

Providing security and privacy to huge and vulnerable songs repository using visual cryptography

Shivendra Shivani¹ · Shailendra Tiwari¹ ·
Krishn K. Mishra² · Zhigao Zheng³ · Arun K. Sangaiah⁴

Received: 21 March 2017 / Revised: 6 September 2017 / Accepted: 20 September 2017 /
Published online: 2 October 2017

© Springer Science+Business Media, LLC 2017, corrected publication November/2017

Abstract In the today's scenario, the number of online song repositories such as iTunes, Hungama.com, etc. is increasing day-by-day. The reason for this can be attributed to the exponential growth in the Internet users in the past few years. These song repositories store huge number of songs (mostly in millions) and charge their users for listening and downloading them. With increased number of users requires more enhanced security measures to protect such vulnerable songs repository. Any breach in security of such song repositories would not only cause huge financial loss but also copyright infringement for the owners. Therefore, in this paper we have presented a novel and efficient approach for providing security and privacy to huge and vulnerable songs repository using visual cryptography. Presented approach not only provides confidentiality to the songs but also provides integrity verification with access control to the songs repository. We have also removed various basic security constraints of $(2, 2)$ visual cryptography existed in most of the state of art approaches like meaningless pattern of the shares, explicit codebook requirement, contrast loss, lossy recovery etc which are eliminated in the proposed approach.

Keywords Visual cryptography · Big data · Audio security · Meaningful shares · Songs repository

1 Introduction

Visual Cryptography (VC) is a kind of secret sharing scheme, first proposed by Naor et al. [18], which provides computation-less decoding of secret information (mainly images). k -out-

✉ Shivendra Shivani
shivendra.shivani@thapar.edu

¹ Thapar University, Patiala, India

² University of Missouri, Columbia, MO 65211, USA

³ Huazhong University of Science and Technology, Wuhan, China









⁴ VIT University, Vellore, India

of- n visual secret sharing (VSS) scheme is a special category of VC where a secret information is encoded into n meaningless shares and printed onto transparencies. These n transparencies are distributed among n participants. Secret image can be decrypted by only superimposing any k or more transparencies. Whereas $k - 1$ or fewer transparencies of the participants cannot decode the secret image, in spite of having in finite computation power. Secret sharing is not the only application of VC; there are many more other applications like access control, identification [17], copyright protection [6], watermarking and visual authentication. One can understand the modus operandi of VSS by Fig. 1 where 2-out-of-2 VSS ($k = 2; n = 2$) scheme is shown. Here a binary image is treated as secret information and each pixel p of secret binary image is encoded into a pair of black and white subpixels for both random shares.

If p is white/black, one of the first/last two columns tabulated under the white/black pixel in Fig. 1 is selected randomly so that selection probability will be 50%. Then, the first two subpixels in that column are allotted to share 1 and the following other two subpixels are allotted to share 2. Independent of whether p is black or white, pixel is encoded into two subpixels of black-white or white-black with equal probabilities.

Thus an individual share has no idea about whether p is black or white. The last row of Fig. 1 shows the superimposition of the two shares, If the pixel p is black, the output of superimposition will be two black subpixels corresponding to a gray level 1. If p is white, then result of superimposition will be one white and one black subpixel, corresponding to a gray level 1/2. Hence by stacking two shares together, we can obtain the approximate visual information of the secret image. Figure 2 shows a visual example of the 2-out-of-2 VSS scheme. Figure 2(a) shows a secret binary image I_{sec} which will be encrypted. As per the encoding scheme shown in Fig. 1, each binary pixel p of I_{sec} is divided into two subpixels in each shares, as shown in Fig. 2(b) and (c). Stacking the two shares leads to the output image shown in Fig. 2(d). The recovered image is decoded without any cryptographic computation. There are some contrast loss which can be noticed in decoded image and the width of the reconstructed image is just twice of the original secret image. In this paper, proposed approach uses the concepts of visual cryptography in order to secure digital audios. There are many researches done in literature which are based on image security. Our foundation for audio watermarking in cloud environment is basically comes from the image based security approaches in cloud. Zhihua Xia et al. suggested a scheme in [24] that supports Content based Image Retrieval (CBIR) over encrypted images without leaking the sensitive information to the cloud server. Zhihua Xia et al. proposed a secure multi-keyword ranked search scheme over encrypted cloud data in [23], which simultaneously supports dynamic update operations like deletion and insertion of documents. Specifically, the vector space model and the widely-used TF x IDF model are combined in the index construction and query generation. A novel color image watermarking scheme is presented by Jianzhong Li et al. in [15] which is based on quaternion Hadamard transform (QHT) and Schur decomposition,. In order to consider the correlation between different color channels and the significant color information, a new color

Fig. 1 2-out of 2 VSS, where a secret pixel is encoded into two subpixels in each of the two shares

Pixel		
Probability	50%	50%
Share 1		
Share 2		
Stack Share 1 & 2		

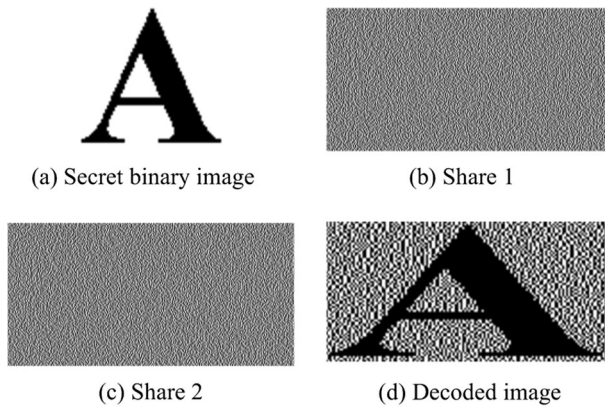


Fig. 2 Example of 2 out of 2 VSS. Secret image is encoded into two random patterns and decoded image has 50% contrasts

image processing tool termed as the quaternion Hadamard transform is also proposed in [15]. A parallel processing approach for images in order to improve the efficiency more than five times in comparison to existing approaches are also presented in [1].

