Research Journal of

Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 6 (4): 270-290, 2014
ISSN 1815-7432 / DOI: 10.3923/rjit.2014.270.290

Study of QR Code Zero Watermarking Systems in Contourlet-SVD and SVD Domains under Noise Attacks

[1]R. Velumani and [2]V. Seenivasagam
[1]Department of Information Technology, Sethu Institute of Technology, Pulloor, Kariapatti, 626115, India
[2]Department of Computer Science and Engineering, National Engineering College, Kovilpatti, 628503, India

Corresponding Author: R. Velumani, Department of Information Technology, Sethu Institute of Technology, Pulloor, Kariapatti, 626115, India Tel: +91 9865768480 Fax: +91 04566 308000

ABSTRACT
Healthcare providers employ Quick Response (QR) codes for patient identification and tracking. Earlier, we have implemented a zero watermarking system in the composite Contourlet Transform (CT), Singular Value Decomposition (SVD) domain to embed a QR code of a Health Level 7 (HL7) PID segment, for patient authentication. The work proposed in this study is an extension of the above which presents a study on the behavior of the system exclusively under intense noise attacks. The purpose of this study is to evaluate the robustness of the systems under noise attacks in the composite CT-SVD and SVD domains. The methodology employed for this study implements watermarking systems employing SVD and Hu's image invariants and extracts the QR code watermark from the host images subjected to AWGN, poisson, salt and pepper and speckle noise attacks. The findings of this investigation show that the system exhibits better robustness in the CT-SVD domain compared to the SVD domain. Further, it is also demonstrated that, lower order Hu's moments are adequate to impart robustness against noise in zero watermarking systems. This research also advocates the need to identify noise invariants for medical images with small regions of interest. Extreme robustness demonstrated by the systems also calls for further investigations on ambiguity attacks on zero watermarking systems.

Key words: Noise, Teleradiology, Hu's moments, contourlet, SVD, zero watermarking, QR code

INTRODUCTION
Healthcare providers, adopt teleradiology services under shortage of in-house radiologists and lack of provisions for subspecialty readings (Benjamin *et al*., 2010). Standards on teleradiology, demand positive patient identification and delivery of past medical history etc., to the reading site (Cramer *et al*., 2008). Legislative standards such as Health Insurance Portability and Accountability Act (HIPAA, 1996) define rigorous patient data security and privacy requirements. An extensive study on the application of watermarking in teleradiology (Nyeem *et al*., 2013), advocates the need for designing multiple watermarking systems to meet the security and privacy needs in teleradiology. Medical images are corrupted by noise during acquisition and transmission, resulting in obvious visual degradations. In this study, we present an extensive study on the performance of our previous work (Seenivasagam and Velumani, 2013), a QR code based zero watermarking system exclusively under noise attacks. Zero watermarking proposed by Chang *et al*. (1999), is a novel watermarking paradigm, in which a watermark is not physically embedded into a host image as in classical watermarking schemes, protecting the fidelity of the host

images. In zero watermarking, a binary pattern generated from the host image features, is combined with the watermark image to generate a secret key during embedding. At the receiving end, on extraction, the same procedure is applied to create a binary pattern which is combined with the secret key to construct the watermark image. Recent zero watermarking schemes in the literature are based on Visual Secret Sharing (VSS) which employs both Visual Cryptography (VC) (Naor and Shamir, 1995) and generalized secret sharing (Guo and Georganas, 2003) approaches. Secret sharing refers to the distribution of a secret image as multiple shares and combining the shares to construct the secret image. The VC defines a set of rules to represent white and black pixels and reveals the secret image by physically superimposing the transparencies of the Secret Shares without any mathematical computations. In VSS based zero watermarking (Chang and Chuang, 2002) schemes, a Master Share is constructed from the essential image features and it is combined with the watermark image to generate a Secret Share at the sender's side. Similarly, a Master Share is generated from the host image and is combined with the Secret Share to reveal the watermark at the receiver's end. Image moments (Prokop and Reeves, 1992) find wide applications in pattern recognition, object classification and image reconstruction. Many authors have testified the invariant nature of image moments, employing them in watermarking schemes to achieve robustness against geometric attacks. However, their robustness has not been studied under the influence of extreme noise attacks.

In this study, we present a detailed study on the performance of our moment based zero watermarking system implemented in CT-SVD domain, against noise attacks. Earlier, the robustness of this system against common signal processing and geometric attacks has been testified with medical images of different modalities and a QR code containing HL7 PID segment. In this study, we have tested the system in both CT-SVD and SVD domains, with the same host images and a QR code watermark generated from a Health Level 7 (HL7) message segment containing patient identification and clinical observation data. Here, the host images are attacked with AWGN (Additive White Gaussian Noise), poisson, salt and pepper and speckle noises and the robustness of the system is evaluated in both the domains, examining the readability of the watermarks constructed from the noisy images.

The experimental results show that, the system offers better robustness in the CT-SVD domain as evinced from the Normalized Correlation (NC) and Bit Error Rate (BER) metrics of the extracted watermarks and readability analysis with QR code decoder software. The NC and BER values of the extracted watermarks are closer to 1 and 0, respectively, signifying high robustness. Even the watermarks extracted from highly distorted host images are readable that leads to ambiguity. It is also observed that the selected invariants are not robust for images with smaller region of interest. Hence, this study brings out two new research issues: (1) Ambiguity attacks in zero watermarking systems and (2) Moment invariants for images with small regions of interest.

Consise accounts on the application of QR codes in healthcare, an overview of HL7 protocol, the characteristics of a few classes of noise prevalent in medical images and description of a few zero watermarking schemes, reported in the literature.

QR CODES IN HEALTHCARE

QR codes are 2D barcodes introduced by Denso-wave to track vehicle parts. Healthcare institutions resort to patient wristbands displaying QR codes, encoded with patient identifiable data to manage front office and clinical procedures. The structure of the QR code is shown in Fig. 1. An overview on QR codes and their applications is elaborately discussed by Soon (2008). The

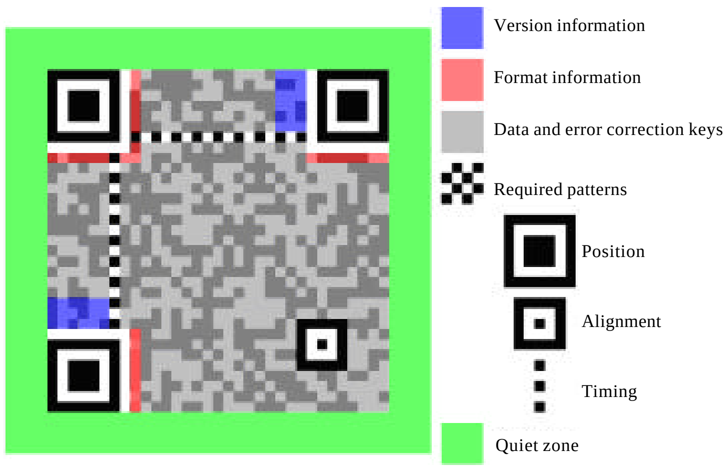


Fig. 1: Structure of QR code. http://en.wikipedia.org/wiki/File:QR_Code_Structure_Example_2.svg

application of 1D, 2D barcodes, Radio Frequency Identification (RFID) tags and QR codes for automatic patient identification has been evaluated by Garcia-Betances and Huerta (2012). The authors advocate the use of QR codes for patient identification in low budgeted health centers, due to their simplicity and ubiquity of smart phones enabled with QR code readers. Further, web links to essential patient information are encoded into QR codes for instant access by paramedics under emergency (Davis, 2012). Chen and Wang (2009) proposed a blind watermarking scheme to embed a QR code and a facial image in the DCT coefficients of a medical image. Another blind watermarking scheme to embed a QR code of the Universal Content Identifier (UCI) for authentication of multimedia content is proposed by Kim *et al.* (2010). This scheme embeds a 64×64 QR code into the spatial, DCT and FFT domains of a digital image of size 512×512.

INTEGRATION OF HL7 AND TELERADIOLOGY

HL7 protocol defines interoperability standards between disparate healthcare providers and stakeholders for exchange, integration and retrieval of electronic health information. It comprises of a collection of message types to handle different events. Each message type consists of a number of segments which carry the message. The patient identification (PID) and observation (OBX) segments contain patient identification and observation data, respectively. A sample HL7 message with PID, OBX and other related segments, is shown in Fig. 2. In teleradiology, images are represented in Digital Imaging and Communications in Medicine (DICOM) formats. The need to integrate DICOM and HL7 as a single protocol to improve the workflow is addressed by Cordos *et al.* (2010). Our zero watermarking system is an approach towards this integration which also preserves the fidelity of the medical images.

