2^2}\right)} \quad (1)$$

where $c' = c\cdot\cos\theta + r\cdot\sin\theta$ and $r' = c\cdot\cos\theta - r\cdot\sin\theta$.

The purpose of L3 analysis is to determine the parameters of the modification model so as to make it the nearest as possible of the real local tamper $\Delta$. The parameters are its center of mass, identified by its row and column positions( $r_0, c_0$ ), the direction of the major axis( $\theta$ ), the deviation( $\sigma_1$ and $\sigma_2$ ) along the major axis and minor axis and the amplitude (A). The L3 signature is computed as a concatenation of six digests $d_u^i$, u=1,...,6, each derived from block $B_i$, by means of a digest function $g_u$ built considering the following properties:

- $g_u$ should be easy to compute.
- $g_u$ should be a linear function, so the digest associated to the modification $\Delta$ can be achieved easily: $g_u(\Delta) = g_u(B_i') - g_u(B_i)$
- $g_u$ should be proportional to the parameters to be estimated.

The proposed digest function $g_u$ is based on image geometric moments. The geometric moments of an image intensity function f(r,c) are defined by[13]

$$M_{nm} = \sum_r^N \sum_c^N r^n c^m f(r,c), \quad \text{n, m=0,1,2.....} \quad (2)$$

The parameters of the generalized 2-D Gaussian function defined on a pixel block can be estimated from its geometric moments as follows:

1) The Gaussian center of mass $(r_0, c_0)$ can be derived from the two first-order moments $(M_{01}, M_{10})$:

$$r_0 = M_{10}/M_{00}\ ,\ c_0 = M_{01}/M_{00} \tag{3}$$

.

2) The direction of the major axis($\theta$), as well as the axis lengths of the Gaussian basis a and b can be estimated by

$$a = \left\{ \frac{2\left[\mu_{20} + \mu_{02} + \sqrt{(\mu_{20} - \mu_{02})^2 + 4\mu_{11}^2}\right]}{\mu_{00}} \right\}^{1/2} \tag{4}$$

$$b = \left\{ \frac{2\left[\mu_{20} + \mu_{02} - \sqrt{(\mu_{20} - \mu_{02})^2 + 4\mu_{11}^2}\right]}{\mu_{00}} \right\}^{1/2} \tag{5}$$

$$\theta = \frac{1}{2}\tan^{-1}\left(\frac{2\mu_{11}}{\mu_{20} - \mu_{02}}\right) \tag{6}$$

$\mu_{nm}$ can be derived from the corresponding geometric moment[14] $M_{nm}$ as

$$\begin{aligned} \mu_{00} &= M_{00} \\ \mu_{10} &= \mu_{01} = 0 \\ \mu_{20} &= M_{20} - r_0 M_{10} \\ \mu_{02} &= M_{02} - c_0 M_{01} \\ \mu_{11} &= M_{11} - c_0 M_{10} \end{aligned} \tag{7}$$

Once the position and the basis ellipse of the Gaussian are estimated, the amplitude of the Gaussian function can be derived from the following relation:

$$M_{00}(G) = A\sum_{r'=1}^{N}\sum_{c'=1}^{N} e^{-\left(\frac{r'-r_0'}{2\sigma_1^2}\right)^2 + \left(\frac{c'-c_0'}{2\sigma_2^2}\right)^2} \tag{8}$$

So for one pixel block Bi, L3 protection and verification processes are achieved in the following way:

1) Integrity protection stage
   a) Compute
   $h_3^i = [g_1(B_i), g_2(B_i), g_{31}(B_i), g_4(B_i), g_5(B_i), g_6(B_i)]$
   $= [M_{00}^{B_i'}, M_{10}^{B_i'}, M_{01}^{B_i'}, M_{11}^{B_i'}, M_{02}^{B_i'}, M_{20}^{B_i'}]$
   b) Embed $h_3^i$ along with other signatures in the RONI

2) Integrity verification stage
   a) Compute the L3-signature of the observed block $B_i'$:
   $h_3^{i'} = [M_{00}^{B_i'}, M_{10}^{B_i'}, M_{01}^{B_i'}, M_{11}, M_{02}^{B_i'}, M_{20}^{B_i'}]$
   b) Compute the geometric moments of the modification $\Delta: h_3^{\Delta} = h_3^{i'} - h_3^i$
   $= [M_{00}^{\Delta}, M_{10}, M_{01}^{\Delta}, M_{11}^{\Delta}, M_{02}^{\Delta}, M_{20}^{\Delta}]$
   c) Compute the parameters of the nearest generalized 2-D Guassian function.