Digital audio watermarking is an important technique to secure and authenticate audio media. We generally classify the existing designs into time domain and transform domain methods, and relate all the reviewed works on audio security with either audio watermarking technique or audio steganography or audio encryption technique [12]. There are various state of art approaches are present in literature to secure the audio signals. Audio signals can be secured by either audio watermarking or basic cryptography techniques. Hu Hwai et al. [10] proposed Robust, transparent and high-capacity audio watermarking in DCT domain. Due to frequency domain, the complexity of this scheme is high. Vivekannad Bhatt et al. [3] proposed an adaptive audio watermarking based on the singular value decomposition in the wavelet domain. This scheme is a hybrid version of both domains viz. frequency and spatial. A perceptual-based DWPT-DCT framework for selective blind audio watermarking is proposed in [11] which is motivated by the human auditory perception. This scheme provides robustness and imperceptibility with respect to the original and recovered audio signal. Al-nuaimy et al. proposed a different type of audio encryption technique in [2] which is based on chaotic encrypted images and SVD. Pranab Kumar et al. proposed a blind SVD-based audio watermarking using entropy and log-polar transformation in [5]. Here copyright protections of audio signals are done using log-polar transformation (LPT). A different kind of audio watermarking is proposed in [13] where multiple watermarks are embedded into the cover signals in order to check the authenticity of the signal. Two novel covert communication techniques are present in [14, 16] using spreadsheets and multi-scroll chaotic system respectively.

Besides aforementioned audio watermarking approaches, there are several state of art audio encryption or data hiding techniques presented in literature. Hemalatha S et al. proposed a integer wavelet transform based audio data hiding technique in [9] which provides high embedding capacity and good imperceptibility to cover signal. Phase coding and LSB based audio steganography presented in [7]. This technique provides both facilities: data fragmentation as well as data encryption. A novel audio steganography technique presented in [25] which is based on block based XOR operations of LSBs. This approach can withstand steganalysis attacks. S Shivani et al. proposed a speech secret sharing approach in [20] which uses the concept of visual cryptography, but this approach only provides confidentiality and

does not provide integrity verification. Reference [19] provides an approach for verifiable visual cryptography in which each share are capable enough to authenticate itself for any tampering. Approach presented in [19] is made for secretly transmitting the images but unable to transmit audio signals.

There is no effective algorithm present in literature for audio security which provides all security requirements like confidentiality, integrity, authentication etc. in a single approach. Proposed approach combines the concepts of VC in audio and addresses obvious problems of VC like random pattern of the shares, lossy recovery of secret, explicit generation of codebook.

The remaining sections of the paper are structured as follows. Proposed approach is described in Section 2. To show the effectiveness of the proposed approach, the experimental results and comparisons with various states of art approaches are discussed in Section 3. Paper is concluded in Section 4.

2 Proposed approach for providing security and privacy to songs using visual cryptography

There are many websites like itunes, hungama.com etc. which provide access (to listen or download) to songs on payment basis to their authentic users. Their servers are nothing but the huge songs repository which must be secured in order to unauthentic access. Since these songs repositories store songs without any encryption hence these are more vulnerable for attacks. If a repository is compromised due to any infiltration attack then the website owner may be treated as convict for copyright violation. Hence these all songs on repository must be kept in repository in secure manner so that in spite any attack, no one will be able to infer the theme of songs. The basic visualization of repository, authentic users and attacker are shown in Fig. 3. Here we can see that if attacker decrypts the single bottleneck point anyhow, then he can

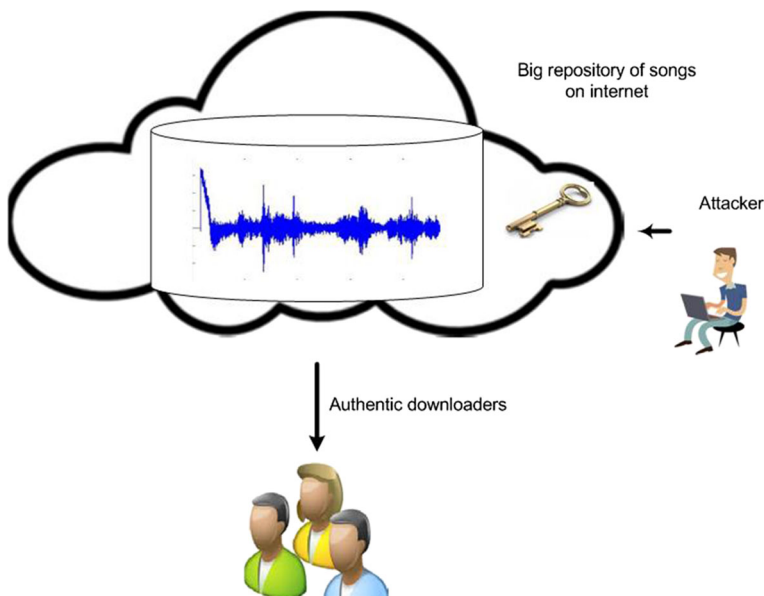


Fig. 3 Visualization of insecure repository of songs

access all songs without any interruption. We have presented an efficient approach in this paper to avoid this type of scenario. Proposed approach is a brand new type of audio security scheme which is nothing but the fusion of image and audio processing with their all basic features. In this approach we are applying the visual cryptography secret sharing approach on audio bit stream. This approach generates two meaningful image shares which are actually embedded with audio files. Meaningful shares provide confidentiality to secret. At the same time proposed approach inherits the properties of 2 out of 2 visual cryptography. It means that, at the receiver end one can decrypt the secret audio if and only if he has both meaningful shares. Otherwise nothing will be decoded. Both shares are self authenticated. If there will be any intentional or unintentional alteration on shares that can be tracked by proposed approach. Most of the previous state of art approaches on image secret sharing generates meaningless shares. Actually randomness of the shares increases the vulnerability for cryptanalysis, hence some meaningful information like registered trademark or any copyright logo are added to the shares. Besides these constraints there are some other limitations like predefine codebook is also removed in proposed approach. Predefined (Explicit) codebook causes excessive memory requirement and overhead at both the sender and receiver end. One can visualize the relations among songs repository, authentic users and attackers in Fig. 4. Here we can see that a song is dividing into two visually meaningful shares which are verifiable in nature. Both shares will be stored in two different repositories. Now if an attacker breaches the security of either repository, he has only meaningful images instead of songs. If he tampers the share images then due to verifiability we can simply detect that shares are not authentic.