NOISE IN MEDICAL IMAGES

Artifacts are introduced into medical images due to noise generated on image acquisition, compression and transmission. Gaussian and non gaussian noises with different regularization models occur in medical images. Most works in the literature deal with AWGN (Lal *et al.*, 2011). The AWGN is a white noise added to the image by the transmission channel that follows a gaussian

```
MSH|^~\&|LCS|LCA|LIS|TEST9999|199807311532||ORU^R01|3630|P|2.2
PID|3|2161348473|20923085580|01572633|20923085580^TESTPAT||19730204|
M|||^^^^00000-0000|||||||86427531^^^03|SSN#                      HERE
PV1||I|^802^1||||8625^Physician^Michael|86-7468^||xxx||||||||V1001
ORC|NW|8642753100013^LIS|20923085580^LCS||||||19980728000000|||PEED
OBR|1|8642753100013^LIS|20923085580^LCS|083824^PANEL
083824^L|||19980728083600||||||
CH13380|19980728000000||||||20923085580||19980730041800|||F
OBX|1|NM|150001^HIV-1              ABS-O.D.            RATIO^L||||||N|X
OBX|2|CE|001719^HIV-1       ABS,        SEMI-QN^L||HTN|||||N|F|19910123||
19980729155700|BN
NTE|1|L|Result:          NEGATIVE          by          EIA          screen.
NTE|2|L|No          antibodies          to          HIV-1          detected.
OBX|3|CE|169999^.^L||SPRCS|||||N|F|||19980728130600|BN
NTE|1|L|NOTE:              Submission              of              serum
NTE|2|L|separator                    tube                    recommended
NTE|3|L|for          this          test.          Thank          you
NTE|4|L|for          your          cooperation          if          you
NTE|5|L|are              already              doing              so.
OBX|4|CE|169998^.^L||SPRCS|||||N|F|||19980728130600|BN
ZPS|1|BN|LABCORP                    HOLDINGS|1447                    YORK
COURT^^BURLINGTON^NC^272152230|8007624344
```


Fig. 2: Sample HL7 message

distribution and constant spectral density. In an image contaminated with AWGN, value of each pixel is the sum of the actual pixel value and a random noise value with gaussian distribution. Poisson or photo counting noise is predominant in Positron Emission Tomography (PET) and fluorescence microscopy. The noise is a characteristic of the image itself and is not influenced by any external sources. In the noisy PET images degraded by poisson noise, the random variables follow a poisson distribution. Salt and pepper noise appears as sparse black and white dots in a corrupted image. It is an impulse noise caused by the malfunctions in the capturing device and synchronization errors during digitization and transmission. Speckle noise is a multiplicative noise that appears as granular patterns commonly in ultrasound images. It is introduced due to scattering effects, increasing the mean gray level in the local area of the image. One can understand the characteristics of poisson and speckle noises from the thesis by Sawatzky (2011). Gonzalez and Woods (2008) have given detailed accounts on the above noise types and the corresponding Probability Density Functions.

SVD AND VSS BASED ZERO WATERMARKING

Hsu and Hou (2005) proposed a scheme in which the Master Share is created from the distribution of means in the host image for a normal population. Wang and Chen (2009) proposed a scheme in the composite DWT-SVD domain in which, the Master Share is created from the SVs of the non-overlapping blocks of the LL subband. A hybrid scheme proposed by Rawat and Raman (2012) is based on Fractional Fourier Transform (FrFT) and SVD. Initially, a subimage is created from selected non-overlapping blocks of the host image. The Master Share is created from the image features extracted by applying FrFT and SVD on the subimage. The Secret Share is generated from the Master Share and the secret watermark image. A VSS based zero watermarking scheme, proposed by Fan *et al*. (2012), employs the Bose-Chaudhuri-Hocquenghem (BCH) code for error correction. An image comprising only selected Most Significant Bit (MSB) planes of the host image is transformed by DWT. A secret key is used to select coefficients of the LL subband to create the

Master Share. The Secret Share is created from the quantized host image, Master Share and the scrambled watermark. The last two schemes are reported to be resilient to both geometric and non-geometric attacks.

METHODOLOGY

Triangular number generation function: A triangular number is a figurate number which can be represented in a triangular pattern with dots as shown in Fig. 3.

Triangular numbers are generated by applying Eq. 1. This function uniquely encodes a pair of integers (a, b) into T which can be factored back without any overhead:

$$T = f(a, b) = \frac{(a+b)^2 + 3a + b}{2} \tag{1}$$

The T values of the coded integer pairs (a, b) for a small set of values is given in Table 1. The sequence of triangular numbers appears in the first row of the table; every pair of integers is distinctly encoded; i.e., f(a, b) and f(b, a) are unique. The integer pair (a, b) can be recovered on applying the Eq. 2-4:

$$C = \frac{\text{sqrt}(8T+1)-1}{2} \tag{2}$$

Where:

$$C = a+b$$

$$a = \frac{T-C(C+1)}{2} \tag{3}$$

Table 1: Triangular numbers

	b			
a	0	1	2	3
0	0	1	3	6
1	2	4	7	11
2	5	8	12	17
3	9	13	18	24

```
*     *     *     *     *
      **    **    **    **
            ***   ***   ***
                  ****  ****
                        *****
1     3     6     10    15
```

Fig. 3: Triangular numbers

$$b = \frac{C(C+3)}{2-T} \tag{4}$$

Hence, it is evident that the features of reversibility and blindness in extraction are intrinsic in the TNG function, i.e., a and b can be recovered back exactly without any side information. In the proposed system, we have applied Eq. 1 for Secret Share generation and Eq. 2-4 for watermark extraction.

Contourlet transform: Do and Vetterli (2005), proposed the Contourlet Transform (CT) which combines Laplacian Pyramid (LP) and Directional Filter Bank (DFB) structure. The framework for Contourlet decomposition is given in Fig. 4. It provides directionality and anisotropy properties in addition to multiscale and time-frequency localization proprieties of wavelets. This transform provides the best approximation of smooth contours and edges of the image subjected to decomposition. On applying CT on an image I, at each level j of contourlet decomposition, a lowpass image I_j is generated at the LP stage. At the DFB stage, a set of band pass images B_j, j = 1, 2,... 2^k, where, k is the number of directional decompositions at each level are generated. While the lowpass image preserves the Low Frequency (LF) components, directional subbands preserve the high frequency components. This process may be repeated for the desired level of decomposition with the lowpass image.

Many researchers have implemented blind and non-blind watermarking algorithms in the Contourlet domain. Rahimi and Rabbani (2011) presented a dual blind watermarking scheme to embed a caption watermark encompassing patient data in the Region of Interest (ROI) and the physician's digital signature watermark in the Region of Non Interest (RONI).

Singular value decomposition: Singular value decomposition is a linear algebraic tool widely used in factorization and approximation of matrices. For any n×n real or complex matrix A, SVD is a factorization of the form given in Eq. 5:

$$[U, S, V] = SVD(A) \tag{5}$$

where, S is a n×n diagonal matrix with nonnegative real numbers on the diagonal; U and V are the unitary matrices of the order n×n.

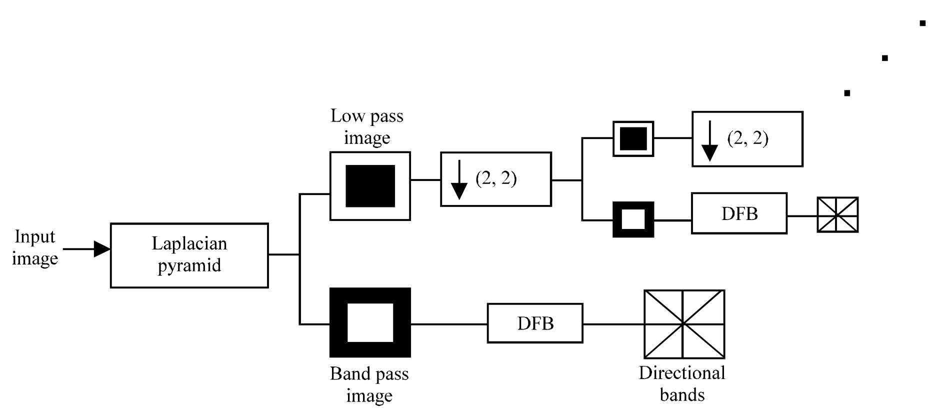


Fig. 4: Contourlet decomposition

The diagonal entries S_{ii} of S are known as the Singular Values (SV) of A and the columns of U and V are called as left-singular vectors and right-singular vectors of A, respectively. Matrix A is reconstructed from the singular and unitary matrices as shown in Eq. 6:

$$A = U \times S \times V' \tag{6}$$

where, V' is the complex conjugate of V.

