VMVC: Verifiable multi-tone visual cryptography

Shivendra Shivani[1]

Received: 23 August 2016 / Revised: 30 December 2016 / Accepted: 20 January 2017

Abstract Traditional k out of n threshold visual cryptography scheme is proposed to hide a secret image into n shares, where only k or more shares can visually reveal the secret image. Most of the previous state of art approaches on visual cryptography are almost restricted in processing of binary images as secret, which are inadequate for many applications like securely transmission of medical images(Store and Forward Telemedicine), forensic images etc. In this paper, a new Verifiable Multi-toned Visual Cryptography (VMVC) scheme is proposed to securely transmit the confidential images on web. Proposed approach also provides cheating prevention, since each pixel of shares contains a self embedding verifiable bit for integrity test of that pixel. Many existing approaches are suffering from many unnecessary encryption constraints like random shares, codebook requirement, contrast loss etc, which all are successfully addressed in proposed approach. Some comparisons with previously proposed methods are also made. Experimental results and analysis are used to prove the efficiency of proposed approach.

Keywords Verifiable visual cryptography · Multi-toned visual cryptography · Secret sharing · Meaningful shares

1 Introduction

Visual Cryptography (VC) is a category of secret sharing scheme, proposed by Naor et al. [17], that allows computation-less decoding of secret images. Mainly in a k-out-of-n visual secret sharing (VSS) scheme, a secret image is encoded into n noise-like shares and printed onto transparencies to distribute them among n participants. Secret image can be decoded by just stacking any k or more transparencies. In spite of using infinite computation power,

✉ Shivendra Shivani
shivendra.shivani@thapar.edu

[1] Thapar University, Patiala, India

Published online: 21 February 2017

$k-1$ or fewer participants can not decode the secret image. Besides the secret sharing, visual cryptography can also be used for number of other purposes including access control, watermarking, copyright protection [5], identification [16] and visual authentication. To demonstrate the working of VSS, consider a 2-out-of-2 VSS ($k=2, n=2$) scheme shown in Fig. 1. Each pixel p of secret binary image is encoded into a pair of black and white subpixels for both 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 alloted to share 1 and the following other two subpixels are alloted 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 an example of the 2-out-of-2 VSS scheme. Figure 2a shows a secret binary image I_{sec} to be encoded. According to the encoding scheme shown in Fig. 1, each pixel p of I_{sec} is divided into two subpixels in each shares, as shown in Fig. 2b and c. Stacking the two shares leads to the output image shown in Fig. 2d. The decoded image is clearly revealed. There are some contrast loss and the width of the reconstructed image is just twice of the original secret image.

The 2-out-of-2 VSS scheme shown above is a special case of the k-out-of-n VSS scheme. A more general model for VSS schemes based on general access structures has been designed by Ateniese et al. in [1]. An access structure is a specified set of all the qualified and forbidden subsets of the shares. The secret image can be decoded by the participants of a qualified subset only. The capabilities of VSS has also been enhanced by allowing gray scale images as secret rather than a binary image [15].

All aforementioned VC methods suffer with problem of noise-like share and may lead to suspicion to cryptanalysis. Shares having meaningful informations are more desirable in terms of the steganography aspect. To overcome this problem, Ateniese et al. [2] proposed the concept of extended visual cryptography (EVC). In EVC, the shares contain both, the secret information along with the meaningful cover images. Secret images can still be revealed only when qualified shares are superimposed together. Shares of EVC scheme, however, provide very low quality visual information of secret image. Nakajima et al. [18] extended the EVC approach for natural gray scale images to improve the visual quality of images. Shyong jian [19] has proposed a visual cryptography approach for color images but problem of noise-like shares continued. To generate meaningful shares, Zhou and Arce [26] proposed Halftone Visual Cryptography (HVC). In Comparison with EVC, the quality of the meaningful shares and reconstructed image are greatly improved in HVC.

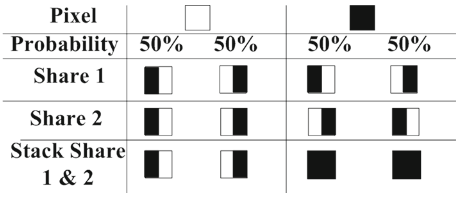

Fig. 1 2-out of 2 VSS, where a secret pixel is encoded into two subpixels in each of the two shares

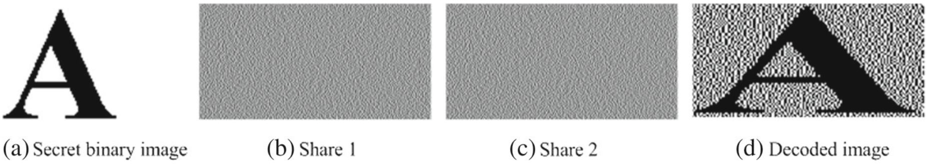
(a) Secret binary image (b) Share 1 (c) Share 2 (d) Decoded image

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

The main disadvantage of this approach is the pixel expansion value, since each pixel is replaced by a halftone cell which is much larger than the pixel itself. One pair of complimentary shares is also required to suppress the visual information of the cover image in the decoded image. Zhonmin et al. [22] has proposed extended version of HVC in which Auxiliary Black Pixel(ABP) is used in place of complimentary shares. Again the disadvantage of this approach is large cell size which increases the size of shares and decoded image.

Most of the previous state of art approaches on visual cryptography are almost restricted in processing of binary images as secret, which are inadequate for many applications like secretly transmitting the multi-toned medical or court evidence images on the web. We can not limit the power of VC for only binary images, hence concept of visual cryptography with gray and color images came into picture.

1.1 Visual cryptography with multi-tone images

Halftone(binary) images as secret are only suitable when we deal with document images. But most of the time we deal with natural and live images for various applications. Sometimes reduction in intensity ranges of secret pixels at decoding phase may loose sensitive and important information of secret image. We can understand it by an analogy:

Let us consider a hospital associated with various scan and diagnosis centers. If unfortunately, expert doctor who deals with medical images is unavailable then we have to transmit the medical images (MRI, CT Scan, X-Ray etc all are in JPEG or any two dimensional format) on the web to be examined by experts. Medical images are very sensible images hence they must be transmitted securely with 100 % recovery assurance because missing or changing of any pixel intensity may mislead to doctors. This type of new security requirements diverted the attention of researchers in new dimension of visual cryptography i.e visual cryptography with multi-tone images.

Carlo et al. [3] defined and analyzed visual cryptography schemes for gray level images. They gave a necessary and sufficient condition for such schemes to exist. They proved the optimality of (k, k, m, g) GVCS. Dau-shun et al. [24] proposed a new gray scale nRVCS with minimum pixel expansion and also proposed an optimal-contrast gray scale RVCS (GRVCS) by using basis matrices of perfect black nRVCS. Finally, they designed an optimal-contrast GRVCS with a minimum number of shares held by each participant. Yasushi Yamaguchi [25] introduced a scheme for extended visual cryptography for continuous-tone images. The scheme is based on parallel error diffusion that can quickly encrypt images with no pixel expansion. The most important feature of this scheme is the optimum tone mapping so that the resulting images may have very high contrast comparing with the conventional schemes. D. Taghaddos et al. [21] proposed a new variant of visual cryptography for gray-scale images. They used bit-level decomposition to extract binary bit planes from a gray-scale image. Then the bit planes are encrypted and recomposed back as two gray-scale shares. The secret image is revealed when two gray-scale shares are superposed.

Shares are very important and sensible objects because they carry secret information, hence tracking of mishandled or tampered share is very essential task. To achieve this objective , a new aspect of VC came into picture i.e. Verifiable Visual Cryptography(VVC).