Novelty of the proposed approach:

Proposed Audio security approach provides following features:

1. Meaningful shares
2. Confidentiality to secret audio file by converting it into images.

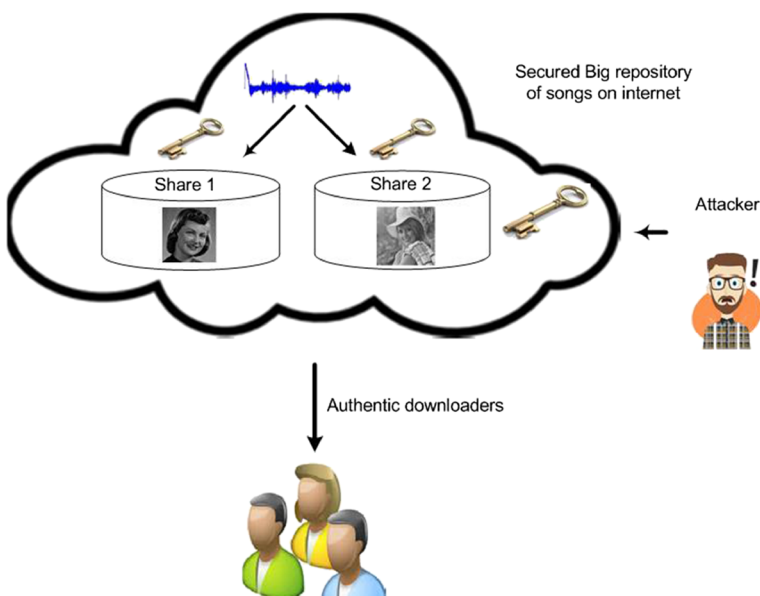


Fig. 4 Visualization of secure repository of songs using proposed approach

3. Implicit generation of codebook.
4. Access control by providing the features of 2 out of 2 Visual Cryptography
5. Each share is self authenticating in nature.

Proposed song security approach using Visual Cryptography is outlined in Fig. 5. There are seven steps to generate two self authenticating meaningful shares for a secret audio file. These seven steps mainly include creation of basis matrices, creation of secret shares then meaningful shares, creation of self authenticating shares, tamper detection, audio extraction and finally secret recovery. Audio signals are recorded in the form of unsigned eight bit integer and each sample is converted into eight bit binary forms. Combined binary vector of each sample is denoted as vector S_b . Step 1 takes S_b as input to generate basis matrix. Step 2 takes basis vector V as input and generate two binary secret vector $S_b^{e_1}$ and $S_b^{e_2}$. Meaningful shares are generated in step 3 by using two cover images C_1 and C_2 (which are going to be displayed on shares), output of this step is denoted by C_{share1} and C_{share2} respectively. In step 4 these meaningful shares are converted into self authenticating shares and denoted by C_{vs1} and C_{vs2} . Due to self authentication feature in shares one can easily track the any mishandled or leaked share in step 5 which was very difficult in previous state of the art approaches. If shares are authentic and unaltered then we can extract the secret shares of audio signals in step 6. Finally audio signals are regenerated in step 7. The detailed description of each steps are discussed next subsections.

2.1 Basis matrix creation

Let $W = \{W_0, \dots, W_{n-1}\}$ be a set of participants which includes all sender and receiver of audio signals. According to Visual Cryptography scheme a secret binary bit stream S_b is encoded into n images which are called secret shares. Let $\Gamma_{Qual} \subseteq 2^W$ and $\Gamma_{Forb} \subseteq 2^W$ where 2^W is power set of W and $\Gamma_{Qual} \cap \Gamma_{Forb} = \emptyset$. The members of Γ_{Qual} are refereed as qualified set and members of Γ_{Forb} are refereed as forbidden set. The pair $(\Gamma_{Qual}, \Gamma_{Forb})$ is called access structure of VSS.

Secret audio signal can be decoded by only qualified set of participants $X \in \Gamma_{Qual}$ whereas any participants $Y \in \Gamma_{Forb}$ cannot decode the secret.

Algorithm 1 Algorithm for Basis Matrix Creation (BMC)

INPUT: b .

OUTPUT: V .

Define: 1) b is single bit

2) V is matrix of dimension 2×2 where $V(1)$ and $V(2)$ Indicate 1st and 2nd row of V