The singular values of S are stable under transpose, flipping, scaling, rotation and translation operations. Further, a few significant SVs are sufficient for best approximation of the image. Hence, SVD is widely applied in implementing robust watermarking systems. A zero watermarking scheme proposed by Ye (2011), employs SVD and Discrete Cosine Transform (DCT) in which, the host image is subjected to SVD and the SV matrix is transformed with DCT to embed and extract the watermark.

Hu's moment invariants: Statistical moments find extensive applications in pattern recognition, object identification and classification. Moments are invariant pattern features used to discriminate the objects under distortions. According to Hu (1962), image patterns can be represented by their geometric moments. The 2D moment of order (p+q) of a digital image f(x, y) of size M×N is defined as:

$$m_{pq} = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} x^p y^q f(x, y) \tag{7}$$

where, p = 0, 1, 2... M-1 and q = 0, 1, 2,... N-1 are integers. The corresponding central moment of order (p+q) is defined as:

$$\mu_{pq} = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} (x-\bar{x})^p (y-\bar{y})^q f(x, y) \tag{8}$$

for p = 0, 1, 2.... M-1 and q = 0, 1, 2,... N-1.
Where:

$$\bar{x} = \frac{m_{10}}{m_{00}} \text{ and } \bar{y} = \frac{m_{01}}{m_{00}} \tag{9}$$

The normalized central moment of order (p+q) is defined as:

$$\eta_{pq} = \frac{\mu_{pq}}{\mu_{00}^{\gamma}} \tag{10}$$

Where:

$$\gamma = \frac{p+q}{2} + 1 \text{ for } p+q = 2, 3,... \tag{11}$$

From the above equations, the 2D moments invariant to translation, scaling, rotation and mirroring are derived as follows:

$$I_1 = \eta_{20}+\eta_{02} \tag{12}$$

$$I_2 = (\eta_{20}-\eta_{02})^2+4\eta^2_{11} \tag{13}$$

$$I_3 = (\eta_{30}-3\eta_{12})^2+(3\eta_{21}-\eta_{03})^2 \tag{14}$$

$$I_4 = (\eta_{30}+\eta_{12})^2+(\eta_{21}+\eta_{03})^2 \tag{15}$$

$$I_5 = (\eta_{30}-3\eta_{12})(\eta_{30}+\eta_{12})[(\eta_{30}+\eta_{12})^2-3(\eta_{21}+\eta_{03})^2]+(3\eta_{21}+\eta_{03})(\eta_{21}+\eta_{03})[3(\eta_{30}+\eta_{12})^2-(\eta_{21}+\eta_{03})^2] \tag{16}$$

$$I_6 = (\eta_{20}-\eta_{02})[(\eta_{30}+\eta_{12})^2-(\eta^2_{10}+\eta_{03})^2]+4\eta_{11}(\eta_{30}+\eta_{12})(\eta_{21}+\eta_{03}) \tag{17}$$

$$I_7 = (3\eta_{21}-\eta_{03})(\eta_{30}+\eta_{12})[(\eta_{30}+\eta_{12})^2-3(\eta_{21}+\eta_{03})^2]+(3\eta_{12}-\eta_{30})(\eta_{21}+\eta_{03})[3(\eta_{30}+\eta_{12})^2-(\eta_{21}+\eta_{03})^2] \tag{18}$$

Out of the seven invariants, I_1 to I_6 are called translation, scaling and rotation invariants. The I_7, whose sign changes to distinguish mirrored images is called the skew invariant. Hu (1962) demonstrated the invariant nature of these moments in recognizing printed uppercase characters. From Eq. 12-18, it is evident that the computational complexity is high for higher order moments. From literature, we also understand that the higher order moments are sensitive to noise. Alghoniemy and Tewfik (2000, 2004) studied the invariance properties of image moments and generated invariant watermarks from the Hu's geometric moments to achieve robustness against geometric attacks. Similarly, a watermarking algorithm for copyright protection of semantic content in a video (Tzouveli *et al*., 2006) generates the invariant watermark from the entire set of weighted Hu's moments of the video object. An analysis on the Hu's moments by Huang and Leng (2010) reports, that the moment invariants change on scaling and rotation and fluctuation of moments decreases as spatial resolution increases. Further, it is also identified that there is no obvious decrease in fluctuation when the resolution goes above a threshold. Hu's moments find applications in designing watermarking systems robust to geometric attacks. In a recent study, an invisible watermarking scheme based on four lower order Hu's moments is proposed, it is found to be superior to a Fast Fourier Transform (FFT) based technique presented in the same study under geometric and noise attacks (Ferdous *et al*., 2012).

Arnold transform: The Arnold Transform is a periodic chaotic transform that maps any coordinate position x, y to x_n, y_n and vice-versa in any n×n space as shown in Eq. 19 and 20. Chaotic transforms are commonly employed in watermarking systems to scramble the watermarks before embedding and to recover the same on extraction:

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\text{mod}\, n) \tag{19}$$

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} (\text{mod}\, n) \tag{20}$$

The periodic and area preserving properties of this transform are suitable for realizing synchronization in watermarking systems. Recent medical image watermarking algorithms employ this transform for scrambling the watermarks (Li *et al*., 2012; Liu *et al*., 2012).

PROPOSED SYSTEM

Watermark generation: We have encoded the HL7 message shown in Fig. 2, into a QR code with open source Zebra Crossing (Zxing) software. We have set the QR code size to be medium, error correction level to be large and Unicode Set Transformation Format-8 (UTF-8) as the encoding standard with the Zxing User Interface. The resultant QR code is of size 230×230×3. We represent it as binary and consider only the inner region of size 109×109 for watermarking, excluding the quiet zone to reduce the computational complexity. The generated QR code and its trimmed form are shown in Fig. 5a-b.

Secret share creation: The Secret Share creation starts with Master Share creation. The Master Share is constructed as a matrix comprising, sign bit sequence of the Hu's moments I_1, I_2 and I_3 computed on the candidate blocks selected from the host image. In the CT-SVD domain, the candidate blocks are selected from the non overlapping LF band. In the SVD domain, the candidate blocks are selected from the non overlapping blocks of the host image itself. The Secret Share is constructed by applying the TNG function on the Master Share and the watermark image in Fig. 5b. The procedures for Secret Share creation are given in Algorithm 1 and 2 and illustrated with Fig. 6 and 7, respectively.

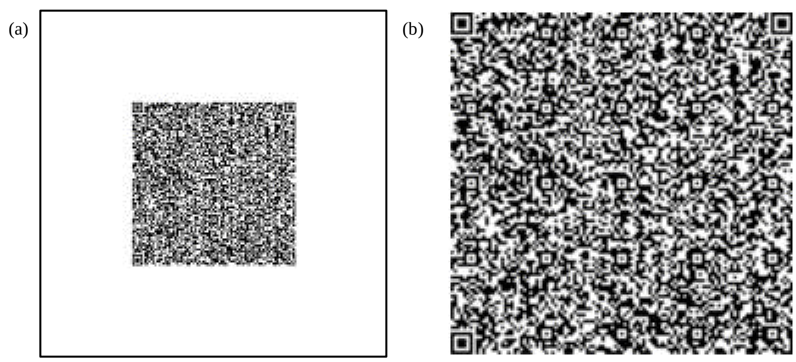


Fig. 5(a-b): Watermark image (a) QR code of watermark contents and (b) Trimmed QR code