1.2 Verifiable visual cryptography (VVC)

Security of visual cryptography scheme is defined under the assumption that all the participants involved are trustworthy. Recovered secret is compromised, if any one of the participants acts as cheater and tries to alter the shares. Hence, there is need for Verifiable Visual Cryptography (VVC). Tsai et al. [8] proposed an image-sharing scheme that combines VC and steganography. In this scheme, secrets are divided into multiple parts that are hidden in the bit-planes of a set of cover images to form stego-images. The objective of this scheme is to prevent anyone who processes only one stego-image from gaining information about the secret. In 2007, Horng et al. [9] proposed a method to identify cheaters with the cost of additional authentication shares which authenticate the integrity of shares prior to stacking them. This method is not computationally effective as well as pixel expansion and noise like shares bring extra cost of managing shares. Wang et al. [23] proposed a visual sharing method with verification ability which first applies few equations to encode a watermark image and a secret image into two unexpanded sharing image. This is followed by scrambling of two sharing images using torus automorphism. In this scheme, it is difficult to manage meaningless shares and Torus automorphism consumes time to scramble images. Hao-Kuan Tso proposed a scheme [20] in which gray scale image is converted to bit plane images and each bit plane image along with seed and verification image encoded image is produced. This scheme is capable of producing meaningless shares with unexpanded shares, however meaningless shares are not realistic images and hence still attracts attacker's attention. Most of the verifiable visual cryptography schemes have the issues of bad recovering quality, pixel expansion, computational complexity, security and accuracy, additional image for authentication etc.

There are various principles and characteristics of VC which must be satisfied by any valid algorithm. Since Verifiable Visual Cryptography(VVC) and Multi-toned Visual Cryptography both are subsets of traditional VC, hence they must follow the common fundamental principles.

1.3 Fundamental principle of visual cryptography

Let $W = \{W_0, ...W_{n-1}\}$ be a set of participants. A VC scheme for a set W is a method to encode a secret binary image I_{sec} into n shares, where each participant in W will receive one secret share. Let $\Gamma_{Qual} \subseteq 2^W$ and $\Gamma_{Forb} \subseteq 2^W$ where 2^W is power set of W and $\Gamma_{Qual} \cap \Gamma_{Forb} = \phi$. 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.

Any qualified set of participants $X \in \Gamma_{Qual}$ can visually reveal the I_{sec} but any partcipants $Y \in \Gamma_{Forb}$ can not. VSS is defined by two parameters: the pixels expansion m which is the number of subpixels in which each pixel p of the secret image I_{sec} is encoded for each share and the contrast α which is the measurement of the difference of a black and white pixel in the decoded image.

Each secret binary pixel p is converted in to m subpixels for each of the n shares. A boolean matrix M of size $n \times m$ is used to describe these subpixels, where value 0 is used to denote white subpixel and value 1 is used for black subpixel. Let r_i be the i^{th} $(i = 1, 2, 3.., n)$ row of M which contains subpixels for i^{th} share. The hamming weight $w(v)$of vector v is proportional to the visual intensity of p where $v = OR(r_{i_1}, r_{i_2}..r_{i_s})$ and $r_{i_1}, r_{i_2}...r_{i_s}$ are the rows of M.

Definition 1.1 [26]: Let $(\Gamma_{Qual}, \Gamma_{Forb})$ be an access structure for n participants. The collections of boolean matrices C_0 and C_1, each of dimension $n \times m$ constitute a VSS scheme where m denotes pixel expansion, if there exist $\alpha(m)$ and t_X for every $X \in \Gamma_{Qual}$ satisfying the following:

1. **Contrast condition:** Any qualified subset $X = \{i_1, i_2..., i_u\} \in \Gamma_{Qual}$ can decode the I_{sec} by stacking the respective transparencies. Formally, for matrix $M \in C_j, (j = 0, 1)$, the row vector $v_j(X, M) = OR(r_{i_1}, r_{i_2}..r_{i_s})$. It holds $w(v_0(X, M)) \leq t_X - \alpha(m).m \forall m \in C_0$ and $w(v_1(X, M)) \geq t_X \forall m \in C_1$. Where $\alpha(m)$ is contrast of reconstructed image and t_X is threshold to visually interpret the reconstructed pixel as black or white.
2. **Security condition:** Any forbidden subset $X = \{i_1, i_2..., i_v\} \in \Gamma_{Forb}$ of v participants has no clue about the secret image.

An access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ must satisfy both above mentioned conditions for any VC scheme.

There is no effective algorithm present in literature for Verifiable Multi-toned Visual Cryptography(VMVC) which addresses all aforementioned and obvious problems of VC in single approach like pixel expansion of secret image, random pattern of the shares, low contrast of the recovered secret, explicit generation of codebook, additional image requirement for authentication etc. In this paper, we have proposed series of algorithms which resolves all disadvantages of state of art approaches in efficient manner by providing verifiable multi-toned meaningful shares, generated by implicit codebook.

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

2 Proposed verifiable multi-toned visual cryptography (VMVC) approach

Proposed VMVC approach is a fusion of VVC and MVC approaches with their all basic features. It also removes many unnecessary encryption constraints present in existing state of art approaches like random pattern of the shares, codebook requirement, contrast loss etc . Randomness of the shares increases the vulnerability for cryptanalysis and may create confusion in share identification in case of large number of participants. Hence to minimize the difficulty for managing the huge number of shares, some meaningful information should be added. These meaningful information may be any additional information about shares or share holders like registered trademark or any copyright logo, to prevent the mishandling or theft of the shares. Besides these constraints there are some other limitations like explicit requirement of codebook and contrast loss. Explicit codebook causes excessive memory requirement and overhead at both the sender and receiver end while contrast loss is also a big problem since it may suppress the important and sensible information of the secret image. Shares are very sensible objects so it is vital task to verify their integrity and authenticity before stacking.

Proposed Verifiable Multi-toned Visual Cryptography Approach removes all above mentioned problems of VC by providing following features:

1. Meaningful shares
2. Unexpanded secret image
3. Multi-toned shares
4. Implicit generation of codebooks.
5. All shares contain their own authentication information generated by self embedding technique.
6. Constant contrast of secret during recovery as 100 %

Proposed Verifiable Multi-toned Visual Cryptography Approach is outlined in Fig. 3. There are five steps to generate two self authenticating meaningful shares a secret image I_{sec}. These five steps mainly include creation of basis matrices, creation of multi-toned shares with verifiable bits, tamper detection and credentials extraction. Step 1 takes at a time two bits of a pixel of I_{sec} as input to generate basis matrix. Step 2 takes a multi-tone secret image I_{sec} and two cover images C_1 and C_2 (which are going to be displayed on shares)