1: **procedure BMC(b)**

2: **if** $b = 0$ **then**

3: $V(1) \leftarrow 01$ or 10

4: $V(2) \leftarrow 01$ or 10

5: **else**

6: $V(1) \leftarrow 01$ or 10

7: $V(2) \leftarrow 01$ or 01

8: **end if**

9: Return b

10: **end procedure**

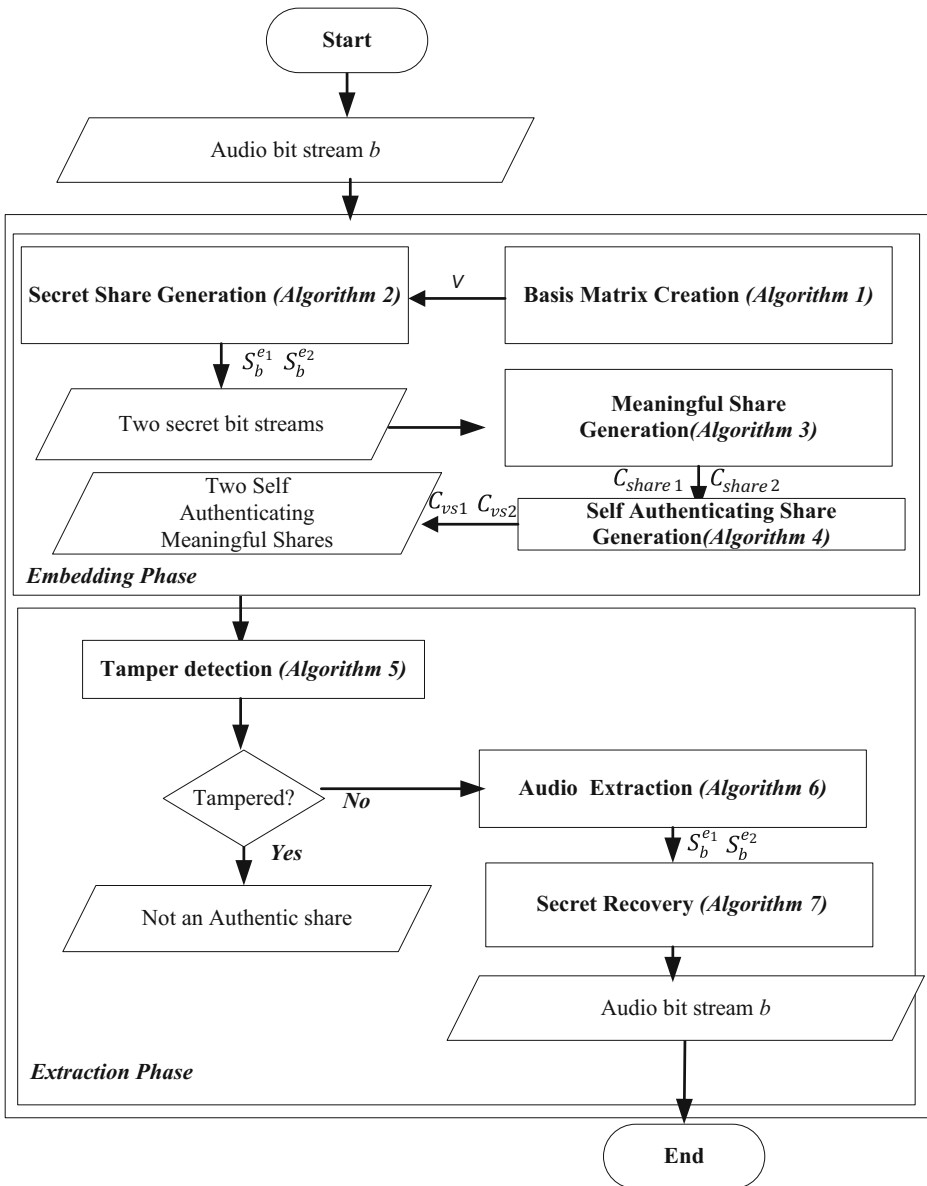


Fig. 5 Flow chart for proposed Self Authenticating Audio Secret Sharing approach

Example-2.1 Let $(\Gamma_{Qual}, \Gamma_{Forb})$ be an access structure for n participants. Proposed Audio secret sharing approach has been taken the concept 2 out of 2 visual cryptography. In case of proposed 2 out of 2 VC approach, if two participants $\{1, 2\}$ are given for an access structure $(\Gamma_{Qual}, \Gamma_{Forb})$, then $\Gamma_{Forb} = \{\{1\}, \{2\}\}$ and $\Gamma_{Forb} = \{\{1, 2\}\}$. $\Gamma_{Forb} = \{\{1\}, \{2\}\}$. Since secret information can be achieved by computing two shares.

In proposed approach pixel expansion m is obtained corresponding to each secret sample of audio for all n shares. Pixel expansion m will be denoted by $n \times m$ boolean matrix M . Let r_i be the i^{th} ($i = 1, 2, 3 \dots, n$) row of M which contains subpixels for i^{th} share. Let $X = \{i_1, i_2 \dots i_s\}$ be the subset of the row of M which will be assigned to s participants. Here OR-logical operation on the corresponding row r_{ik} ($k = 1, 2, 3 \dots s$) of M can be used to simulate the superimposing operations of shares in X . Result of this operation is a row vector $V (V = OR(r_{i_1}, r_{i_2}, \dots, r_{i_s}))$. The Hamming weight of V is approximation of gray level of superimposed pixel p and denoted by $w(V)$.

Definition-2.1 [26] Let $(\Gamma_{Qual}, \Gamma_{Forb})$ be an access structure for n participants. Two $n \times m$ boolean matrices $S_{i,j \in \{0,1\}}^{ij}$ are called basis matrices, if the sets C^{ij} are obtained by permuting columns of S^{ij} in all possible ways, respectively, S^{ij} satisfy the following two conditions.

1. Contrast condition: If $X = \{i_1, i_2 \dots i_u\} \in \Gamma_{Qual}$, the row vectors V_0 and V_1 (for extreme white and black combination of bits) obtained by doing OR operation on rows $i_1, i_2 \dots i_u$ of S^{ij} respectively, satisfy

$$w(V_0) \leq t_X - \alpha(m) \times m \tag{1}$$

and

$$w(V_1) \geq t_X \tag{2}$$

2. Security condition: Any subset $X = \{i_1, i_2 \dots i_v\} \in \Gamma_{Forb}$ of v participants has no information of the secret signal. The collection of two matrices $D_j (j = 0, 1)$ of size $v \times m$ formed by extracting rows $i_1, i_2 \dots i_v$ from each matrix C^{ij} are indistinguishable.

Where t_X is the threshold to interpret the reconstructed sample as black or white and $\alpha(m)$ is called the relative difference referred to as the contrast of the decoded signal, it can be obtained by

$$t_X = \min(w(V_1(X, M))) \tag{3}$$

where $M \in C_1$

$$\alpha(m) = \frac{\min(w(V_1(X, M))) - \max(w(V_0(X, M)))}{m} \tag{4}$$

The matrix M is randomly selected from C^{ij} for any signal sample.

Proposed *Algorithm 1* is used to create two basis matrices V of size $n \times m$ for binary bit 1 and 0. Two encoding sets of V can also be obtained by permuting the columns of respective V .

First of all each sample signal is converted into eight bit binary form. Basis matrix is generated for each binary bit of sample.

Example-2.2 Let $n=2$ and V^0, V^1 be the two basis matrices for two different bits 0 and 1 of sample of signal. According to algorithm 1 $V^0 = [10 \ 10]$ and according to algorithm 1 $V^1 = [01 \ 10]$.

One can see that single row of matrix V^i contains only single 1 and 0 for each binary signal sample. Hence it will be very difficult to find belonging sample by insufficient number of share. One can also take the different permutations of column of basis matrix by following way

$$V^0 = \left\{ \left[\begin{array}{c} 10 \\ 10 \end{array} \right], \left[\begin{array}{c} 01 \\ 01 \end{array} \right] \right\}$$

$$V^1 = \left\{ \left[\begin{array}{c} 10 \\ 01 \end{array} \right], \left[\begin{array}{c} 01 \\ 10 \end{array} \right] \right\}$$

Once we get the basis matrices for binary bits of S_b , we proceed further for next algorithm.

2.2 Secret share generation

In this step we take the generated basis matrices as input. Two random bit streams S_b^{e1} and S_b^{e2} are generated by concatenating the elements of first and second rows of V respectively as shown in Algorithm 2. The length of S_b^{e1} and S_b^{e2} is $2 \times \text{length}(S_b)$. Now these two bit streams will be passed to next step in order to generate meaningful shares.

Algorithm 2 Algorithm for Secret Share Generation(SSG)

INPUT: S_b .

OUTPUT: S_b^{e1}, S_b^{e2} .

Define: 1) \parallel shows the concatenation operation.

2) V is matrix of dimension 2×2 where $V(1)$ and $V(2)$

Indicate 1st and 2nd row of V

1: **procedure** SSG(S_b)

2: **for** $i \leftarrow 1$ to $\text{length}(S_b)$ **do**

3: $V \leftarrow \text{Call}(BMC(S_b(i)))$

4: $S_b^{e1} \leftarrow S_b^{e1} \parallel V(1)$

5: $S_b^{e2} \leftarrow S_b^{e2} \parallel V(2)$

6: **end for**

7: Return S_b^{e1}, S_b^{e2}

8: **end procedure**

2.3 Creation of meaningful secret shares

Two meaningful binary cover images C_1 and C_2 are required as template to generate two meaningful secret images C_{share1} and C_{share2} . If the size of C_1 and C_2 is $M \times N$ then length of $S_b^{e1} = \frac{M \times N}{4}$. According to Algorithm 3, C_1 and C_2 will be divided into 2×2 non overlapping blocks and hence each bit of S_b^{e1} and S_b^{e2} will be assigned to respective block of C_1 and C_2 .