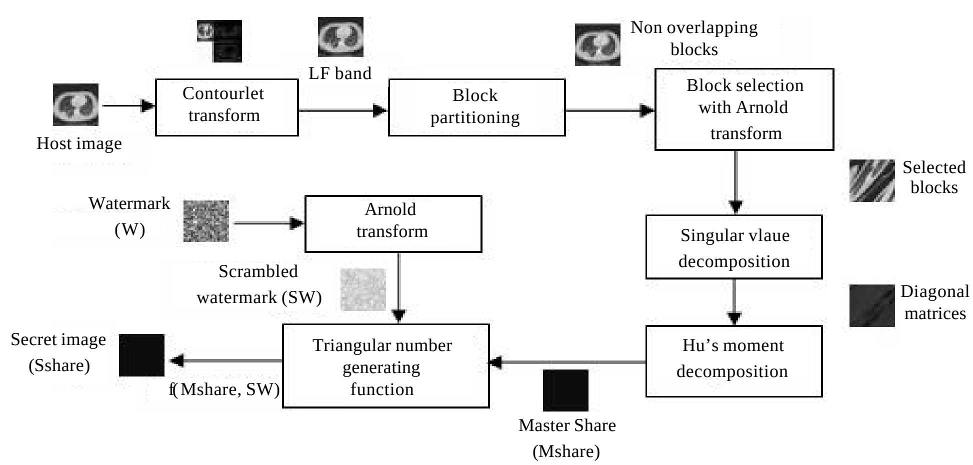


Fig. 6: Secret Share creation in CT-SVD domain

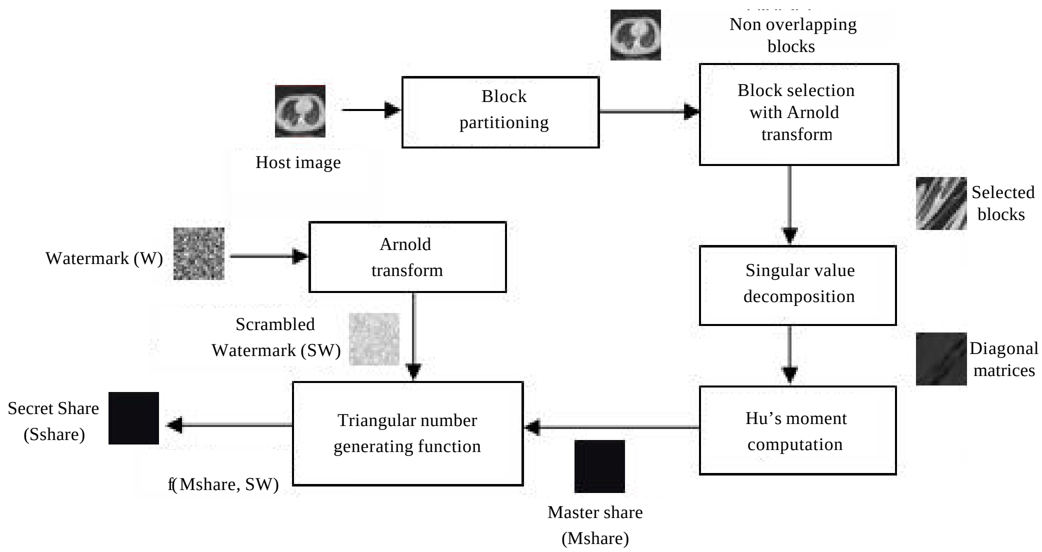


Fig. 7: Secret Share creation in SVD domain

Algorithm 1: Secret Share creation CT-SVD domain

Input: Host Image H of size N×N, Watermark W of size m×m, Key (k_i, k_j) for initial block selection, size of block b×b, Number of iterations i for Arnold Transform

Output: Secret Share Sshare of size m×m

Step 1: Apply Contourlet Transform on H to generate a n×n LF subband
Step 2: Perform b×b block partitioning on the LF subband to generate n/b×n/b non overlapping blocks
Step 3: Apply Arnold Transform on W to generate scrambled watermark SW
Step 4: Perform steps 5-9 for each bit W_{ij} of watermark
Step 5: Apply Arnold Transform on (k_i, k_j) to select a block for Master Share creation; Increment k_i and k_j by 1
Step 6: Apply SVD to the selected block to generate U, S and V matrices
Step 7: Compute Hu's moment invariants I_1, I_2 and I_3 for the diagonal matrix S
Step 8: Create a 3 bit Master Share Mshare out of the sign bits of I_1, I_2 and I_3
Step 9: Encode Mshare and SW with Eq. 1 to generate Secret Share Sshare, of size m×m i.e., Sshare = f (Mshare, SW)

Algorithm 2: Secret Share creation SVD domain

Input: Host Image H of size N×N, Watermark W of size m×m, Key (k_i, k_j) for initial block selection, size of block b×b, Number of iterations i for Arnold Transform

Output: Secret Share Sshare of size m×m

Step 1: Perform b×b block partitioning on H to generate N/b×N/b non overlapping blocks
Step 2: Apply Arnold Transform on W to generate scrambled watermark SW
Step 3: Perform steps 4-8 for each bit W_{ij} of watermark
Step 4: Apply Arnold transform on (k_i, k_j) to select a block for Master Share creation; Increment k_i and k_j by 1
Step 5: Apply SVD to the selected block to generate U, S and V matrices
Step 6: Compute Hu's moment invariants I_1, I_2 and I_3 for the diagonal matrix S
Step 7: Create a 3 bit Master Share Mshare out of the sign bits of I_1, I_2 and I_3
Step 8: Encode Mshare and SW with Eq. 1 to generate Secret Share Sshare, of size m×m i.e., Sshare = f (Mshare, SW)

Watermark construction: Similar to Secret Share creation, watermark construction also begins with Master Share construction. The watermark is obtained by mere subtraction of Master

Share from the Secret Share. The detailed procedure for implementing watermark construction in CT-SVD and SVD domains are given in Algorithm 3 and 4 and illustrated with Fig. 8 and 9, respectively.

Algorithm 3: Watermark construction in CT-SVD domain

Input: Host image H of size N×N, Secret Share Sshare of size m×m, Key (k_i, k_j) for initial block Selection, size of block b×b, Number of iterations i for Arnold Transform

Output: Watermark W of size m×m

Step 1: Apply Contourlet Transform on H to generate a n×n LF subband

Step 2: Perform b×b block partitioning on the LF subband to generate n/b×n/b non overlapping blocks

Step 3: Perform steps 4-9 for each element of Sshare

Step 4: Apply Arnold transform on (k_i, k_j) to select a block for Master Share creation; Increment k_i and k_j by 1

Step 5: Apply SVD to selected block to generate U, S and V matrices

Step 6: Compute the Hu's invariant moments I_1, I_2 and I_3 the diagonal matrix S

Step 7: Create a 3 bit Master Share Mshare out of the sign bits of I_1, I_2 and I_3

Step 8: Compute C from Sshare with Eq. 2:

$$C = \frac{\text{sqrt}(8\times \text{Sshare}+1)-1}{2}$$

where, C = Sum (Mshare, SW)

Step 9: Subtract Mshare from C to get SW

Step 10: Apply Arnold Transform on SW to reveal the watermark W

Algorithm 4: Watermark construction in SVD domain

Input: Host image H of size N×N, Secret Share Sshare of size m×m, Key (k_i, k_j) for initial block Selection, size of block b×b, Number of iterations i for Arnold Transform

Output: Watermark W of size m×m

Step 1: Perform b×b block partitioning on H to generate N/b×N/b non overlapping blocks

Step 2: Perform steps 3-8 for each element of Sshare

Step 3: Apply Arnold transform on (k_i, k_j) to select a block for Master Share creation; Increment k_i and k_j by 1

Step 4: Apply SVD to selected block to generate U, S and V matrices

Step 5: Compute the Hu's invariant moments I_1, I_2 and I_3 for the diagonal matrix S

Step 6: Create a 3 bit Master Share Mshare out of the sign bits of I_1, I_2 and I_3

Step 7: Compute C from Sshare with Eq. 2:

$$C = \frac{\text{sqrt}(8\times \text{Sshare}+1)-1}{2}$$

where, C = Sum (Mshare, SW)

Step 8: Subtract Mshare from C to get SW

Step 10: Apply Arnold Transform on SW to reveal the watermark W

From the illustrations, we can see that the embedding and extraction algorithms follow the same procedure for Master Share creation. For system implementation in SVD domain the algorithms begin with block partitioning on the host image.

RESULTS AND ANALYSIS

We have implemented system in the CT-SVD and SVD domains with the host images of size 512×512 shown in Fig. 10a-g and the watermark image in Fig. 5b with MATLAB 12 software. For