### 3.3. Data Repairing

In this level, a PNG image is created from the original image I with an alpha channel plane. Next data for authentication and repairing are computed from the input image and taken as input to (k,n) threshold scheme. Then the share values are mapped subsequently into a small range of alpha channel values and the mapped secret shares are randomly embedded into the alpha channel. The block diagrams describing this level are depicted in Fig. 3.4 and Fig.3.5.

#### 3.3.1. Generation of Stego Image

Inorder to generate a stego image, first the input image I is converted into binary form, so that it yields a binary version $I_b$. Then the image I is transformed into a PNG image with an alpha channel plane $I_\alpha$. Take in raster scan order a

IJSER

$4\times5$ block $B_b$ of $I_b$ with pixels $p_1,....,p_{20}$ and generate the authentication signal. Then generate partial shares from the authentication signal using (k,n) threshold scheme. Add 238 to each of the shares, resulting in the new values which fall in the nearly total transparency range of 238 through 254 in the alpha channel plane. Embed the first four partial shares in the first 16 pixels of $B_\alpha$ and the remaining shares in randomly selected pixels outside $B_\alpha$ using the key K.

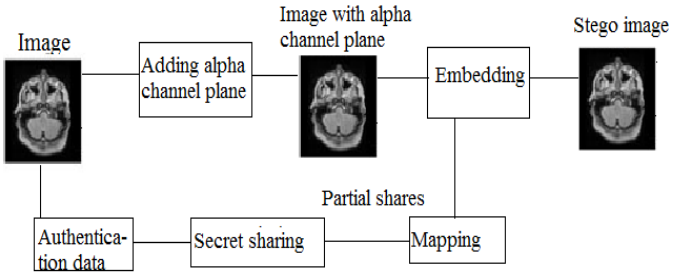


Fig. 3.3 Generation of Stego Image

### 3.3.2. Repairing of Original Image

For repairing the image first convert the stego image into binary form, that yields a binary version denoted as $I_b$ .Take in a raster scan order an unprocessed block $B_b^{'}$ from $I_b^{'}$ with pixel values $p_1$ through $p_{20}$ and find the twenty pixel values from the corresponding block $B_\alpha^{'}$ in the alpha channel plane. Substract 238 from each of the pixel values and obtain the corresponding shares. From these shares obtain the secret and and compare it with the pixel values of the corresponding block $B_b^{'}$ from $I_b^{'}$ and if any mismatch occurs mark $B_b^{'}$, the corresponding block $B^{'}$ and all partial shares as tampered. Inorder to collect the remaining shares, use the key K and collect the four pixels in $I_\alpha^{'}$ in the same order as they were randomly selected for $B_b^{'}$ and subtract 238 from each of the values and obtain the corresponding shares. Inorder to repair the image select the four shares that are not marked as tampered from the block $B_b^{'}$ in $I_b^{'}$ corresponding to $B^{'}$ and using these shares as input perform the recovery procedure of the thresold sheme and obtain the secret. Use this secret to repair the tampered pixel values and obtain the repaired image $I_r$ .

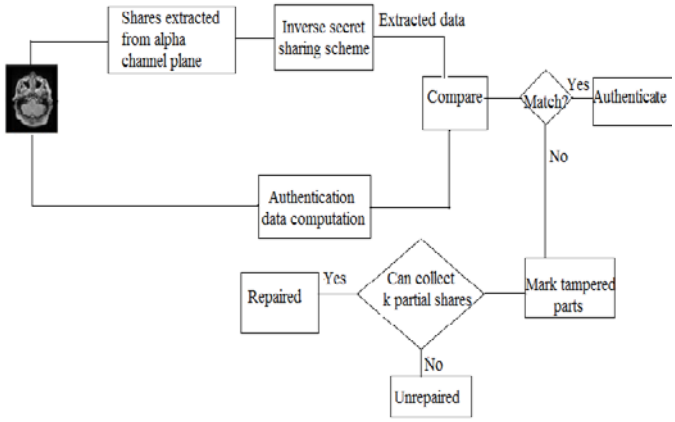


Fig. 3.4 Repairing of Medical Image

### 3.3.3. (k,n) Threshold Secret Sharing Scheme

This scheme enables to make n shares and recover the secret from k or more shares using XOR operations, for arbitrary threshold k and the no of participants n. The distribution algorithm and the recovery algorithm are depicted below:

Table 3. Algorithm of the Function $MAT()$

**INPUT** : $t_0, t_1, \ldots, t_{k-1}$
**OUTPUT** : M

1: for $i \leftarrow 0$ to $k-1$ do
2: for $j \leftarrow 0$ to $n_p - 2$ do
3: $\mathrm{v}_{(t_i,j)} \leftarrow VEC(t_i, j) = \left[\mathrm{i}_j^{n_p-1}\ \mathrm{i}_{t_i+j}^{n_p}\ \mathrm{i}_{2t_i+j}^{n_p}\ \ldots\ \mathrm{i}_{(k-2)t_i+j}^{n_p}\ \mathrm{i}_{j-t_i-1}^{n_p-1}\right]$
4: end for
5: end for
6: $\mathrm{G} \leftarrow (\mathrm{v}_{(t_0,0)}, \ldots, \mathrm{v}_{(t_{k-1},n_p-2)})^{\mathrm{T}}$
7: $\begin{bmatrix} \mathrm{G}_2 & \mathrm{G}_1 & \mathrm{J}_1 \\ \emptyset & \mathrm{G}_0 & \mathrm{J}_0 \end{bmatrix} \leftarrow FG\left(\left[\mathrm{G} \quad \mathrm{I}_{k(n_p-1)}\right]\right) = \left[\bar{\mathrm{G}} \quad \mathrm{J}\right]$
8: $\left[\mathrm{I}_{n_p-1} \quad \mathrm{M}\right] \leftarrow BG\left(\left[\mathrm{G}_0 \quad \mathrm{J}_0\right]\right)$
9: return M

IJSER

**Table 1.** Distribution Algorithm of Proposed $(k, n)$-Threshold Scheme

**INPUT** : $s \in \{0,1\}^{d(n_p-1)}$
**OUTPUT** : $(w_0, \ldots, w_{n-1})$

1: $s_0 \leftarrow 0^d$, $s_1 \parallel \cdots \parallel s_{n_p-1} \leftarrow s$
2: **for** $i \leftarrow 0$ to $k-2$ **do**
3: **for** $j \leftarrow 0$ to $n_p - 1$ **do**
4: $r_j^i \leftarrow GEN(\{0,1\}^d)$
5: **end for**
6: **end for** (discard $r_{n_p-1}^0$)
7: **for** $i \leftarrow 0$ to $n-1$ **do**
8: **for** $j \leftarrow 0$ to $n_p - 2$ **do**
9: $w_{(i,j)} \leftarrow \left(\bigoplus_{h=0}^{k-2} r_{h \cdot i+j}^h\right) \oplus s_{j-i}$
10: **end for**
11: $w_i \leftarrow w_{(i,0)} \parallel \cdots \parallel w_{(i,n_p-2)}$
12: **end for**
13: **return** $(w_0, \ldots, w_{n-1})$

To make shares 3 steps are required. First the distristribution algorithm divides the secret $s \in \{0,1\}^{d(n_p-1)}$ into $n_p - 1$ pieces of d-bit sequence $s_1,...,s_{n_p-1} \in \{0,1\}^d$ equally at line 1, where $s_0$ denotes a d-bit zero sequence. Next at lines 2 - 6 $(k-1)n_p - 1$ pieces of d bit random numbers $r_0^0 ....r_{n_p-1}^{k-2}$ are chosen from $\{0,1\}^d$ independently from each other, where GEN( $\chi$ )denotes a function to generate an ( $\log_2|\chi|$ )- bit random no from a finite $\chi$ . At lines 7 - 12 ,algorithm makes pieces of shares by means of the following equation:

$$w_{(i,j)} = \left\{\bigoplus_{h=0}^{k-2} r_{h.i+j}^h\right\} \oplus s_{j-i} \qquad (9)$$

where $0 \le i \le n-1, 0 \le j \le n_p - 2$ . Finally these pieces are concatenated and shares $w_i = w_{(i,0)} \| \ldots \| w_{(i,n_p-2)}$ are constructed.