2.4 Creation of self authenticating meaningful secret shares

Shares are most sensible objects because they carry secret information; hence they must be untampered and authentic before decoding. To achieve this objective we need to create self authenticating or verifiable shares which are capable enough to track their tampered region. Algorithm 4 is used to generate two verifiable meaningful secret shares C_{vs1} and C_{vs2} . Self embedding technique is used to create a single authentication bit for each block of size 2×2 of C_{share1} and C_{share2} .

Example-2.3 Let us consider a block of C_{share1} is [11 01] as an input to this Algorithm 4. If corresponding rows β and columns γ for each bit of given block are [row\col. 37 38 10211 10301]. According to Algorithm 4 to calculate self embedding authentication bit, we do XOR between secret bits with fifth MSB of their corresponding row and column values.

Algorithm 3 Algorithm for Meaningful Share Generation (MSG)

INPUT: S_b^{e1}, S_b^{e2}, C_1 and C_2 .

OUTPUT: C_{share1}, C_{share2} .

Ensure:

- (1) $B_{C_1}^k$ is k^{th} block of C_1 where $k = 1$ to $\frac{M \times N}{4}$.
 - (2) $B_{C_1}^{k,d}$ is d^{th} bit of k^{th} block of C_1 where $k = 1$ to 4.
 - (3) $S_b^{e1}(d)$ is d^{th} bit of S_b^{e1} secret bit stream.
 - (4) $B_{C_{share1}}^k$ is d^{th} bit of k^{th} block of C_{share1} where $k = 1$ to 4.
 - (5) $d \leftarrow$ Random number from 1 to 4.
 - 1: **for** $k = 1$ to $\frac{M \times N}{4}$ **do**
 - 2: $B_{C_1}^{k,d} \leftarrow S_b^{e1}(d)$
 - 3: $B_{C_2}^{k,d} \leftarrow S_b^{e2}(d)$
 - 4: $B_{C_{share1}}^k \leftarrow B_{C_1}^k$
 - 5: $B_{C_{share2}}^k \leftarrow B_{C_2}^k$.
 - 6: **end for**
 - 7: **return** C_{share1}, C_{share2} .
-

Algorithm 4 is used to generate single authentication bit A_u for each block of C_{share1} and C_{share2} .

Algorithm 4 Algorithm for Self Authenticating Meaningful Share Generation

INPUT: C_{share_1}, C_{share_2} .

OUTPUT: C_{vs_1}, C_{vs_2} .

Ensure:

- (1) β_{ij}, γ_{ij} are row and column of the $(i, j)_{th}$ pixel respectively.
 - (2) $b^u(P)$ indicates the of u^{th} bit of pixel P.
 - (3) P_{ij} is $(ij)^{th}$ bit of C_{share_k} where $k \in \{1,2\}$.
 - (4) A_{s_1} and A_{s_2} are two empty vectors of size 1×4 .
 - (5) \wedge is bit wise AND operator
 - (6) \parallel is sign of concatenation.
- 1: \forall block B of size 2×2 of C_{share_k}
 - 2: for $i \leftarrow 1$ to 2 **do**
 - 3: for $j \leftarrow 1$ to 2 **do**
 - 4: $A_{s_1} \leftarrow A_{s_1} \parallel ExOr(b^5(\beta_{ij}), P_{ij})$
 - 5: $A_{s_2} \leftarrow A_{s_2} \parallel ExOr(b^5(\gamma_{ij}), P_{ij})$
 - 6: $A_u \leftarrow \{\sum_{u=0}^3 (A_{s_1}^u \wedge A_{s_2}^u)\} mod 2$
 - 7: $B(R) \leftarrow A_u$
 - 8: **end for**
 - 9: **end for**
 - 10: $C_{vs_k} \leftarrow C_{share_k}$
 - 11: **return** C_{vs_1}, C_{vs_2} .
-

2.5 Tamper detection

One can only get the actual authentic secret audio signal at receiver end, when share are not tampered intentionally or unintentionally during transmission. Hence before decoding the secret audio signal, we must check the both shares for alteration. Algorithm 5 is used to identify the tampered pixel for both shares. Here we just extract the R^{th} pixel of each block of size 2×2 of C_{vs_1} and C_{vs_2} and recalculate it by Algorithm 4. Now bit wise comparison is done between extracted and recalculated bit matrices. If any mismatch found then that pixel will be marked as tampered one.

Algorithm 5 Algorithm for Tamper Detection

INPUT: C_{vs_1}, C_{vs_2} .

OUTPUT: Tampered Region

- 1: $\forall B$ of of C_{vs_k}
 - 2: Calculate A_u for block B using Algorithm 4
 - 3: $A_u^e \leftarrow B(R)$
 - 4: **if then** $A_u \neq A_u^e$
 - 5: Mark B as tampered block
 - 6: **end if**
 - 7: **return** Tampered Block.
-

2.6 Audio extraction

Once we realize that received meaningful shares are not intentionally or unintentionally altered then we extract the secret bits of audio signals from each meaningful shares using algorithm 6.

Algorithm 6 Algorithm for Audio Extraction

INPUT: C_{vs_1}, C_{vs_2} .

OUTPUT: $S_b^{e_1}$ and $S_b^{e_2}$

1: $\forall B$ of of C_{vs_1}

2: $S_b^{e_1} \leftarrow S_b^{e_1} \parallel B(d)$

3: $\forall B$ of of C_{vs_2}

4: $S_b^{e_2} \leftarrow S_b^{e_2} \parallel B(d)$

5: **return** $S_b^{e_1}$ and $S_b^{e_2}$.

2.7 Secret audio signal recovery

Secret audio signal recovery of proposed approach require little bit computation. In this phase, according to Algorithm 7, after verifying the authenticity of both shares C_{vs_1} and C_{vs_2} , secret signal recovery is done. To recover a samples, we need to both bit streams $S_b^{e_1}$ and $S_b^{e_2}$.

Algorithm 7 Algorithm for audio signal recovery

INPUT: $S_b^{e_1}, S_b^{e_2}$.

OUTPUT: S_r .

Define: 1) S_r is a vector of length same as S_b

2) \parallel is sign of concatenation.