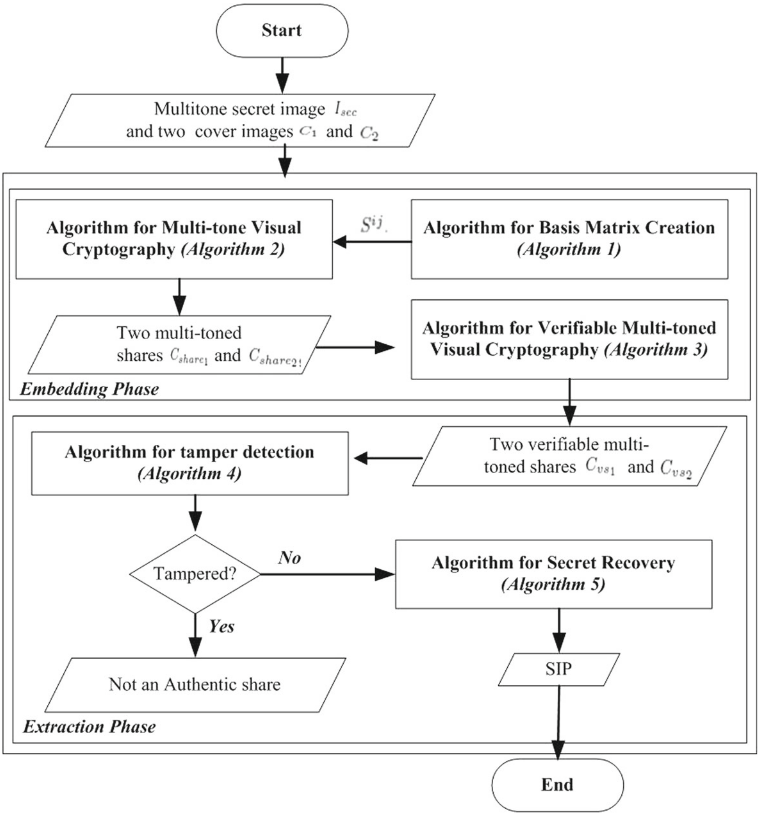
Start
Multitone secret image I_{sec} and two cover images C_1 and C_2
Algorithm for Multi-tone Visual Cryptography (Algorithm 2)
S^{ij}
Algorithm for Basis Matrix Creation (Algorithm 1)
Two multi-toned shares C_{share_1} and C_{share_2}
Algorithm for Verifiable Multi-toned Visual Cryptography (Algorithm 3)
Embedding Phase
Algorithm for tamper detection (Algorithm 4)
Two verifiable multi-toned shares C_{vs_1} and C_{vs_2}
Tampered?
No
Algorithm for Secret Recovery (Algorithm 5)
Yes
Not an Authentic share
SIP
Extraction Phase
End

Fig. 3 Flow chart for proposed VMVC approach

as input along with generated basis matrices to create two multi-toned meaningful shares C_{share_1} and C_{share_2}. Due to meaningful information on shares one can easily track the any mishandled or leaked share which was very difficult for random shares, if large number of participants are there. In step 3 a verifiable bit is generated by self-embedding technique for each pixel of shares to prevent the cheating to check the authenticity of shares. The output of this step is denoted by C_{vs_1} and C_{vs_2}. According to property of self-embedding bit, it will be destroyed after any alteration on share and thus altered location of a share can be easily marked. Hence tamper detection and secret image extraction can be done in step 4 and 5 respectively. The detailed description of each steps are discussed next subsections.

2.1 Basis matrix creation

Let $W = \{W_0, \ldots W_{n-1}\}$ be a set of participants. A Visual Cryptography scheme for a set W is a method to encode a secret binary image I_{sec} into n images called shares, where each participant in W will receive one secret share. Let $\Gamma_{Qual} \subseteq 2^W$ and $\Gamma_{Forb} \subseteq 2^W$ where 2^W is power set of W and $\Gamma_{Qual} \cap \Gamma_{Forb} = \phi$. 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.

Any qualified set of participants $X \in \Gamma_{Qual}$ can visually reveal the I_{sec} but any participants $Y \in \Gamma_{Forb}$ can not. VSS is defined by two parameters: the pixels expansion m and the contrast α, α is the measurement of the difference of a black and white pixel in the decoded image.

Example 2.1 Let $(\Gamma_{Qual}, \Gamma_{Forb})$ be an access structure for n participants. In case of proposed 2 out of 2 VMVC approach, if two participants $\{1, 2\}$ are given for an access structure $(\Gamma_{Qual}, \Gamma_{Forb})$, then $\Gamma_{Forb} = \{\{1\}, \{2\}\}$ and $\Gamma_{Qual} = \{\{1, 2\}\}$ as secret information can be achieved by stacking two shares.

In proposed approach pixel expansion m is obtained corresponding to each secret gray pixel for all n shares. Pixel expansion m will be denoted by $n \times m$ boolean matrix M. Here value 0 is used for white subpixel and 1 is for black subpixel. Let r_i be the i^{th} $(i = 1, 2, 3.., n)$ row of M which contains subpixels for i^{th} share. Let $X = \{i_1, i_2, i_3 \ldots i_s\}$ be the subset of the row of M which will be assigned to s participants. Here OR-logical operation on the corresponding row $r_{i_k}(k = 1, 2, 3..s)$ of M can be used to simulate the superimposing operations of shares in X. Result of this operation is a row vector V $(V = OR(r_{i_1}, r_{i_2}, \ldots r_{i_s}))$. The Hamming weight of V is approximation of gray level of superimposed pixel p and denoted by $w(V)$.

Definition 2.1 [22]: Let $(\Gamma_{Qual}, \Gamma_{Forb})$ be an access structure for n participants. Two $n \times m$ boolean matrices $S^{ij}_{i,j \in \{0,1\}}$ are called basis matrices, if the four sets C^{ij} are obtained by permuting the first & second and third & fourth columns of S^{ij} in all possible ways, respectively, S^{ij} satisfy the following two conditions.

1. **Contrast condition:** If $X = \{i_1, i_2 \ldots, i_u\} \in \Gamma_{Qual}$, the row vectors V_0 and V_1 (for extreme white and black combination of bits) obtained by doing OR operation on rows $i_1, i_2 \ldots i_u$ 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 $X = \{i_1, i_2 ..., i_v\} \in \Gamma_{Forb}$ of v participants has no information of the secret image. The collection of two matrices $D_j (j = 0, 1)$ of size $v \times m$ formed by extracting rows $i_1, i_2 ..., i_v$ from each matrix C^{ij} are indistinguishable.

Where t_X is the threshold to visually interpret the reconstructed pixel as black or white and $\alpha(m)$ is called the relative difference referred to as the contrast of the decoded image, 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 SIPs.

Proposed Algorithm 1 is used to create four basis matrices S^{ij} of size $n \times m$ and four encoding sets C^{ij} which are obtained by permuting the columns of respective S^{ij}. First of all each SIP is converted into eight bit binary form. These eight bits are further collected as four combinations of two bits which are denoted as ij. Therefore four basis matrices are generated for each SIP.

Algorithm 1 Basis Matrix Creation (BMC)

```
INPUT: i,j.
OUTPUT: $S^{ij}$.
Ensure:
    (1) $S^{ij}$ is empty matrix of size $2 \times 4$ where $S_r^{ij}$ indicates $r^{th}$ row.
    (2) Initialize $S_1^{ij}$ by any of the four bits vector element from ([1010], [0110], [1001], [0101])

if $i \neq j$ then
    if $i = 0$ then
        $S_2^{ij} \leftarrow$ ([1001], [0101], [1010], [0110])    ▷ Assign one element corresponding to $S_1^{ij}$.
    else
        $S_2^{ij} \leftarrow$ ([0110], [1010], [0101], [1001])    ▷ Assign one element corresponding to $S_1^{ij}$.
    end if
else
    if $i = 0$ then
        $S_2^{ij} \leftarrow$ ([1010], [0110], [1001], [0101])    ▷ Assign one element corresponding to $S_1^{ij}$.
    else
        $S_2^{ij} \leftarrow$ ([0101], [1001], [0110], [1010])    ▷ Assign one element corresponding to $S_1^{ij}$.
    end if
end if
return$S^{ij}$
```

Example 2.2 Let S^{00}, S^{01}, S^{10} & S^{11} be the indications of four basis matrices for two different bits of secret image of a VC scheme having $n = 2$. For a particular index of the secret image, S^{ij} represents two bits of eight bit binary representation of secret image pixel. Algorithm 1 is applied in order to calculate the basis matrices by following way:

For S^{00}:

Initially $S_1^{00} = [1010]$ which is taken randomly from the vector ([1010], [0110], [1001], [0101]) According to Algorithm 1, choose [1010]'s corresponding value to represent 00 i.e S_2^{ij} = [1010] hence $S^{00} = \begin{bmatrix} 1010 \\ 1010 \end{bmatrix}$