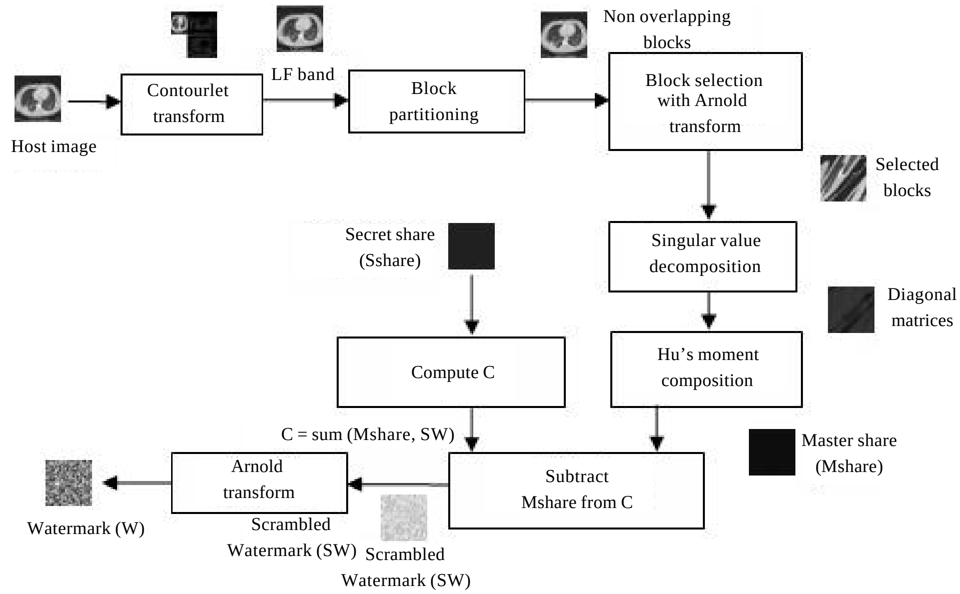


Fig. 8: Watermark construction in CT-SVD domain

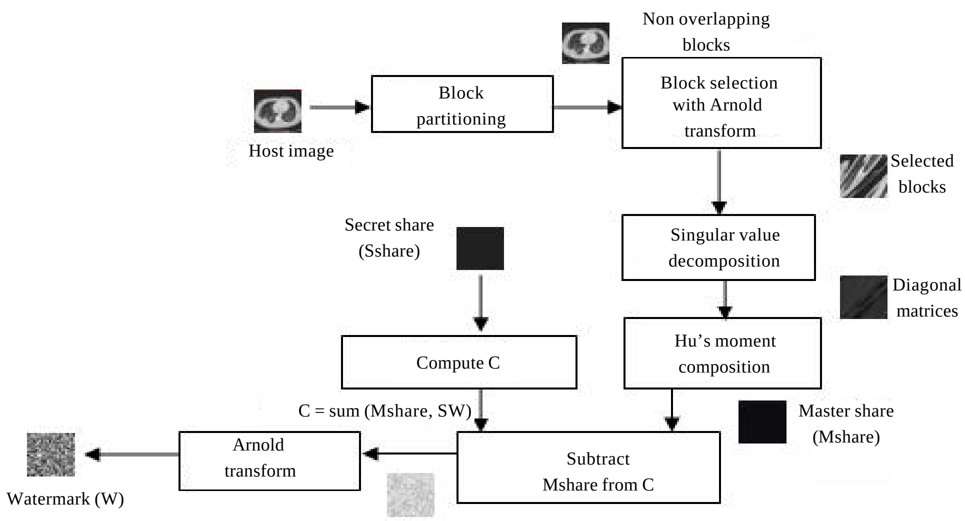


Fig. 9: Watermark construction in SVD domain

implementation in CT-SVD domain, initially we have subjected the host images to 1 level contourlet decomposition. The LF band of size 256×256 is divided into non overlapping blocks assuming b×b = 2×2. This gives a block space of 128×128. Similarly, we have implemented the algorithms in the SVD domain assuming b×b = 4×4. Accordingly, the host image is divided into 128×128 non overlapping blocks each size 4×4. Rest of the assumptions are same for both the domains. We have made the assumptions, $k_i = 64$, $k_j = 64$, i.e., k = (64, 64) and n = 6. By 6 iterations of Arnold Transform, k is mapped to (127, 62). For the watermark bit W_{11}, the block (127, 62) is selected out of the candidate block space and SVD is applied on that and I_1, I_2 and I_3 are computed for the diagonal matrix. The sign bit sequence of these invariants is the Master Share for W_{11}. Similarly, the Master Share is created for the rest of the watermark bits by incrementing both k_i and k_j by 1.

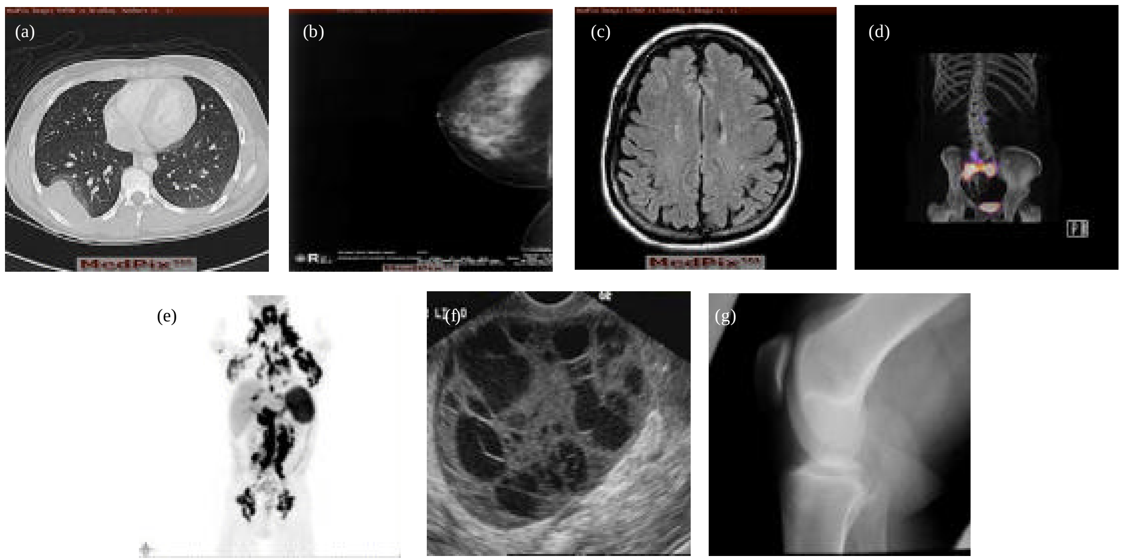


Fig. 10(a-g): Host images (a) CT scan, (b) Mammogram, (c) MRA, (d) Nuclear, (e) PET, (f) Ultrasound and (g) X-ray

The Secret Share is created applying TNG function on the Master Share and the corresponding scrambled watermark bits. Similarly on extraction, the Master Share is created for the host image and is subtracted from the Secret Share to reveal the scrambled watermark.

The watermarks extracted from these images are evaluated with BER, NC, Structural Similarity Index Measure (SSIM) and Universal Image Quality Index (UIQI) metrics. These performance metrics evaluate to ideal values demonstrating that, the watermarks constructed are intact for all modalities when the host images are unaltered. We have evaluated the performance of the system under noise attacks for all the modalities in both the domains. We have generated the attacked host images by adding AWGN, poisson, salt and pepper and speckle noise with MATLAB 12 software. AWGN is added for values of SNR ranging from 1-10 dB in increments of 1 dB resulting in 10 attacked images under each modality. Similarly, poisson noise is added to each of the host images to generate 1 attacked image from each. Salt and Pepper Noise is added in increments of 0.1 from 0.1-1 resulting in 10 attacked images in each modality. Speckle noise is added in increments of 0.08 from 0.04-1, resulting in 13 attacked images for each modality. We evaluated the robustness of the watermarks and thus the system, with the NC values and the readability of the watermarks with the Zxing decoder. We have tabulated the same for the watermarks extracted from these images in Table 2-5 for AWGN, poisson, salt and pepper and speckle noise attacks, respectively. The symbols ✓ and ⊠ are used to denote that a watermark is readable and unreadable, respectively. Tables show that the NC values are closer to unity in both the domains.

However, we can also see that, many watermarks are not decodable in spite of similarity to the original watermark. This can be attributed to the loss of significant data required for error correction. Watermarks not recognized by decoders under AWGN attacks in both domains are shown in Fig. 11.