**Table 2.** Recovery Algorithm of Proposed $(k, n)$-Threshold Scheme

**INPUT** : $(w_{t_0}, w_{t_1}, \ldots, w_{t_{k-1}})$
**OUTPUT** : $s$

1: **for** $i \leftarrow 0$ to $k-1$ **do**
2: $w_{(t_i,0)} \parallel \cdots \parallel w_{(t_i,n_p-2)} \leftarrow w_{t_i}$
3: **end for**
4: $\mathbf{w} \leftarrow (w_{(t_0,0)}, \ldots, w_{(t_0,n_p-2)}, \ldots, w_{(t_{k-1},0)}, \ldots, w_{(t_{k-1},n_p-2)})^{\mathrm{T}}$
5: $\mathbf{M} \leftarrow MAT(t_0, \ldots, t_{k-1})$
6: $(s_1, \ldots, s_{n_p-1})^{\mathrm{T}} \leftarrow \mathbf{M} \cdot \mathbf{w}$
7: $s \leftarrow s_1 \parallel \cdots \parallel s_{n_p-1}$
8: **return** $s$

In the recovery procedure, first, each share is divided into d-bit pieces at lines 1 - 3. Next, at line 4, $k(n_p - 1)$ dimensional vector w is generated, which is a vector of divided pieces of shares. At line 5, $k(n_p - 1) \times k(n_p - 1)$ binary matrix M is obtained by the function MAT(). All divided pieces of the secret, $s_1,...,s_{(n_p-1)}$ are recovered by calculating M.w at line 6. Finally the secret s is recovered by concatenating $s_1,...,s_{(n_p-1)}$ at line 7.

In MAT function, first a ( $kn_p - 2$ )- dimensional binary vector $v_{(t_i,j)}$ is obtained from indexes $t_i$ and j at lines 1 - 5. VEC() denotes the function to make $v_{(t_i,j)}$ , where $i_y^x$ denotes a x- dimentional binary row vector such that the only y-th element equals one ( $0 \le y \le x-1$ ) and the others are zero. $v_{(t_i,j)}$ is defined as the generator vector of $w_{(t_i,j)}$ , i.e, $w_{(t_i,j)} = v_{(t_i,j)}.e$ , where e is defined by

$$e = (r_0^0,....r_{n_p-2}^0,.....,r_o^{k-2},...,r_{n_p-1}^{k-2}, s_1,....,s_{n_p-1})^T$$

IJSER

At line 6, the $k(n_p-1)\times(kn_p-2)$ binary matrix G is generated as follows:

$$G=(v_{(t_0,o)},.....v_{(t_0,n_p-2)},.....,v_{(t_{k-1},0)},..,v_{(t_{k-1},n_p-2)})^T$$

which is the generator matrix such that w=G . r. At line 7, the matrix $\left|GI_{k(n_p-1)}\right|$ is generated by column-wise concatenation, and transformed into a row echelon form $\left[\overline{G}\,J\right]=FG(\left[GI_{k(n_p-1)}\right])$ by performing the forward elimination step of Gaussian elimination with the elementary row operations on GF(2),where FG() and $I_{k(n_p-1)}$ denote a forward elimination function and the $k(n_p-1)\times k(n_p-1)$ identity matrix, respectively. Furthermore, $\overline{G}$ and J correpond to the transformed matrices from G and $I_{k(n_p-1)}$ respectively, and $\left[\overline{G}\,J\right]$ is divided into block matrices denoted as follows:

$$\left[\overline{G}\,J\right]=\begin{Vmatrix} G_2 & G_1 & J_0 \\ \phi & G_0 & J_0 \end{Vmatrix}$$

where $G_0$, $G_1$ and $G_2$ are an $(n_p-1)\times(n_p-1)$ block matrix, $(k-1)(n_p-1)\times(n_p-1)$ block matrix and $(k-1)(n_p-1)\times(kn_p-n_p-1)$ block matrix, respectively. $J_0$ and $J_1$ are an $(n_p-1)\times k(n_p-1)$ block matrix and a $(k-1)(n_p-1)\times k(n_p-1)$ block matrix, respectively. Then the backward substitution part of Gaussian elimination is executed on $\left[G_0\,J_0\right]$, and the matrix [ $\left[I_{n_p-1}M\right]=BG(\left[G_0\,J_0\right])$ is obtained, where BG() and M denote the function of backward substitution and a transformed matrix from $J_0$ respectively. Finally MAT() outputs M as a matrix to recover $s_1,...,s_{(n_p-1)}$ from divided pieces of shares.