For S^{01}

Initially S_1^{01} = [0110] which is taken randomly from the vector ([1010], [0110], [1001], [0101])

According to Algorithm 1, choose [0110]'s corresponding value to represent 01 i.e S_2^{ij} = [0101] hence $S^{01} = \begin{bmatrix} 0110 \\ 0101 \end{bmatrix}$

For S^{10}

Initially S_1^{10} = [1001] which is taken randomly from the vector ([1010], [0110], [1001], [0101])

According to Algorithm 1, choose [1001]'s corresponding value to represent 10 i.e S_2^{ij} = [0101] hence $S^{10} = \begin{bmatrix} 1001 \\ 0101 \end{bmatrix}$

For S^{11}

Initially S_1^{11} = [0101] which is taken randomly from the vector ([1010], [0110], [1001], [0101])

According to Algorithm 1, choose [0101]'s corresponding value to represent 11 i.e S_2^{ij} = [1010] hence $S^{11} = \begin{bmatrix} 0101 \\ 1010 \end{bmatrix}$

hence basis matrices for S^{00}, S^{01}, S^{10} and S^{11} are as follows:

$$S^{00} = \begin{bmatrix} 1010 \\ 1010 \end{bmatrix} \quad S^{01} = \begin{bmatrix} 0110 \\ 0101 \end{bmatrix} \quad S^{10} = \begin{bmatrix} 1001 \\ 0101 \end{bmatrix} \quad S^{11} = \begin{bmatrix} 0101 \\ 1010 \end{bmatrix}$$

One can see that single row of matrix S_{ij} contains only two 1 and two 0s or its different permutations for SIP 0 and 1 both. Hence it will be very difficult to find belonging SIP by insufficient number of share. According to Algorithm 1 the collection of basis and encoding matrices C^{ij} for S^{ij} can be written as

$$\begin{aligned} C^{00} &= \{[\,10101010\,] \quad ,[\,01100110\,] \quad ....[\,01010101\,]\} \\ C^{01} &= \{[\,10101001\,] \quad ,[\,01100101\,] \quad ....[\,01010110\,]\} \\ C^{10} &= \{[\,10100110\,] \quad ,[\,01011001\,] \quad ....[\,10010101\,]\} \\ C^{11} &= \{[\,10100101\,] \quad ,[\,01101001\,] \quad ....[\,10010110\,]\} \end{aligned}$$

One can see that C^{ij} can be obtained by the different permutations of first and second columns as well as third and fourth columns of S^{ij}. For S^{ij} contrast and security condition can be verified. $t_X = min(w(V_1(X, M)))$ where $M \in C^{ij}$, since here we are taking all rows of M so $\forall w(V_1) = \{4\}$ hence $t_X = 4$ and $max(w(V_0)) = 2$. Since pixel expansion $m = 4$ hence $\alpha(m) = \frac{1}{2}$. For contrast condition $w(V_0) \leq t_X - \alpha(m) \times m$ and $w(V_1) \geq t_X$ must be satisfied that is $2 \leq 4 - (\frac{1}{2} \times 4)$ or $2 \leq 2$ and $4 \geq 4$. Actually this contrast value is intermediate value and only applicable when human visual system is used for decryption but in proposed approach a little bit computation is also required which enhances the contrast as 100 %. Γ_{Forb} contains all the isolated shares and for ensuring the security condition we have to show that any single row of C_j is indistinguishable. There will be number of permutations of only one combination of 0 and 1 that is 1100 in C^{ij}. One can not infer the belonging SIP. Once we get the four basis matrices for eight bit binary value of a secret information pixel, we proceed further for next algorithm.

2.2 Creation of multi-toned meaningful secret shares

Two meaningful cover images C_1 and C_2 are required as template to generate two multi-toned meaningful secret images C_{share_1} and C_{share_2}. According to Algorithm 2, first rows of all four basis matrices for a SIP are embedded into four LSBs of first cover image. Similarly second rows of all four basis matrices for same SIP are embedded into four LSBs of second cover image. One can understand it by Example 2.3.

Example 2.3 In order to create the meaningful shares, let us consider an instance when SIP is 55 and its corresponding 2 × 2 blocks of C_1 and C_2 are $\begin{bmatrix} 128 & 36 \\ 29 & 10 \end{bmatrix}$ and $\begin{bmatrix} 17 & 99 \\ 21 & 59 \end{bmatrix}$ respectively. The eight bit binary representation of SIP, C_1 and C_2 are 00110111, $\begin{bmatrix} 10000000 & 00100100 \\ 00011101 & 00001010 \end{bmatrix}$ and $\begin{bmatrix} 00010001 & 01100011 \\ 00010101 & 00111011 \end{bmatrix}$ respectively. As per the Algorithm 1, there are four basis matrices generated for four pairs of binary bits of SIP. Basis matrices for SIP 55 are $S^{00} = \begin{bmatrix} 1010 \\ 1010 \end{bmatrix}$, $S^{11} = \begin{bmatrix} 1001 \\ 0110 \end{bmatrix}$, $S^{10} = \begin{bmatrix} 1010 \\ 1001 \end{bmatrix}$ and $S^{10} = \begin{bmatrix} 0101 \\ 1010 \end{bmatrix}$. Algorithm 2 takes these basis matrices and binary representation of blocks as input and rearrange the first four LSBs of each pixel of both blocks according to corresponding basis matrix. Now the resultant binary representation of blocks will be as $C_{share_1} = \begin{bmatrix} 10001010 & 00101001 \\ 00011010 & 00000101 \end{bmatrix}$ and $C_{share_2} = \begin{bmatrix} 00011010 & 01100110 \\ 00011001 & 00111010 \end{bmatrix}$. Final multi-toned meaningful secret shares will be denoted as $C_{share_1} = \begin{bmatrix} 138 & 41 \\ 26 & 5 \end{bmatrix}$ and $C_{share_2} = \begin{bmatrix} 26 & 102 \\ 25 & 58 \end{bmatrix}$ respectively which are imperceptibly similar as their original values. Similarity analysis will be considered in next section.

Algorithm 2 Algorithm for Multi-tone Visual Cryptography (MVC)

```
INPUT: $I_{sec}$ of size $n \times m$ and two different gray cover images $C_1$ and $C_2$ of size $2n \times 2m$.
OUTPUT: $C_{share_1}, C_{share_2}$.
Ensure:
    (1) $V_{sec}$ is vector of $I_{sec}$ taken row wise.
    (2) $V_{c_1}$ and $V_{c_2}$ are vectors of blocks having dimension $2 \times 2$ of cover images $C_1$ and $C_2$ respectively.
    (3) Size of $V_{sec}$, $V_{c_1}$ and $V_{c_2}$ is $1 \times (n \times m)$.
    (4) $B_{\alpha}^{V_{c_k}}$ is $\alpha^{th}$ block of vector $V_{c_k}$ where size of $\alpha = 1 \times (n \times m)$ and $k = 1, 2$.
    (5) $B_{\alpha}^{V_{c_k}}(a)$ indicates $a^{th}$ pixel of block where $a = 1to4$.
    (6) $b^u$ is $u^{th}$ bit of 8 bit vector $b$.

for $\alpha = 1$ to $n \times m$ do
    $b \leftarrow \lfloor \frac{V_{sec}(\alpha)}{2^u} \rfloor mod2$                ▷ Where $u = 0, 1, , 7$
    $v \leftarrow 1, a \leftarrow 1$
    while $v \neq 8$ do
        $S^{ij} \leftarrow BMC(b^v, b^{v+1})$
        $B_{\alpha}^{V_{c_k}}(a) \leftarrow S_k^{ij}$     ▷ Embed the row vector of $S_k^{ij}$ to four LSBs of $B_{\alpha}^{V_{c_k}}(a)$.
        $v \leftarrow v + 2$
        $a \leftarrow a + 1$
    end while
    Assign all updated blocks of $V_{c_1}$ and $V_{c_2}$ to $C_1$ and $C_2$ respectively to form
    $C_{share_1}, C_{share_2}$.
end for
return$C_{share_1}, C_{share_2}$
```

2.3 Creation of verifiable multi-toned 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 3 is used to generate two verifiable multi-tone secret shares C_{vs_1} and C_{vs_2}. Self embedding technique is used to create a single authentication bit for each pixel of C_{share_1} and C_{share_2}. One can understand the working of Algorithm 3 by Example 2.4.