Table 2: NC and readability under AWGN attacks

	Modality							
SNR (dB)	Domain	CT	Mammogram	MRA	Nuclear	PET	Ultrasound	X-ray
1	CT-SVD	0.9989 ✓	0.9930☒	0.9989✓	0.9988✓	0.9989✓	0.9993✓	0.9990✓
	SVD	0.9988✓	0.9908☒	0.9965☒	0.9960☒	0.9989✓	0.9991✓	0.9967☒
2	CT-SVD	0.9990✓	0.9928☒	0.9989✓	0.9986✓	0.9994✓	0.9993✓	0.9988✓
	SVD	0.9989✓	0.9912☒	0.9965☒	0.9974☒	0.9988✓	0.9991✓	0.9966☒
3	CT-SVD	0.9989✓	0.9929☒	0.9989✓	0.9986✓	0.9994✓	0.9992✓	0.9988✓
	SVD	0.9987✓	0.9912☒	0.9962☒	0.9972✓	0.9988✓	0.9991✓	0.9965☒
4	CT-SVD	0.9989✓	0.9922☒	0.9989✓	0.9989✓	0.9995✓	0.9992✓	0.9987✓
	SVD	0.9989✓	0.9905☒	0.9964☒	0.9978✓	0.9989✓	0.9991✓	0.9968☒
5	CT-SVD	0.9988✓	0.9922☒	0.9988✓	0.9990✓	0.9993✓	0.9992✓	0.9985✓
	SVD	0.9987✓	0.9911☒	0.9964☒	0.9979✓	0.9987✓	0.9991✓	0.9966☒
6	CT-SVD	0.9991✓	0.9924☒	0.9987✓	0.9989✓	0.9994✓	0.9991✓	0.9988✓
	SVD	0.9986✓	0.9916☒	0.9960☒	0.9977✓	0.9988✓	0.9991✓	0.9965☒
7	CT-SVD	0.9989✓	0.9926☒	0.9985✓	0.9990✓	0.9995✓	0.9992✓	0.9988✓
	SVD	0.9985✓	0.9910☒	0.9964☒	0.9981✓	0.9988✓	0.9991✓	0.9967☒
8	CT-SVD	0.9988✓	0.9926☒	0.9985✓	0.9990✓	0.9995✓	0.9992✓	0.9985✓
	SVD	0.9985✓	0.9913☒	0.9961☒	0.9982✓	0.9988✓	0.9991✓	0.9963☒
9	CT-SVD	0.9988✓	0.9923☒	0.9985✓	0.9990✓	0.9994✓	0.9992✓	0.9989✓
	SVD	0.9987✓	0.9909☒	0.9959☒	0.9983✓	0.9987✓	0.9991✓	0.9966☒
10	CT-SVD	0.9989✓	0.9914☒	0.9985✓	0.9991✓	0.9995✓	0.9992✓	0.9989✓
	SVD	0.9984✓	0.9912☒	0.9960☒	0.9981✓	0.9988✓	0.9990✓	0.9967☒

Table 3: NC and readability under poisson noise attacks

	Modality						
Domain	CT	Mammogram	MRA	Nuclear	PET	Ultrasound	X-ray
CT-SVD	0.9994✓	0.9927☒	0.9991✓	0.9988✓	0.9996✓	0.9987✓	0.9992✓
SVD	0.9991✓	0.9866☒	0.9973☒	0.9971✓	0.9992✓	0.9977✓	0.9983✓

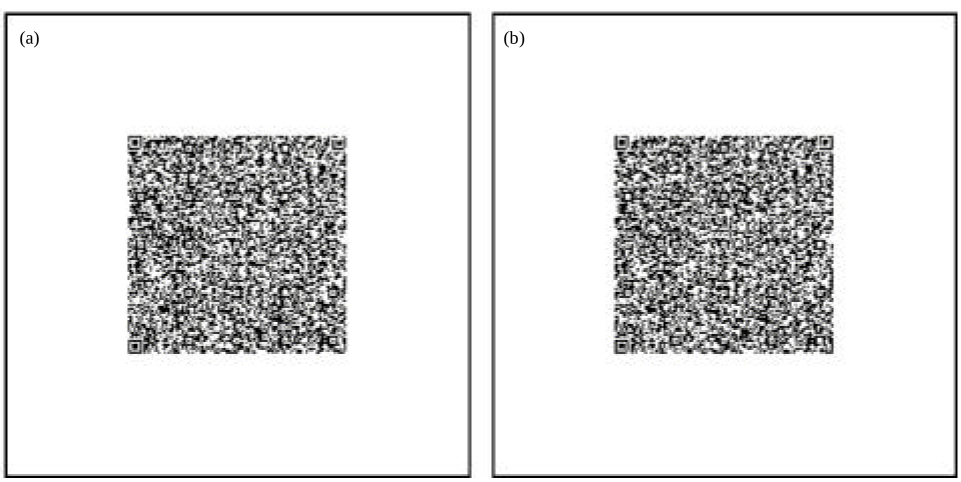


Fig. 11(a-b): Undecodable watermarks (a) CT-SVD and (b) SVD domain

Table 4: NC and readability under salt and pepper noise attacks

Noise density	Domain	Modality CT	Mammogram	MRA	Nuclear	PET	Ultrasound	X-ray
0.1	CT-SVD	0.9994✓	0.9928☒	0.9995✓	0.9987✓	0.9998✓	0.9987✓	0.9993✓
	SVD	0.9991✓	0.9875☒	0.9984☒	0.9971✓	0.9994✓	0.9977✓	0.9989✓
0.2	CT-SVD	0.9994✓	0.9928☒	0.9995✓	0.9987✓	0.9998✓	0.9987✓	0.9993✓
	SVD	0.9991✓	0.9875☒	0.9984☒	0.9971✓	0.9994✓	0.9977✓	0.9989✓
0.3	CT-SVD	0.9994✓	0.9928☒	0.9995✓	0.9987✓	0.9998✓	0.9987✓	0.9993✓
	SVD	0.9991✓	0.9875☒	0.9984☒	0.9971✓	0.9994✓	0.9977✓	0.9989✓
0.4	CT-SVD	0.9994✓	0.9928☒	0.9995✓	0.9987✓	0.9998✓	0.9987✓	0.9993✓
	SVD	0.9991✓	0.9875☒	0.9984☒	0.9971✓	0.9994✓	0.9977✓	0.9989✓
0.5	CT-SVD	0.9994✓	0.9928☒	0.9995✓	0.9987✓	0.9998✓	0.9987✓	0.9993✓
	SVD	0.9991✓	0.9875☒	0.9984☒	0.9971✓	0.9994✓	0.9977✓	0.9989✓
0.6	CT-SVD	0.9994✓	0.9928☒	0.9995✓	0.9987✓	0.9998✓	0.9987✓	0.9993✓
	SVD	0.9991✓	0.9875☒	0.9984☒	0.9971✓	0.9994✓	0.9977✓	0.9989✓
0.7	CT-SVD	0.9994✓	0.9928☒	0.9995✓	0.9987✓	0.9998✓	0.9987✓	0.9993✓
	SVD	0.9991✓	0.9875☒	0.9984☒	0.9971✓	0.9994✓	0.9977✓	0.9989✓
0.8	CT-SVD	0.9994✓	0.9928☒	0.9995✓	0.9987✓	0.9998✓	0.9987✓	0.9993✓
	SVD	0.9991✓	0.9875☒	0.9984☒	0.9971✓	0.9994✓	0.9977✓	0.9989✓
0.9	CT-SVD	0.9994✓	0.9928☒	0.9995✓	0.9987✓	0.9998✓	0.9987✓	0.9993✓
	SVD	0.9991✓	0.9875☒	0.9984☒	0.9971✓	0.9994✓	0.9977✓	0.9989✓
1.0	CT-SVD	0.9994✓	0.9928☒	0.9995✓	0.9987✓	0.9998✓	0.9987✓	0.9993✓
	SVD	0.9991✓	0.9875☒	0.9984☒	0.9971✓	0.9994✓	0.9977✓	0.9989✓

From Table 2-5, we understand that the system behaves consistently in the CT-SVD domain. The system provides robustness against the four noise attacks for all modalities and noise parameters, except for mammograms in the CT-SVD domain. In the SVD domain, the system provides robustness to only CT, PET and Ultrasound images against AWGN attacks. We can see that only the watermarks extracted from attacked nuclear image with 1 and 2 dB SNR are not readable. Like in CT-SVD domain, we can see that watermarks extracted from mammograms do not withstand any of the noise attacks from the lowest to the highest intensities. In addition to mammograms, attacked MRA and X-ray images are also vulnerable to AWGN attacks.

We also understand that the mammogram and MRA images are not robust under poisson attacks in the SVD domain. It can also be seen that the system behaves similarly in both the domains for salt and pepper attacks invariably from the smallest to highest noise densities. Experimental results show that under salt and pepper noise attacks, the NC values are uniform for all image modalities, for all noise densities in both domains. Under speckle noise attacks, the robustness of the system is not consistent for MRA images in SVD domain, i.e., watermarks extracted from few attacked images with higher variances are robust.