## 4. EXPERIMENTAL RESULT

A comparison of the capabilities of the proposed method with conventional image authentication scheme is shown in table.

Table 4. Comparison of the capabilities of the proposed method with conventional image authentication scheme.

| | Distortion in Stego Image | Tampering Localization Capability | Repair Capability | Distribution of Authenti-cated Image parts | Manipulation of Data Embedding |
|---|---|---|---|---|---|
| Conventional Authentication Method | Yes | Yes | No | Non blank part | Pixel flippability |
| Proposed Method | No | Yes | Yes | Entire Image | Alpha Channel Pixel Replacement |

The conventional image authentication scheme will create distortion in the stego image during the authentication process. ie, Conventional image authentication methods which usually embed authentication signals into the cover image itself will unavoidably cause destruction to the image content to a certain extent. Different from such methods, the proposed method utilizes the pixels' values of the alpha channel for the purpose of image authentication and data repairing, leaving the original image untouched and so causing no distortion to it. More importantly, only the proposed method has the capability of repairing the tampered parts of an authenticated image.

## 5. CONCLUSION

The proposed system is used for verifying the integrity of medical images and for reparing the original image. This system distinguishes four levels of integrity decision: detection, localization, approximation of the image alteration and data recovery. Cryptographic hashes and checksums are used for achieving L1 and L2, which provide best detection performance and dispersion property. For the third level,any malevolent local modifications is approximated by its nearest 2-D generalized Gaussian function whose parameters are derived from the image geometric moments. Finally an authentication scheme with a data repair capability based on secret sharing scheme is used for reparing the tampered image.

The generated authentication signal is transformed into partial shares by a (k,n) threshold secret sharing scheme,

which are then distributed into an alpha channel plane to create a stego-image in the PNG format. The undesired opaque effect visible in the stego-image coming from embedding the partial shares is eliminated by mapping the share values into a small range of alpha channel values near their maximum transparency value of 255.

In the process of image block authentication, a block in the stego-image is regarded as having been tampered, if the computed authentication signal does not match with that extracted from corresponding partial shares in the alpha channel plane. For self-repairing of the content of a tampered block, the recovery procedure of the secret sharing scheme is used to compute the original content of the block from any k untampered shares.

**REFERENCES**

[1]. L. Kobayashi and S. Furuie, "Proposal for DICOM multiframe medical image integrity and authenticity," J. Digital Imag., vol. 22, no. 1, pp. 71- 83, 2009.
[2]. M. T. Madsen, K. S. Berbaum, A. N. Ellingson, B. H. Thompson,B. F. Mullan, and R. T. Caldwell, "A new software tool for removing,storing, and adding abnormalities to medical images for perception research studies,"
[3]. H. Huang, G. Coatrieux, H. Shu, L. Luo, and Ch. Roux, "Blind integrity verification of medical images," IEEE Trans. Inf. Technol. Biomed.
[4]. B. Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C. Hoboken, NJ, USA: Wiley, 1996.
[5]. B. Preneel, "MACs and hash functions: State of the art," Inf. Security Tech. Report
[6]. X. Guo and T. Zhuang, "Lossless watermarking for verifying the integrity of medical images with tamper localization," J. Digital Imag..
[7]. H. Farid, "Image forgery detection," IEEE Signal Process. Mag., vol. 26, no. 2, pp. 16-25, Mar. 2009.
[8]. H. Yang and A. C. Kot, "Binary image authentication with tampering localization by embedding cryptographic signature and block identifier,"
[9]. G. Coatrieux, H. Maitre, andB. Sankur, "Strict integrity control of biomedicalimages,"
[10]. G. Coatrieux, C. Le Guillou, J. M. Cauvin, and C. Roux, "Reversible watermarking for knowledge digest embedding and reliability control in medical images,"
[11]. A. Wakatani, "Digital watermarking for ROI medical images by using compressed signature image,"
[12]. I. Avcibas, S. Bayram, N. Memon, M. Ramkumar, and B. Sankur, "Aclassifier design for detecting image manipulations,"
[13]. M.K. Hu, "Visual pattern recognition by moment invariants," IRE Trans. Inf. Theory, vol. 8, no. 2, pp. 179-187, 1962.
[14]. H. Huang, G. Coatrieux, H. Shu, L. Luo, and Ch. Roux, "Blind integrity verification of medical images,"

IJSER