Example 2.4 In order to add verifiability in the meaningful shares, let us consider a previously processed block $\begin{bmatrix} 138 & 41 \\ 26 & 5 \end{bmatrix}$ as an input to this Algorithm 3. If corresponding rows β and columns γ for each pixel of given block are $\left[\begin{array}{c|cc} & 37 & 38 \\ \hline 102 & 138 & 41 \\ 103 & 26 & 5 \end{array}\right]$. According to Algorithm 3 to calculate self embedding authentication bit, we do XOR between first four LSBs of pixels with their corresponding row and column values. For 138, A_{s_1} and A_{s_2} are calculated as 1111 and 1100 respectively. For 41, A_{s_1} and A_{s_2} are calculated as 1111 and 1111 respectively and so on. Finally determined authentication bit for all four pixels are given as $A_u = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$. In order to generate verifiable multi-toned meaningful share, these bits are updated on fifth LSBs of their corresponding pixel values of shares. Updated intensities meaningful share are $C_{vs_1} = \begin{bmatrix} 138 & 41 \\ 26 & 21 \end{bmatrix}$.

Algorithm 3 Algorithm for Embedding of Verifiable Multi-tone VC (VMVC)

INPUT: C_{share_1} and C_{share_2}.
OUTPUT: C_{vs_1}, C_{vs_2}
Ensure:

(1) β_{ij}, γ_{ij} are row and column of the $(ij)_{th}$ pixel respectively.
(2) $b^u(P)$ indicates the u^{th} bit of pixel P.
(3) P_{ij} is $(ij)^{th}$ pixel 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.

```
$\forall C_{share_k}$
for $i \leftarrow 1$ to $2n$ do
    for $j \leftarrow 1$ to $2m$ do
        $A_{s_1} \leftarrow ExOr(b^u(\beta_{ij}), b^u(P_{ij}))$          ▷ ExOr of 4 LSBs.
        $A_{s_2} \leftarrow ExOr(b^u(\gamma_{ij}), b^u(P_{ij}))$          ▷ $u = 0, 1, ..3$
        $A_u \leftarrow \{\sum_{u=0}^{3} (A^u_{s_1} \wedge A^u_{s_2})\} mod2$
        $b^5(P_{ij}) \leftarrow A_u$
    end for
end for
$C_{vs_k} \leftarrow C_{share_k}$
return $C_{vs_1}, C_{vs_2}$
```

2.4 Tamper detection

One can only get the actual authentic secret image at receiver end, when it is not tampered intentionally or unintentionally during transmission. Hence before decoding the secret image, we must check the both shares for alteration. Algorithm 4 is used to identify the tampered pixel for both shares. Here we just extract the fifth LSB of each pixel and recalculate it by Algorithm 3. 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.

2.5 Secret image recovery

Secret image recovery of proposed approach require little bit computation. In this phase, according to Algorithm 5, after verifying the authenticity of both shares C_{vs_1} and C_{vs_2}, secret image recovery is done. To recover a SIP, we need to extract four LSBs of every pixels of corresponding 2 × 2 blocks of C_{vs_1} and C_{vs_2}. Four pairs of pixels from corresponding block of C_{vs_1} and C_{vs_2} generate eight bits of SIP. Example 2.5 demonstrates this procedure more clearly.

Algorithm 4 Algorithm for Tamper Detection

```
INPUT: $C_{vs_1}, C_{vs_2}$
OUTPUT: Tamperd Region
$\forall P_{ij}\ of\ C_{vs_k}$
Calculate $A_u$ using Algorithm VMVC
$A_u^e \leftarrow b^5(P_{ij})$
if thenA_u $\neq A_u^e$
    Mark $P_{ij}$ as tampered pixel.
end if
return Tampered $P_{ij}$.
```

Example 2.5 This example shows the recovery process of the secret information. With continuation of aforementioned examples, let us consider two verifiable multi-toned meaningful share's blocks are $C_{vs_1} = \begin{bmatrix} 138 & 41 \\ 26 & 21 \end{bmatrix}$ and $C_{vs_2} = \begin{bmatrix} 26 & 118 \\ 25 & 58 \end{bmatrix}$. By comparing extracted and recalculated fifth LSB, one can localize the tampered region. If shares are untampered then according to Algorithm 5, one can decode exact secret information pixel. As per the Algorithm 5 extract four LSBs of each pixel of both blocks $\begin{bmatrix} 1010 & 1001 \\ 1010 & 0101 \end{bmatrix}$ and $\begin{bmatrix} 1010 & 0110 \\ 1001 & 1010 \end{bmatrix}$. Here elements of first and second blocks are represented as ζ_1 and ζ_2 respectively. Now μ is calculated by doing element wise OR operation between all set of ζ_1 and ζ_2 as $\begin{bmatrix} 1010 & 1111 \\ 1011 & 1111 \end{bmatrix}$. These four bit elements are further reduced to two bit elements by Algorithm 5 like $\begin{bmatrix} 00 & 11 \\ 01 & 11 \end{bmatrix}$. Vector representation of this matrix is [00110111], hence the resultant SIP is 55. Unaltered value of SIP is achieved which shows the 100 % contrast and imperceptibility between original and recovered secret image.

2.6 Performance analysis

Verifiable multi-toned meaningful shares C_{vs_1} and C_{vs_2} must satisfy the contrast and security conditions. Since we are dealing with gray-scale images, hence imperceptibility between C_k & C_{vs_k} and I_{sec} & I_{reco} must belong to acceptable range.

Lemma 1 ***Imperceptibility between C_k & C_{vs_k} must belong to an acceptable range in terms of PSNR.***
Since five LSBs of each pixels of C_k is altered during creation of cover image to verifiable multi-toned meaningful shares, hence a pixel can have minimum change of intensity as 0 and maximum change of intensity as 31 from its original value.

Lemma 2 ***If C_{vs_k} is unaltered then I_{sec} and I_{reco} will be identical.***
If C_{vs_k} is unaltered then I_{sec} and I_{reco} will be identical because SIPs are perfectly recovered by using little bit computations. For example if stacking of four LSBs two corresponding pixels is 1011, then it is further processed to its actual bits i.e. 01 by Algorithm 5.