There does not exist any zero watermarking scheme in literature for embedding the QR code. Hence, we have compared the performance of our system with other zero watermarking schemes which embed a 64×64 binary logo within the standard Lena, Baboon and Boat images in Table 6. We can understand that higher values of NC are achieved by the proposed system for a much bigger watermark of size 109×109. Similarly, we have also compared the performance of our systems with that of a conventional QR code watermarking system proposed by Kim *et al.* (2010)

Table 5: NC and readability under speckle noise attacks

		Modality						
Variance	Domain	CT	Mammogram	MRA	Nuclear	PET	Ultrasound	X-ray
0.04	CT-SVD	0.9994✓	0.9934☒	0.9985✓	0.9988✓	0.9996✓	0.9987✓	0.9991✓
	SVD	0.9991✓	0.9886☒	0.9969✓	0.9971✓	0.9991✓	0.9977✓	0.9983✓
0.12	CT-SVD	0.9994✓	0.9927☒	0.9988✓	0.9988✓	0.9997✓	0.9987✓	0.9993✓
	SVD	0.9991✓	0.9872☒	0.9972✓	0.9971✓	0.9992✓	0.9977✓	0.9984✓
0.20	CT-SVD	0.9994✓	0.9928☒	0.9991✓	0.9988✓	0.9998✓	0.9987✓	0.9991✓
	SVD	0.9991✓	0.9867☒	0.9971☒	0.9971✓	0.9992✓	0.9977✓	0.9984✓
0.28	CT-SVD	0.9994✓	0.9928☒	0.9991✓	0.9988✓	0.9997✓	0.9987✓	0.9993✓
	SVD	0.9991✓	0.9866☒	0.9976✓	0.9971✓	0.9992✓	0.9977✓	0.9983✓
0.36	CT-SVD	0.9994✓	0.9928☒	0.9991✓	0.9988✓	0.9997✓	0.9987✓	0.9994✓
	SVD	0.9991✓	0.9867☒	0.9975☒	0.9971✓	0.9992✓	0.9977✓	0.9984✓
0.44	CT-SVD	0.9994✓	0.9928☒	0.9991✓	0.9988✓	0.9997✓	0.9987✓	0.9994✓
	SVD	0.9991✓	0.9868☒	0.9977☒	0.9971✓	0.9992✓	0.9977✓	0.9985✓
0.52	CT-SVD	0.9994✓	0.9927☒	0.9991✓	0.9988✓	0.9997✓	0.9987✓	0.9993✓
	SVD	0.9991✓	0.9869☒	0.9977✓	0.9971✓	0.9992✓	0.9977✓	0.9983✓
0.6	CT-SVD	0.9994✓	0.9928☒	0.9991✓	0.9988✓	0.9997✓	0.9987✓	0.9994✓
	SVD	0.9991✓	0.9871☒	0.9978☒	0.9971✓	0.9992✓	0.9977✓	0.9985✓
0.68	CT-SVD	0.9994✓	0.9928☒	0.9991✓	0.9988✓	0.9996✓	0.9987✓	0.9993✓
	SVD	0.9991✓	0.9872☒	0.9981☒	0.9971✓	0.9993✓	0.9977✓	0.9986✓
0.76	CT-SVD	0.9994✓	0.9928☒	0.9991✓	0.9988✓	0.9997✓	0.9987✓	0.9993✓
	SVD	0.9991✓	0.9872☒	0.9978☒	0.9971✓	0.9993✓	0.9977✓	0.9986✓
0.84	CT-SVD	0.9994✓	0.9928☒	0.9991✓	0.9988✓	0.9996✓	0.9987✓	0.9993✓
	SVD	0.9991✓	0.9873☒	0.9978✓	0.9971✓	0.9992✓	0.9977✓	0.9985✓
0.92	CT-SVD	0.9994✓	0.9928☒	0.9991✓	0.9988✓	0.9997✓	0.9987✓	0.9993✓
	SVD	0.9991✓	0.9875☒	0.9981☒	0.9971✓	0.9992✓	0.9977✓	0.9986✓
1.00	CT-SVD	0.9994✓	0.9928☒	0.9992✓	0.9988✓	0.9997✓	0.9987✓	0.9993✓
	SVD	0.9991✓	0.9873☒	0.9981✓	0.9971✓	0.9992✓	0.9977✓	0.9983✓

Table 6: Performance comparison under noise attacks with NC values

	Existing schemes for 64×64 bit logo				Proposed scheme for 109×109 QR code	
Attack	Hsieh and Huang (2004)	Hsu and Hou (2005)	Wang and Chen (2009)	Rawat and Raman (2012)	CT-SVD	SVD
Gaussian noise addition	0.723	0.761	0.989	0.959	0.9989	0.9984

in Table 7. The Bit Error Rate (BER) values of the extracted watermarks are compared under JPEG compression attacks. The lowest BER values reported by Kim *et al*. (2010) are taken for a fair comparison.

DISCUSSION

From the experimental results, we found that the proposed system offers better robustness in the CT-SVD domain compared to the SVD domain. From the underlying principles of zero watermarking, it is apparent that the robustness to attacks depends upon the stability of the Master Share. We have shown the differences in Master Share between attacked and unattacked host images, under all attacks for selected parameters in Table 8. We can see that, the differences are highly pronounced in the SVD domain. Though the differences follow the same pattern, the

Table 7: Performance comparison under compression attacks with BER values

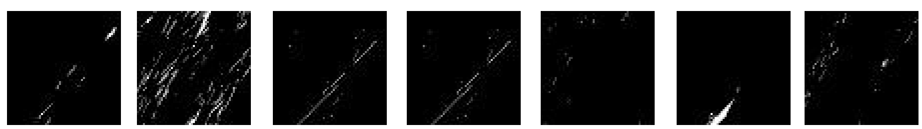
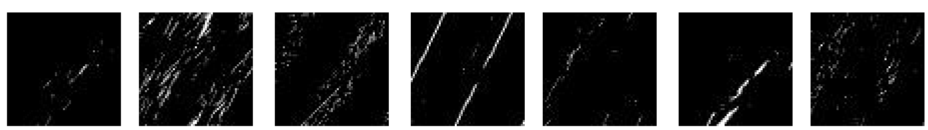
Proposed schemes by Kim *et al*. (2010)	Quality factors 100% 0.0732 (spatial)	90% 0.1953 (spatial)	80% 4.6143 (spatial)	70% 12.085 (spatial)
CT				
CT-SVD	0.0001	0.0001	0.0006	0.0005
SVD	0.0012	0.0016	0.0012	0.0011
Mammogram				
CT-SVD	0.0185	0.0182	0.0253	0.0209
SVD	0.0199	0.0195	0.0279	0.0288
MRA				
CT-SVD	0.0002	0.0002	0.0002	0.0006
SVD	0.0039	0.0045	0.0029	0.0039
Nuclear				
CT-SVD	0.0001	0.0001	0.0001	0.0002
SVD	0.0017	0.0024	0.0021	0.0016
PET				
CT-SVD	0.0004	0.0005	0.0009	0.0010
SVD	0.0011	0.0014	0.0011	0.0013
Ultrasound				
CT-SVD	0.0001	0.0001	0.0001	0.0001
SVD	0.0033	0.0007	0.0009	0.0008
X-ray				
CT-SVD	0.0022	0.0018	0.0034	0.0042
SVD	0.0034	0.0038	0.0033	0.0036

The BER values of extracted watermarks are compared with the lowest of the values reported by Kim *et al*. (2010)

variations are confined to smaller regions in CT-SVD domain and scattered over large regions in the SVD domain. Classical watermarking systems demand the intactness of the extracted watermarks sufficient to be recognized by naked eye, for authentication or copyright protection applications. However, QR code based systems have a much rigorous requirement that the watermarks must be decodable by a QR code decoder.

The robustness of the proposed system against highly intensive noise attacks is attributed to the Hu's invariants and the stability of the SVs. We have shown that robustness can be achieved with three lower order Hu's invariant moments, instead of the entire set of seven invariants. The security of the proposed system is determined with these parameters: number of levels of contourlet decomposition, the size of the partitioned blocks, initial block selection and the number of iterations for Arnold Transform. The proposed system offers good degree of freedom to select these parameters within the permissible space. For example, the number of levels of contourlet decomposition and the size of the partitioned blocks depends upon the size of the watermark. In the proposed system, we have chosen these parameters such that the embedding block space is 128×128. Further, the initial block selection offers freedom to select any arbitrary block within this space. Above all, the number of iterations of the Arnold Transform determines the synchronization of the watermark. It is evident that any attempt to compromise the proposed system requires the adversary to know the exact values of these parameters. It would be highly unrealistic to determine the value of these parameters with a blind brute force attack due to the computational complexities. Further, another level of security can be added by permuting I_1, I_2 and I_3 for Master Share creation.