1: **procedure** $SD(S_b)$

2: **while** $i \neq \text{length}(S_b^{e_1})$ **do**

3: $B \leftarrow OR(S_b^{e_1}(i, i-1), S_b^{e_2}(i, i-1))$

4: **if** $B = 01$ **then**

5: $S_r \leftarrow S_r \parallel 0$

6: **else**

7: $S_r \leftarrow S_r \parallel 1$

8: **end if**

9: $i \leftarrow i + 1$

10: **end while**

11: **Return** S_r

12: **end procedure**

Au is a kind of fragile watermark which is produced by self embedding technique. Fragile watermark is destroyed after any intentional or unintentional attack on cover signal [21]. In proposed approach cover signal is nothing but the audio samples. Block wise authentication is done for tampered meaningful share. Au bit is generated for each

block of size 2×2 by using Algorithm 4. If a single bit will be changed in original, we can track that received signal is not authentic.

2.8 Performance analysis

Self Authenticating meaningful shares C_{vs_1} and C_{vs_2} must satisfy the contrast and security conditions. Since we are dealing with binary cover images, hence the values of objective evaluation parameters between C_k & C_{vs_k} must be satisfactory enough.

Lemma 1 Imperceptibility between C_k & C_{vs_k} must be satisfactory enough in terms of objective evaluation parameters.

Since two bits of a block of size 2×2 of C_{share_k} is altered in order to make C_{vs_k} . One bit is dedicated for verifiability of block whereas other one bit is dedicated for secret audio signal. Remaining two bits are the visible information of the cover image. Hence only 50% information is different between cover image C_k and C_{vs_k} , hence imperceptibility must belong to an acceptable range.

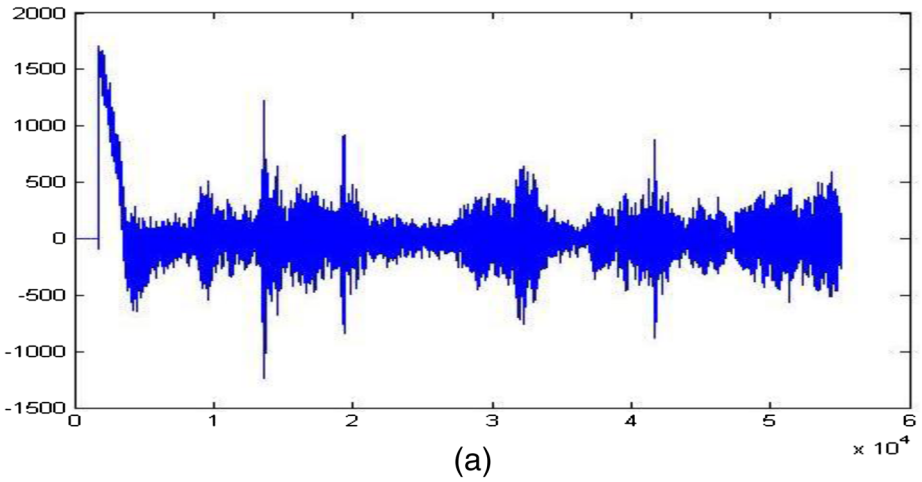
Lemma 2 Original Audio signal S_b will be recovered as it is if C_{vs_k} will be unaltered.

If C_{vs_k} is unaltered then S_b can be recovered as it is at receiver end. Because one can extract secret audio signals from bit d of each block of size 2×2 of C_{vs_k} and both extracted share will be computed in order to recover the audio.

3 Experimental results and comparisons

Experiments have been performed on various audio signals. Here we have taken all audio signals in unsigned eight bit integer form so that it's sample can be easily converted into eight bit binary form. Proposed self authenticating audio secret sharing approach has been verified and illustrated for two shares. All cover images are taken in halftone format using existing error diffusion technique because it looks like gray scale image. Figure 6 shows overall gist of our proposed approach. Figure 6 (a) shows the graphical representation of the secret audio signal which are to be transmitted securely. Images (b) and (c) are self authenticating meaningful shares C_{vs_1} and C_{vs_2} respectively. Image (d) is nothing but the recovered signal at the receiver end. We can see here that recovered secret audio signal at receiver end is same as original one, since there is no tampering is done on self authenticating meaningful share.

Each share is embedded with authentication bits generated by self embedding techniques in order to verify its integrity. If any tampering will be done intentionally or unintentionally during offline storage or transmission, it can be easily tracked by proposed approach. Figure 7 demonstrate the integrity verification of shares, where images (a) original secret audio signal and (b) are tampered version of the original one. One can easily identify the authenticity of shares using algorithm 5. White pixels in Fig. 7 (c) show the tampered portion of share. Tamper localization is done without the help of original share. Since block based authentication is done here hence alteration in a single bit leads the whole block as tampered. Table 1 shows the accuracy of tamper detection. Here we tabulated the tampering results of four self



(b)



(c)

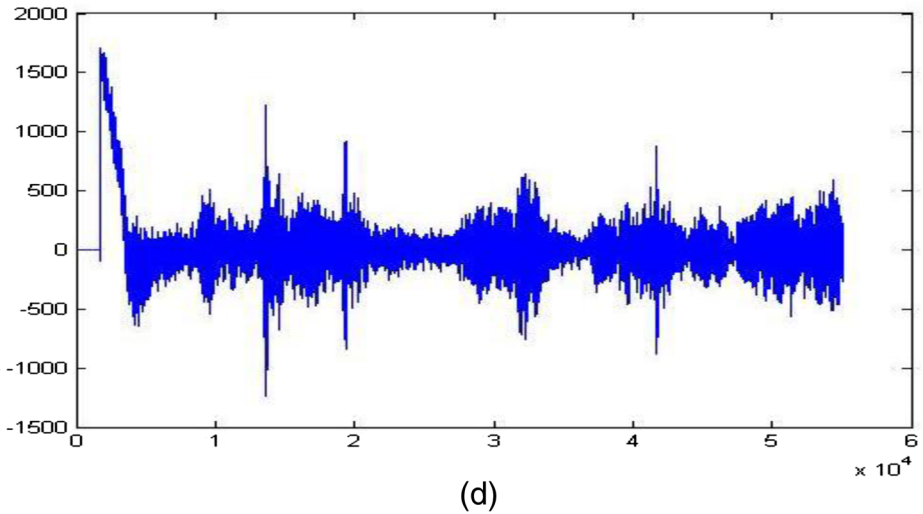
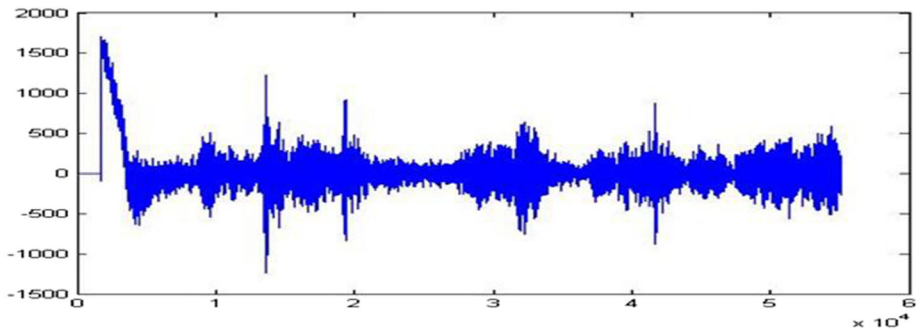