Algorithm 5 Algorithm for Secret Recovery

```
INPUT: $B_\alpha^{V_{c1}}, B_\alpha^{V_{c2}}$
OUTPUT: Secret Information Pixel (SIP).
Ensure:
    (1) $\zeta_1, \zeta_2$ and $\mu$ are NULL vector of size $1 \times 4$
    (2) $B_s$ is NULL vector of size $1 \times 8$
    (3) $\mu_{i,j}$ represents $i$ and $j^{th}$ elements of vector $\mu$.
    (4) $X||b$ shows the concatenation of bit $b$ to vector $X$.
    (5) $\vee$ represents bitwise OR operator.

for $x \leftarrow 1$ to 2 do
    for $y \leftarrow 1$ to 2 do
        $\zeta_1 \leftarrow b^u(B_\alpha^{V_{c1}}(x, y))$
        $\zeta_2 \leftarrow b^u(B_\alpha^{V_{c2}}(x, y))$        ▷ Where $u = 0, 1..3$
        $\mu \leftarrow \zeta_1 \vee \zeta_2$
        if $\mu_{1,2} = 01$ or 10 then
            $B_s||0$
        else
            $B_s||1$
        end if
        if $\mu_{3,4} = 01$ or 10 then
            $B_s||0$
        else
            $B_s||1$
        end if
    end for
end for
$SIP \leftarrow \sum_{u=0}^{7} B_s(u) \times 2^u$
return $SIP$
```

Lemma 3 ***Secret image I_{reco} recovered by two shares C_{vs_1} and C_{vs_2} has contrast value $\alpha = 100\ \%$ with respect to I_{sec}.***
Threshold can be calculated as $t_X = min(w(V_1))$, since here we are taking all bits of a block so $\forall w(V_1) = \{4\}$ hence $t_X = 4$, similarly $max(w(V_0) = 2$. Since pixel expansion $m = 4$ hence $\alpha(m) = \frac{4-2}{4} \rightarrow \frac{1}{2}$. For contrast condition $w(V_0) \leq t_X - \alpha(m) \times m$ and $w(V_1) \geq t_X$ must be satisfied that is $2 \leq 4 - (\frac{1}{2} \times 4)$ or $2 \leq 2$ and $4 \geq 4$. This 50 % contrast is applicable when only stacking is considered for decoding. But we use little bit computations in Algorithm 5 which finally increase the contrast up to 100 %.

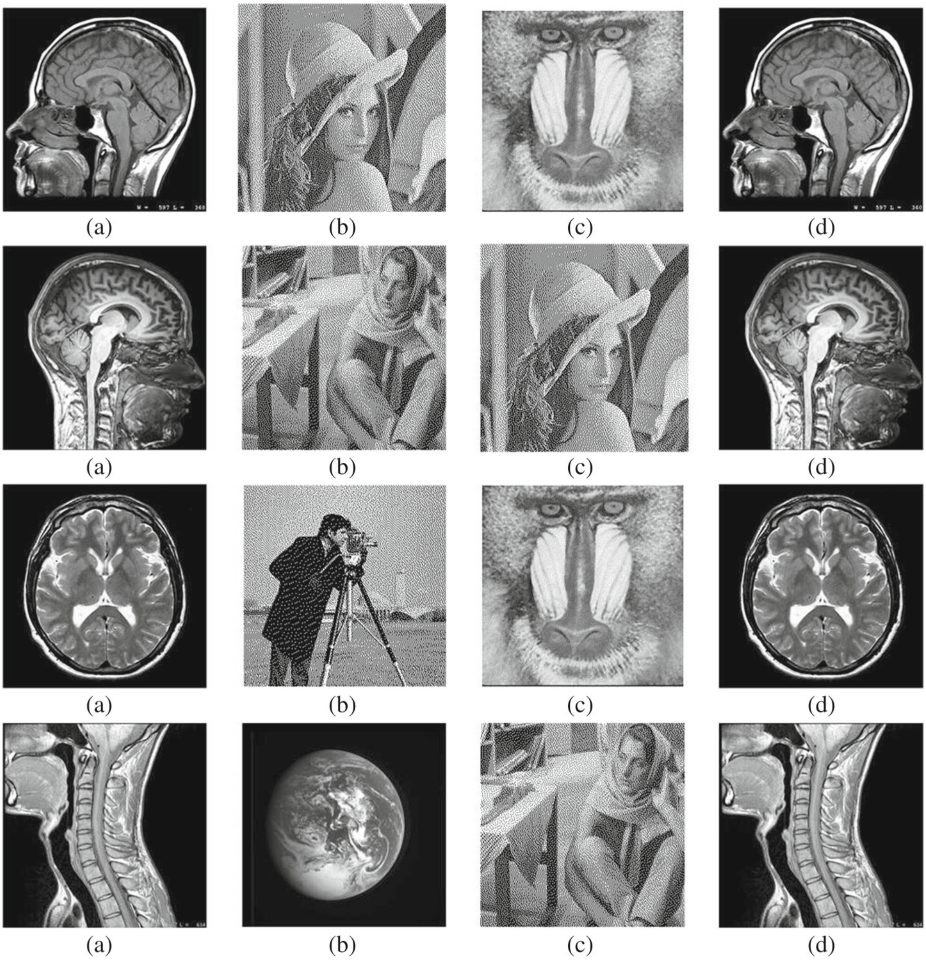

Fig. 4 (**a**) Original medical images I_{sec}, (**b**) Verifiable multi-toned share C_{vs_1}, (**c**) Verifiable multi-toned share C_{vs_2} (**d**) Recovered secret I_{reco}

Lemma 4 ***C_{vs_k} has no visible information about secret images.***
Γ_{Forb} contains all the isolated shares and for ensuring the security condition we have to show that any single row of S^{ij} is indistinguishable. There will be number of permutations of only one combination of 0 and 1 that is 1100 in each S_k^{ij}. One can not infer the belonging SIP.

Table 1 Imperceptibility measurement using PSNR between I_{sec} and I_{reco}

	Medical Image 1	Medical Image 2	Medical Image 3	Medical Image 4
PSNR	Infinite	Infinite	Infinite	Infinite

3 Experimental results and comparisons

Experiments have been performed on various images of different sizes. Here we have taken many medical images as secret and various standard images as cover. VMVC approach has been verified and illustrated for two shares. Figure 4 shows overall effectiveness and accuracy of our approach. Figure 4a represent all telemedicine images which are to be transmitted securely. set of images (b) and (c) are verifiable multi-toned meaningful shares C_{vs_1} and C_{vs_2} respectively. Set of images (d) are nothing but the recovered images. We can see here that recovery of secret telemedicine images are with 100 % accuracy. Imperceptibility between I_{sec} and I_{reco} can be verified by Table 1 .