Table 8: Differences in master share with NC values

		Modality						
Attack	Domain	CT	Mammogram	MRA	Nuclear	PET	Ultrasound	X-ray
AWGN SNR: 1 dB	CT-SVD	0.9906	0.9389	0.9880	0.9880	0.9912	0.9936	0.9896
								
	SVD	0.9905	0.8845	0.9676	0.9669	0.9913	0.9917	0.9720
								
Poisson	CT-SVD	0.9952	0.9375	0.9915	0.9892	0.9974	0.9869	0.9923
								
	SVD	0.9927	0.8826	0.9737	0.9718	0.9932	0.9801	0.9847
								
Salt and pepper noise desnity: 1	CT-SVD	0.9952	0.9380	0.9951	0.9892	0.9981	0.9869	0.9936
								
	SVD	0.9927	0.8916	0.9859	0.9718	0.9949	0.9801	0.9906
								
Speckle variance: 0.8	CT-SVD	0.9952	0.9380	0.9918	0.9892	0.9977	0.9869	0.9934
								
	SVD	0.9927	0.8892	0.9801	0.9718	0.9934	0.9801	0.9857
								

However, we have observed that the proposed system is not robust with mammogram images in both the domains for all the noise attacks. This is attributed to the nature of the image we have taken. Black pixels are predominant in the left half of our mammogram image due to which the entire set of invariant moments of the partitioned blocks in this region are zeros. These moments get altered due to the introduction of noise and hence, the Master Shares differ for and unattacked images leading to imprecise watermark construction. Hence, it is required to formulate new approaches to counter this issue in medical images with small regions of interest. As an alternative, only the region of interest can be iteratively considered in computing the Master Share to achieve robustness.

CONCLUSION

In this study, we have proposed a zero watermarking system to embed a HL7 message in the form of a QR code for medical image authentication and improved radiology readings. The proposed system is implemented and tested in the CT-SVD and SVD domains. From the experimental results, we find that the composite CT-SVD domain provides better robustness to noise attacks rampant in medical images. The simplicity of the proposed system, its robustness, security and the infiltration of smart phones enabled with QR code readers, imply the practicability of deploying the system in healthcare institutions to provide better care to remote destinations deprived of in-house radiologists. The proposed system can be improved by identifying alternate transforms and their combinations for Master Share creation. This study signifies the need to carry out further research to identify invariants in medical images with smaller regions of interest which are highly vulnerable to attacks.

ACKNOWLEDGMENT

We acknowledge Richard Wheeler for granting us permission to illustrate the structure of the QR code.

REFERENCES

Alghoniemy, M. and A.H. Tewfik, 2000. Image watermarking by moment invariants. Proceeding of the IEEE International Conference on Image Processing, Volume 2, September 10-13, 2000, Vancouver, BC., Canada, pp: 73-76.

Alghoniemy, M. and A.H. Tewfik, 2004. Geometric invariance in image watermarking. IEEE Trans. Image Process., 13: 145-153.

Benjamin, M., Y. Aradi and R. Shreiber, 2010. From shared data to sharing workflow: Merging PACS and teleradiology. Eur. J. Radiol., 73: 3-9.

Chang, C.C. and J.C. Chuang, 2002. An image intellectual property protection scheme for gray-level images using visual secret sharing strategy. Pattern Recognit. Lett., 23: 931-941.

Chang, C.C., K.F. Hwang and M.S. Hwang, 1999. A block based digital watermarks for copy protection of images. Proceedings of the 5th Asia-Pacific Conference on Communications and Fourth Optoelectronics and Communications Conference, Volume 2, October 18-22, 1999, Beijing, China, pp: 977-980.

Chen, W.Y. and J.W. Wang, 2009. Nested image steganography scheme using QR-barcode technique. Opt. Eng., Vol. 48. 10.1117/1.3126646

Cordos, A., B. Orza, A. Vlaicu, S. Meza, C. Avram and B. Petrovan, 2010. Hospital information system using HL7 and DICOM standards. WSEAS Trans. Inform. Sci. Appl., 7: 1295-1304.

Cramer, B., G, Butler, J. Chalaoui, K. Silverthorn, L. Lepanto and D. Koff, 2008. CAR standards for teleradiology. http://www.car.ca/uploads/standards%20guidelines/Standard_Teleradiology_EN.pdf

Davis, K., 2012. Emergency workers scan QR codes for quick access to health info. http://www.computerworld.com/s/article/9227599/Emergency_workers_scan_QR_codes_for_quick_access_to_health_info

Do, M.N. and M. Vetterli, 2005. The contourlet transform: An efficient directional multiresolution image representation. IEEE Trans. Image Process., 14: 2091-2106.

Fan, T.Y., B.C. Chieu and H.C. Chao, 2012. Robust copyright-protection scheme based on visual secret sharing and Bose-Chaudhuri-Hocquenghem code techniques. J. Electron. Imaging, Vol. 21. 10.1117/1.JEI.21.4.043018

Ferdous, M., M. Ferdous and M. ShorifUddin, 2012. Invisible watermarking technique for copyright protection. J. Imaging Vision Res., 1: 2-6.

Garcia-Betances, R.I. and M.K. Huerta, 2012. A review of automatic patient identification options for public health care centers with restricted budgets. Online J. Publ. Health Inform., Vol. 4. 10.5210/ojphi.v4i1.4011

Gonzalez, R.C. and R.E. Woods, 2008. Digital Image Processing using MATLAB. 3rd Edn., Prentice Hall, New York.

Guo, H. and N.D. Georganas, 2003. A novel approach to digital image watermarking based on a generalized secret sharing scheme. Multimedia Syst., 9: 249-260.

HIPAA, 1996. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy, security and breach notification rules. http://www.hhs.gov/ocr/privacy/index.html.

Hsieh, S.L. and B.Y. Huang, 2004. A copyright protection scheme for gray-level images based on image secret sharing and wavelet transformation. Proceedings of the 31st Annual International Symposium on Computer Architecture, June 23, 2004, Munchen, Germany, pp: 661-666.

Hsu, C.S. and Y.C. Hou, 2005. Copyright protection scheme for digital images using visual cryptography and sampling methods. Opt. Eng., Vol. 44. 10.1117/1.1951647

Hu, M.K., 1962. Visual pattern recognition by moment invariants. IEEE Trans. Inform. Theory, 8: 179-187.

Huang, Z. and J. Leng, 2010. Analysis of Hu's moment invariants on image scaling and rotation. Proceedings of the 2nd International Conference on Computer Engineering and Technology, Volume 7, April 16-18, 2010, Chengdu, pp: V7-476-V7-480.

Kim, J., N. Kim, D. Lee, S. Park and S. Lee, 2010. Watermarking two dimensional data object identifier for authenticated distribution of digital multimedia contents. Signal Process.: Image Commun., 25: 559-576.

Lal, S., M. Chandra, G.K. Upadhyay and D. Gupta, 2011. Removal of additive gaussian noise by complex double density dual tree discrete wavelet transform. MIT Int. J. Electron. Commun. Eng., 1: 8-16.

Li, X.W., S.J. Cho and S.T. Kim, 2012. 2-D CAT-based medical image watermarking algorithm. Int. J. Comput. Theory Eng., 4: 722-725.

Liu, G., H. Liu and A. Kadir, 2012. Wavelet-based color pathological image watermark through dynamically adjusting the embedding intensity. Comput. Math. Methods Med., Vol. 2012. 10.1155/2012/406349

Naor, M. and A. Shamir, 1995. Visual Cryptography. In: Advances in Cryptology, De Santis, A. (Ed.). Springer, Berlin, Heidelberg, ISBN: 978-3-540-60176-0, pp: 1-12.

Nyeem, H., W. Boles and C. Boyd, 2013. A review of medical image watermarking requirements for teleradiology. J. Digital Imaging, 26: 326-343.

Prokop, R.J. and A.P. Reeves, 1992. A survey of moment-based techniques for unoccluded object representation and recognition. CVGIP Graph. Models Image Process., 54: 438-460.

Rahimi, F. and H. Rabbani, 2011. A dual adaptive watermarking scheme in contourlet domain for DICOM images. Biomed. Eng. Online, Vol. 10. 10.1186/1475-925X-10-53

Rawat, S. and B. Raman, 2012. A blind watermarking algorithm based on fractional Fourier transform and visual cryptography. Signal Process., 92: 1480-1491.

Sawatzky, A., 2011. (Nonlocal) Total variation in medical imaging. Ph.D. Thesis, Institute for Computational and Applied Mathematics, University of Munster, Germany.

Seenivasagam, V. and R. Velumani, 2013. A QR code based zero-watermarking scheme for authentication of medical images in teleradiology cloud. Comput. Math. Methods Med., Vol. 2013. 10.1155/2013/516465

Soon, T.J., 2008. QR code. Synth. J., 3: 59-78.

Tzouveli, P., K. Ntalianis and S. Kollias, 2006. Video object watermarking using Hu moments. Proceedings of the 13th International Conference on Systems, Signals and Image Processing, September 21-23, 2006, Budapest, Hungary, pp: 1-6.

Wang, M.S. and W.C. Chen, 2009. A hybrid DWT-SVD copyright protection scheme based on k-means clustering and visual cryptography. Comput. Stand. Interfaces, 31: 757-762.

Ye, T.Y., 2011. A robust zero-watermark algorithm based on singular value decomposition and discrete cosine transform. Parallel Distrib. Comput. Networks, 137: 1-8.