Fig. 6 **a** Original audio signal S_b , **b** Self authenticating meaningful share C_{vs1} , **c** Self authenticating meaningful share C_{vs2} **d** Recovered audio signal



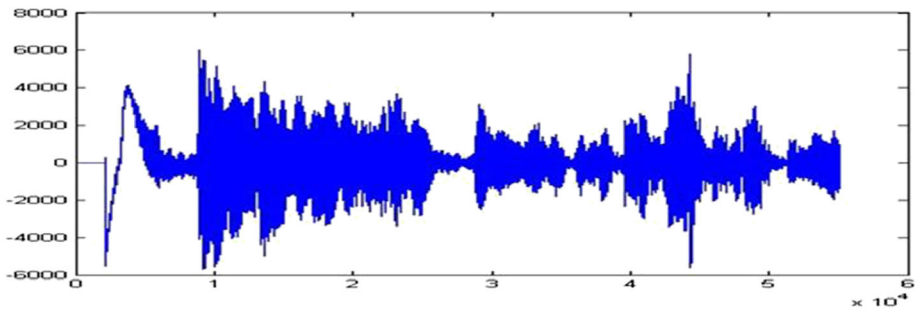
(a)



(b)



(c)



(d)

Fig. 7 **a** Original audio secret signal, **b**Tampered version of self authenticating meaningful share C_{vs_k} , **c** Detected pixels, **d** Modified audio signal at the receiver end

Table 1 Alteration detection accuracy of proposed approach

Shares	No. of altered pixels	No. of altered pixels	Accuracy
Face	1420	1500	94.6%
Baboon	1710	1849	92.4%
Girl	1117	1200	93.0%
Barbara	715	891	80.2%

Table 2 The comparison of relative reports on VC

Method	Lossless recovery	Meaningful Share	Share authentication	Codebook Generation
Rimba et al. [4]	No	No	No	Explicit
Shinya Washio [22]	Yes	No	No	Implicit
Hemalatha S [8]	No	Yes	No	Implicit
Proposed Approach	Yes	Yes	Yes	Implicit
Ideal Values	Yes	Yes	Yes	Implicit

authenticating meaningful shares. One can observe that tamper localization is done with very satisfactory level.

3.1 Comparison of relative reports on VC

Proposed approach is a very new and different kind of audio secret sharing approach which is not proposed in literature till now. Various essential qualitative characteristics of Visual cryptography and secret sharing have been considered to compare the proposed approach with existing approaches on audio secret sharing as shown in Table 2. Few of qualitative parameters for comparison of VC are described as follows:

1. Contents of shares: Most of the existing algorithms generate shares which are random in nature. These shares are highly vulnerable for cryptanalysis and also may be cause of confusion in share identification. Hence there should be some meaningful information on shares. This information may be any additional information about shares or share holders.
2. Contrast $\alpha(m)$ of the Share: The value of contrast (m) must be as high as possible so that the quality of meaningful share image C_{vs_k} remains same as original cover image C_k . Since for security issues there are some contrast loss in all VC schemes, hence this contrast loss must be minimized.
3. Security Criteria: Any subset of Γ_{Forb} must show no information about the secret audio signal and for Γ_{Forb} rows from any matrix of $V_{j(j \in \{0, 1\})}$ must be indistinguishable with respect to S_b .
4. Codebook Requirement: Most of the existing algorithms on secret sharing require codebook, explicitly, at the time of encoding and decoding process. Codebooks are nothing but a pattern of all combinations of basis matrices which are decided for various possibilities of signal samples. Since explicit codebooks are very difficult to manage and require excessive static memory for storing, hence explicit requirement of codebook is biggest overhead for any secure sharing algorithm.
5. Share authentication: Shares are very important and sensible primitives in secret sharing hence they must be protected during any transmission. Self embedding method is best way to protect the shares because extra authentication images are not required in this case.
6. Lossless decryption of secret signal: One cannot compromise with the original audio secret signals because lossy recovery may change the entire meaning.

There are lots of other approaches on audio security present in literature which can be compared with the proposed mechanism but in Table 2 we have compared only those latest approaches on audio security which can be defined by aforementioned qualitative parameters.

4 Conclusions

In this paper a novel approach for self authenticating audio using visual cryptography with meaningful shares has been proposed for securely storing various songs on huge repository. Proposed method eliminates various basic security constraints of visual cryptography like random pattern of shares, explicit codebook requirement, contrast loss, lossy recovery etc. Proposed approach basically uses the concept of 2 out of 2 visual cryptography scheme where both secret shares are visually meaningful which provide confidentiality (vital security requirement) to secret audio signal during transmission. All blocks of size 2×2 of both meaningful shares C_{share_k} are contained with self embedding authentication bits which is a kind of block based fragile watermark that confirms authentication and content based integrity of both shares and hence secret audio signal. The experimental results and comparison with the most of the existing state of art approaches in all aspects of audio security show the effectiveness of proposed self authenticating audio security approach.