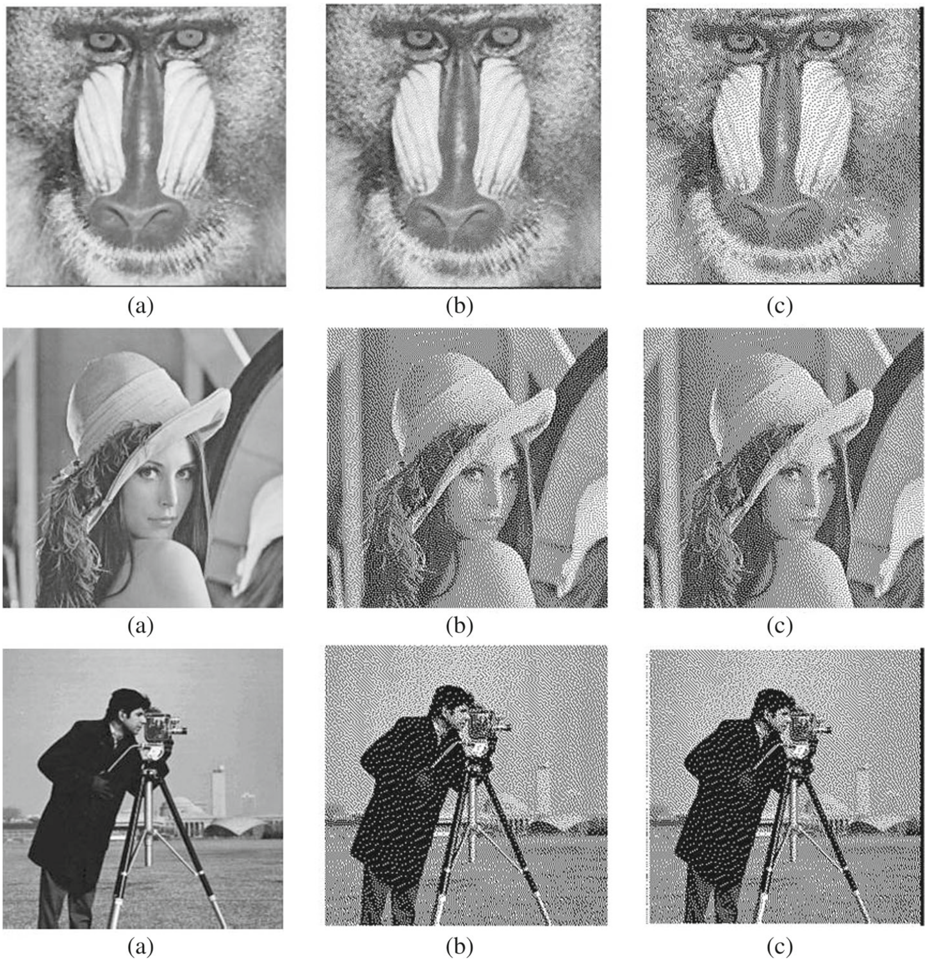

Fig. 5 (**a**) Original cover image C_k (**b**) Multi-toned meaningful share C_{share_k} (**c**) Verifiable multi-toned meaningful share C_{vs_k}

Table 2 Imperceptibility measurement using PSNR between C_k & C_{share_k} and C_k & C_{vs_k}

Cover Images	C_k & C_{share_k}	C_k & C_{vs_k}
Lena	39 dB	32 dB
Baboon	29.6 dB	27 dB
Cameraman	33.1 dB	29.7 dB
barbara	26.8 dB	26 dB
earth	31 dB	29.5 dB

In proposed approach, we are maintaining the imperceptibility of meaningful shares with their cover images also. One can see that Fig. 5, where set of images (a) show the original cover images and set of images (b) and (c) are after the embedding of secret image and verifiable bits respectively. Imperceptibility between C_k & C_{share_k} and C_k & C_{vs_k} are shown

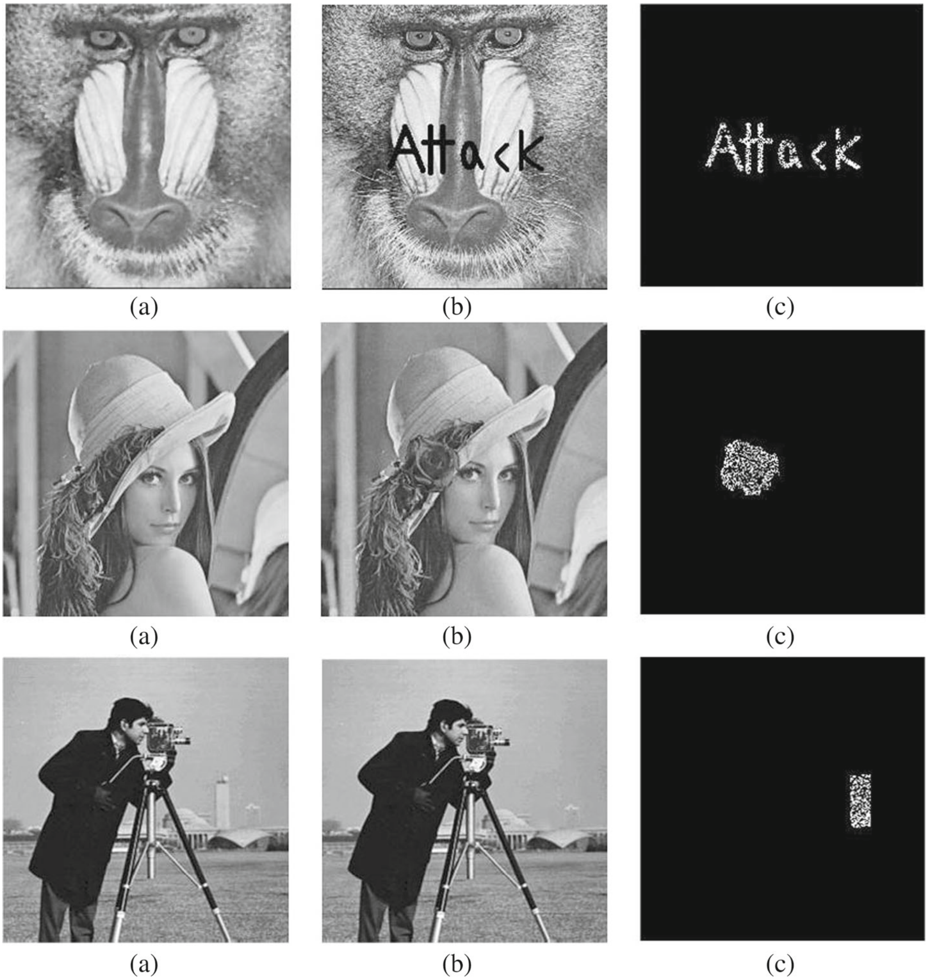

Fig. 6 (**a**) Verifiable multi-toned shares, (**b**) Tampered version, (**c**) Detected pixels

in Table 2. The average energy of distribution caused by embedding of secret and verifiable bits on each pixel can be calculated as

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(I(i,j) - K(i,j))^2 \tag{5}$$

Where MSE is mean square value which is for $m \times n$ two multi-tone images I and K in which one of the image is original cover image and another one is share image. Now the PSNR is defined as

$$PSNR = 10log_{10}\frac{(MAX)^2}{MSE} \tag{6}$$

Each share contains authentication bits to verify their integrity. If their will be any alteration intentionally or unintentionally during transmission, it will be detected by proposed approach. Figure 6 demonstrate the integrity verification of shares, where images (a) are meaningful shares and (b) are their tampered version. Using Algorithm 4, one can easily identify that shares are authentic or not. White pixels in Fig. 4 c show the tampered portion of images. Table 3 shows the accuracy of tamper detection.

3.1 Comparison of relative reports on VC

Various essential characteristics of VC have been taken in our consideration for comparing the proposed approach with existing one as shown in Table 4. Few of qualitative parameters for comparison of VC are described as follows:

1. **Pixel Expansion m for secret image:** Pixel expansion m is number of subpixels by which one secret information pixel (SIP) p is encoded. So m must be as small as possible so that dimension of shares remain same as I_{sec}.
2. **Decoding Process:** Decoding of secret image may be either by only human visual system or by using little bit computation.
3. **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.
4. **Contrast $\alpha(m)$ of the Decoded Image:** The value of contrast $\alpha(m)$ must be as high as possible so that the quality of secret image remains same as decoded one. Since for security issues there are some contrast loss in all VC schemes, hence this contrast loss must be minimized.