References

1. Al-Ayyoub M, AlZu'bi S, Jararweh Y, Shehab MA, Gupta BB (2016) Accelerating 3D Medical Volume Segmentation Using GPUs. Springer, MTAP
2. Al-Nuaimy W, El-Bendary MAM, Shafik A, Shawki F, Abou-El-azm AE, El-Fishawy NA, Elhalafawy SM et al (2011) An SVD audio watermarking approach using chaotic encrypted images. *Digital Signal Process* 21(6):764–779
3. Bhat V, Sengupta I, Das A (2010) An adaptive audio watermarking based on the singular value decomposition in the wavelet domain. *Digital Signal Process* 20(6):1547–1558
4. Ciptasari RW, Rhee K-H, Sakurai K (2014) An enhanced audio ownership protection scheme based on visual cryptography. *EURASIP J Inf Secur* 1(1):2
5. Dhar PK, Shimamura T (2015) Blind SVD-based audio watermarking using entropy and log-polar transformation. *JISA* 20:74–83
6. Fu MS, Au OC (2004) Joint visual cryptography and watermarking. *Int. Conf. Multimedia and Expo in Proc. IEEE, Taipei, Taiwan*
7. George JT, Arokiaaraj Jovith A (2016) A Fragmented Approach: Audio Steganography using Phase Coding and LSB. *Int J Appl Eng Res* 11(7):5228–5230
8. Hemalatha S, Dinesh Acharya U, Renuka A (2015) Wavelet Transform Based Steganography Technique to Hide Audio Signals in Image. *Procedia Comput Sci* 47:272–281
9. Hemalatha S, Dinesh Acharya U, Renuka A (2016) Audio data hiding technique using integer wavelet transform. *Int J Electron Secur Digit Forensics* 8(2):131–147
10. Hu H-T, Hsu L-Y (2015) Robust, transparent and high-capacity audio watermarking in DCT domain. *Signal Process* 109:226–235
11. Hu H-T, Hsu L-Y, Chou H-H (2014) Perceptual-based DWPT-DCT framework for selective blind audio watermarking. *Signal Process* 105:316–327
12. Hua G, Huang J, Shi YQ, Goh J, Thing VLL (2016) Twenty years of digital audio watermarking—a comprehensive review. *Signal Process* 128:222–242
13. Khalil M, Adib A (2014) Audio watermarking with high embedding capacity based on multiple access techniques. *Digital Signal Process* 34:116–125
14. Lee C-W, Tsai W-H (2013) A covert communication method via spreadsheets by secret sharing with a self-authentication capability. *J Syst Softw* 86(2):324–334
15. Li J, Yu C, Gupta BB, Ren X (2017) Color image watermarking scheme based on quaternion Hadamard transform and Schur decomposition. Springer, MTAP
16. Liu H, Kadir A, Li Y (2016) Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and one-time keys. *Optik-Int J Light and Electron Optics* 127(19):7431–7438
17. Naor M, Pinkas B (1997) Visual authentication and identification. *Crypto97, LNCS*, vol. 1294, pp 322340
18. Naor M and Shamir A (1995) Visual cryptography, *Advances in Cryptography: EUROCRYPT94, LNCS, Perugia, Italy*, vol. 950, pp. 112

19. Shivani S, Agarwal S (2016) VPVC: Progressive Verifiable Visual Cryptography. *Pattern Anal Applic* Doi: <https://doi.org/10.1007/s10044-016-0571-x>, ISSN 1433-7541
20. Shivani S, Agarwal S (n.d.) Speech Secret Sharing. *Advances in Computer Science and Information Technology (ACSIT)* p-ISSN: 2393-9907; e-ISSN: 2393-9915, Vol. 3, Issue 2
21. Singh D, Shivani S, Agarwal S (2013) Quantization-based fragile watermarking using block-wise authentication and pixel-wise recovery scheme for tampered image. *Int J Image Graph* 13(02):1340002
22. Washio S, Watanabe Y (2014) Security of audio secret sharing scheme encrypting audio secrets with bounded shares. In 2014 I.E. International Conference on Acoustics, Speech and Signal Processing (ICASSP) Florence, pp. 7396–7400
23. Xia Z, Wang X, Sun X, Wang Q (2015) A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data. *IEEE Trans Parallel Distrib Syst* 27(2):340–352
24. Xia Z, Wang X, Zhang L, Qin Z, Sun X, Ren K (2016) A Privacy-preserving and Copy-deterrence Content-based Image Retrieval Scheme in Cloud Computing. *IEEE Trans Inf Forensics Secur* 11(11):2594–2608
25. Zarepour-Ahmadabadi J, Ahmadabadi MES, Latif AM (2016) An adaptive secret image sharing with a new bitwise steganographic property. *Inform Sci* 369:467–480
26. Zhou Z, Arce GR, Di Crescenzo G (2006) Halftone visual cryptography. *IEEE Trans Image Process* 15(8): 24412453



Shivendra Shivani is currently working in Thapar University, Patiala as Lecturer. He has received his B.E. degree, in computer science and engineering from CSVTU in 2009, after that he has completed master degree from National Institute of Technology Allahabad, India in Information security in 2011. He has received Ph.D. degree from National Institute of Technology Allahabad, India with Visual Cryptography as an area of interest. His current research interest includes Digital watermarking, Pattern Recognition, Computer Vision, Algorithms, Compression, Biometrics, Visual Cryptography and Face recognition.



Shailendra Tiwari is currently a Lecturer in CSE Department, Thapar University Patiala. He received his PhD in Computer Science & Engineering from the Indian Institute of Technology (BHU) in 2016, and ME degree in CSE from the Punjab Engineering College (PEC) University of Technology, Chandigarh, India in 2008. His research interests include image processing and computer vision, medical image reconstruction, segmentation algorithm in medical imaging, optimisation techniques and other non-invasive problem estimation.



Krishn K. Mishra has received his PhD degree from National Institute of Technology, Allahabad, India. Currently he is working in Department of Mathematics and Computer Science, University of Missouri, USA. His current research interest includes Genetic Algorithm, Neural Network, Digital watermarking, Pattern Recognition, Multimedia Security etc.



Zhigao Zheng is with Services Computing Technology and System Lab/Cluster and Grid Computing Lab/Big Data Technology and System Lab, School of Computer Science and Technology, Huazhong University of Science and Technology. He is the guest editor of ACM/Springer Mobile Networks and Applications, Multimedia Tools and Applications, Journal of Intelligent & Fuzzy Systems, Computers & Electrical Engineering, International Journal of Networking and Virtual Organisations (IJNVO) and so on, he is also the reviewer of many journals such as IEEE Transactions on Big Data, IEEE Transactions on Industrial Informatics, Journal of Network and Computer Applications, The Journal of Supercomputing, Multimedia Tools and Applications and some top conference such as SC'16, CCGrid'16, NPC'15 and NPC'16. His main research interest is focused on parallel and distributed computing. He is a member of CCF, IEEE and ACM.



Arun Kumar Sangaiah has received his Master of Engineering (ME) degree in Computer Science and Engineering from the Government College of Engineering, Tirunelveli, Anna University, India. He had received his Doctor of Philosophy (PhD) degree in Computer Science and Engineering from the VIT University, Vellore, India. He is presently working as an Associate Professor in School of Computer Science and Engineering, VIT University, India. His area of interest includes software engineering, computational intelligence, wireless networks, bio-informatics, and embedded systems