Table 3 Alteration detection accuracy of proposed approach

Shares	No. of altered pixels	No. of detected pixels	Accuracy
Lena	1739	1302	74.8 %
Baboon	1930	1549	80.25 %
Cameraman	1287	936	72.7 %
barbara	1173	891	75.9 %
earth	2533	1852	73.11 %

Table 4 The comparison of relative reports on VC

Method	Pixel Expansion	Decoding	Meaningful Share	$\alpha(m)$	Share Authentication	Codebook Generation	Limit of Shares	Type of Secret Image
Naor and Shamir [17]	Yes(2 times)	Stack	No	1/2	No	Explicit	n	Halftone
Fang and Lin [6]	Yes (4 times)	Stack	No	1/2	No	Explicit	n	Halftone
Ateniese et al. [1]	Yes	Stack	No	1/2	No	Explicit	n	Halftone
Giuseppe et al. [2]	Yes(4 times)	Stack	Yes	1/4	No	Explicit	n	Halftone
Jin et al. [13]	Yes(4 times)	Stack & Compute	No	1/4	No	Explicit	n	Halftone
Zhi Zhou et al. [26]	Yes(16 times)	Stack	Yes	1/16	No	Explicit	2	Halftone
Wen Pim et al. [7]	Yes(4 times)	Stack	Yes	1/4	No	Implicit	n	Halftone
Z Wang et al. [22]	Yes(12 times)	Stack	Yes	1/12	No	Explicit	n	
Y Chang et al. [10]	No	Stack	No	(k-1)/2	No	Explicit	n	Halftone
Y-C Hou et al. [12]	No	Stack	Yes	1/4	No	Explicit	2	Halftone
Y-C Hou et al. -1 [11]	No	Stack	No	1/2	No	Implicit	n	Halftone
Y-C Hou et al. -2 [11]	No	Stack	Yes	1/4	No	Implicit	n	Halftone
T-H Chen et al. [4]	No	Stack	No	7/17	No	Implicit	n	Halftone
S J Shyu et al. [19]	No	Stack	No	1/4	No	Implicit	2	Halftone
Horng et al. [9]	Yes	Stack	No	$1/n$	Yes(Additional Share)	Implicit	n	Halftone
Wang et al. [23]	No	Compute	No	1	Yes(Additional Share)	Implicit	2	Halftone
Hao-Kuan Tso [20]	No	Compute	Yes	1	Yes(Additional Share)	Implicit	8	Halftone
Yasushi Yamaguchi [25]	No	Compute	No	1	No	Implicit	n	Multitone
Chang-Chou Lin et al. [14]	Yes	Stack	No	$k/9$	No	Implicit	2	Multitone
D. Taghaddos et al. [21]	Yes	Stack	No	$1/2$	No	Explicit	2	Multitone
Proposed Approach	No(for secret)	Compute	Yes	1	Yes(Self Embedding)	Implicit	2	Multitone

5. **Security Criteria:** Any subset of Γ_{Forb} must show no information about the secret image and for Γ_{Forb}, rows from any matrix of $C_{j(j\in\{0,1\})}$ must be indistinguishable with respect to p.
6. **Codebook Requirement:** Most of the existing algorithms on VC require codebook, explicitly, at the time of encoding and decoding process. Codebooks are nothing but a pattern of all combinations of C_0 and C_1, which are decided for various possibilities of pixels. 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 VC algorithm .
7. **Limit of Shares:** To generalize the VC algorithm there should not be any fixed limit of shares. Because practically, we can not restrict the number of participants for any particular application.
8. **Security of Shares:** Shares are very sensible objects in visual cryptography hence there should be some method to make share protected. By this way one can easily verify the authenticity and integrity of shares at the time of any conflict. Self embedding is the best way to achieve this objective because it does not require any extra authentication images.

4 Conclusions

In this paper a novel approach for verifiable multi-toned visual cryptography(VMVC) with meaningful shares has been proposed for securely transmission of various confidential images. Proposed method eliminates various basic security constraints of VC like pixel expansion of secret image, random pattern of shares, explicit codebook requirement and contrast loss. Proposed approach is basically 2 out of 2 secret sharing scheme where both shares are also multi-toned and meaningful in nature which may provide confidentiality to secret images during transmission . All pixels of both shares are contained with self embedding authentication bits, which ensures authentication and integrity of shares and hence secret image. The experiments and comparison with state of art approaches in all aspects of visual cryptography show the effectiveness of proposed VMVC approach. From the experimental results, we found that irrespective of contents in the shares, the probability of occurrence of original pixels of secret image in the decoded image is 1.0.

References

1. Ateniese G, Blundo C, De Santis A, Stinson DR (1996) Visual cryptography for general access structures. Inf Comput 129(2):86–106
2. Ateniese G, Blundo C, De Santis A, Stinson DR (2001) Extended capabilities for visual cryptography. Theor Comput Sci 250:143–161
3. Blundo C, Santis AD, Naor M (2000) Visual cryptography for grey level images. Journal of Information Processing Letters 75(6):255–259
4. Chen TH, Tsao KH (2009) Visual secret sharing by random grids revisited. Pattern Recognit 42(9):2203–2217
5. Fu MS, Au OC (2004) Joint visual cryptography and watermarking. In: Proceedings IEEE Int. Conf. Multimedia and Expo, Taipei, Taiwan
6. Fang WP, Lin JC (2006) Progressive viewing and sharing of sensitive images. Patt Recog Image Anal 16(4):638–642
7. Fang WP (2008) Friendly progressive visual secret sharing. Pattern Recogn 41(4):1410–1414
8. Feng JB, Wu HC, Tsai CS, Chu YP (2005) A new multi-secret images sharing scheme using Largrange's interpolation. J Syst Softw 76(3):327–339

9. Horng G, Chen TH, Tsai DS (2007) A cheating prevention scheme for binary visual cryptography with Homogeneous secret image. Pattern Recogn 40(8):2356–2366
10. Hou Y-C, Quan Z-Y (2011) Progressive Visual Cryptography with Unexpanded Shares. IEEE Trans Circuits Syst Video Technol 21:11
11. Hou Y-C, Quan Z-Y, Tsai C-F, Tseng A-Y (2013) Block-based progressive visual secret sharing Elsevier. Inf Sci 233:290–304
12. Hou Y-C, Wei S-C, Lin C-Y (2014) Random-Grid-Based Visual Cryptography Schemes. IEEE Trans Circuits Syst Video Technol 24:5
13. Jin D, Yan WQ, Kankanhalli MS (2005) Progressive color visual cryptography. J Electron Imag 14(3):1–13
14. Lin C-C, Tsai W-H (2003) Visual cryptography for gray-level images by dithering techniques. Pattern Recogn Lett 24:349–358
15. MacPherson LA (2002) Grey level visual cryptography for general access structures. M.S. thesis University of Waterloo, Ontario, Canada
16. Naor M, Pinkas B (1997) Visual authentication and identification. Crypto97, LNCS 1294:322–340
17. Naor M, Shamir A (1995) Visual cryptography. Adv Cryog EUROCRYPT'94, LNCS 950:1–12
18. Nakajima M, Yamaguchi Y (2002) Extended visual cryptography for natural images. In: J. WSCG, vol 10, pp 303–310
19. Shyu SJ (2007) Image encryption by random grids. Patt Recog 40(3):1014–1031
20. Tso H-K (2013) Secret Sharing Using Meaningful Images, Journal of Advanced Management Science, Vol. 1, No. 1
21. Taghaddos D, Latif A (2014) Visual Cryptography for Gray-scale Images Using Bit-level, Journal of Information Hiding and Multimedia Signal Processing. Ubiquitous International, Vol. 5, No. 1
22. Wang Z, Arce GR, Crescenzo GD (2009) Halftone visual cryptography via error diffusion. IEEE Trans Inf Forensics Secur 4(3):383–396
23. Wang Z-h (2011) Sharing a Secret Image in Binary Images with Verification, Journal of Information Hiding and Multimedia Signal Processing Ubiquitous International
24. Wang D-S, Song T, Dong L, Yang C-N (2013) Optimal Contrast Grayscale Visual Cryptography Schemes With Reversing, IEEE Transactions on Information Forensics and Security, Vol. 8, No. 12
25. Yamaguchi Y (2015) Extended visual cryptography for continuous-tone images: effect of the optimum tone mapping. Int. J. Information and Communication Technology, Vol. 7, No. 1
26. Zhou Z, Arce GR, Di Crescenzo G (2006) Halftone visual cryptography. IEEE Trans Image Process 15(8):2441–2453

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.