A (n, n) Threshold Non-expansible XOR based Visual Cryptography with Unique Meaningful Shares

Priyanka Singh, Balasubramanian Raman, Manoj Misra

PII: S0165-1684(17)30225-6
DOI: 10.1016/j.sigpro.2017.06.015
Reference: SIGPRO 6514

To appear in: *Signal Processing*

Received date: 4 November 2016
Revised date: 15 March 2017
Accepted date: 13 June 2017

Please cite this article as: Priyanka Singh, Balasubramanian Raman, Manoj Misra, A (n, n) Threshold Non-expansible XOR based Visual Cryptography with Unique Meaningful Shares, *Signal Processing* (2017), doi: 10.1016/j.sigpro.2017.06.015

Highlights

- A (n, n) Threshold Non-expansible XOR based Visual Cryptography with Unique Meaningful Shares has been proposed in this article for securing media information prior to outsourcing to cloud data centers.
- The secret media information is obscured into multiple meaningful shares without any pixel expansion, share alignment problem, contrast loss, explicit codebook requirement, and limitation on number of participants.
- The recovery of the secret media information is lossless at the receiver end that makes it suitable for applications that comprise of sensitive information.
- Outsourcing media information into meaningful shares reduces the vulnerability of the scheme to cryptanalysis as compared to random shares. In case of attacks at the cloud data centers, the altered regions can be detected by the scheme.

A (n, n) Threshold Non-expansible XOR based Visual Cryptography with Unique Meaningful Shares

Priyanka Singh, Balasubramanian Raman, and Manoj Misra

Department of Computer Science and Engineering, Indian Institute of Technology Roorkee,Roorkee, Uttarakhand, INDIA

Abstract

Cloud-based multimedia systems are attracting end users with high end infrastructure resources and enormous storage facilities. However, there persists a high chance of leakage of sensitive information if outsourced to the remote cloud servers without encryption. In this article, a secure way of obscuring the information based on XOR based Visual Cryptography (VC) has been proposed. It obscures the secret information into multiple meaningful shares prior to outsourcing which reduces the vulnerability of random looking shares to cryptanalysis. The scheme also overcomes the problems existing in the traditional VC schemes like pixel expansion, share alignment problem, contrast loss, explicit codebook requirement, limitation on number of participants and lossy recovery of the secret. Proposed scheme ensures perfect recovery of the secret with high boost in contrast at the authentic entity end. Three novel algorithms have been proposed for generation of basis matrices, generation of random shares and conversion of random shares to meaningful shares to achieve this objective. The visual quality of the meaningful shares and the recovered secret image is quite good as evaluated by various objective error metrics. Comparative results based on various aspects of visual cryptography prove the efficacy of the proposed approach over existing state-of-the-art approaches.

Keywords: Cloud, XOR based Visual Cryptography, Unexpanded, Meaningful Shares, Pixel Expansion, Objective Error Metrics.

1. Introduction

Cloud-based media hosting has become very popular nowadays owing to the explosive growth in multimedia content. End users are facilitated with multiple service benefits like high end computational resources, storage capacity, infrastructure facilities, accessibility, etc. from anywhere around the globe. Various applications like media live streaming [6], media coding [47], media contrast enhancement [36], media transcoding [12] etc are deployed at the cloud servers to exploit these benefits [49]. However, the wide attacking surface of the public cloud and the vulnerability of the content to security breaches is urging the society to adopt to protocols that can ensure the security of the stored content [3, 35]. One possible solution may be encrypting the content prior to outsourcing at the cloud servers. But an encrypted content attracts attention that some secret content is residing and hence increases the chances of its breaches. Thus, devising a prototypical model that can safely transmit the content to the receiver end utilizing the service benefits of the cloud-based architecture can prove to be very beneficial. In this article, one such approach based on XOR based visual cryptography for outsourcing confidential information to the cloud servers has been proposed. It distributes the confidential information into multiple meaningful shares that look like ordinary information and hence can be sent securely over the cloud servers without attracting any unwanted attention. To devise such a scheme, one needs to address multiple challenges like minimization of storage requirements, computational overheads while decryption, quality of obtained shares and recovered information, etc.

Traditional visual cryptography was based on the notion of human visual system and perfect cipher. Thus, it ensured security without heavy computations. The basic idea was to distribute the information of the secret into multiple random looking shares which revealed no information individually but on superposition of shares, they revealed the information. In a k out of n visual secret sharing(VSS) scheme, a minimum number of k shares were required to reveal the secret. The shares were information theoretically secure. This implies no matter how much power an adversary has, he could not infer anything from the combination of less than k shares. To illustrate the working of the basic two out of two VSS scheme, the codebook is depicted in Fig.1. Each pixel of the secret is encoded into two sub pixels of the two shares. Depending upon the value of the secret pixel as either '1' or '0', the combinations are chosen from the codebook. In case of black pixel, super-

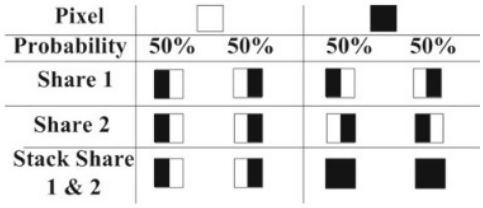

Figure 1: 2 out of 2 VSS Scheme with each pixel of secret encoded into two subpixels of the shares

position of the share pixels gives two black pixels, whereas in case of white pixel of the secret, one back and one white pixel is obtained. The codebook must be designed in such a way that just by observing an individual share, one cannot guess whether the secret pixel is black or white. Built on the concept of boolean OR function, the system was proved to be unconditionally secure and equivalent to one time pad encryption scheme [26, 25]. However, problems of pixel expansion, contrast loss in recovered secret, pixel alignment problem, mishandling of random shares, etc needed attention. Later, various issues of Naor and Shamir OR based scheme were studied extensively like the concept of meaningless share [37, 22], perfect reconstruction of the black pixels [4, 18], contrast of revealed secret image [14, 5], cheating prevention issues [16, 8, 19, 7]etc. But certain disadvantages still persisted like the load of carrying the transparencies for physical stacking, restriction on the usage of secret key to only once due to one time pad property, lower quality physical properties like color, resolution, contrast etc.

XOR based VC scheme evolved as one of the possible solutions to address the aforementioned issues. The foremost advantage of XOR based VC scheme was eradication of pixel alignment problem existing in traditional VC scheme. Decryption of the secret from the shares could be done by small and light weighted cheap computational devices in a XOR based VC scheme. Improvement in the contrast of the recovered secret image could be achieved that was limited to at most 1/2 in OR-based VC schemes. Many XOR based VC schemes have been proposed in the literature [42, 45, 40, 32, 21, 39]. A XOR based scheme with some valid constructions was proposed in [32]. However, the scheme demanded the codebook explicitly and the shares obtained were meaningless. Liu et al. gained an improvement in the contrast of the recovered image but the demand of explicit codebook, pixel expansion in the shares and random pattern on the shares still existed [21]. The random share

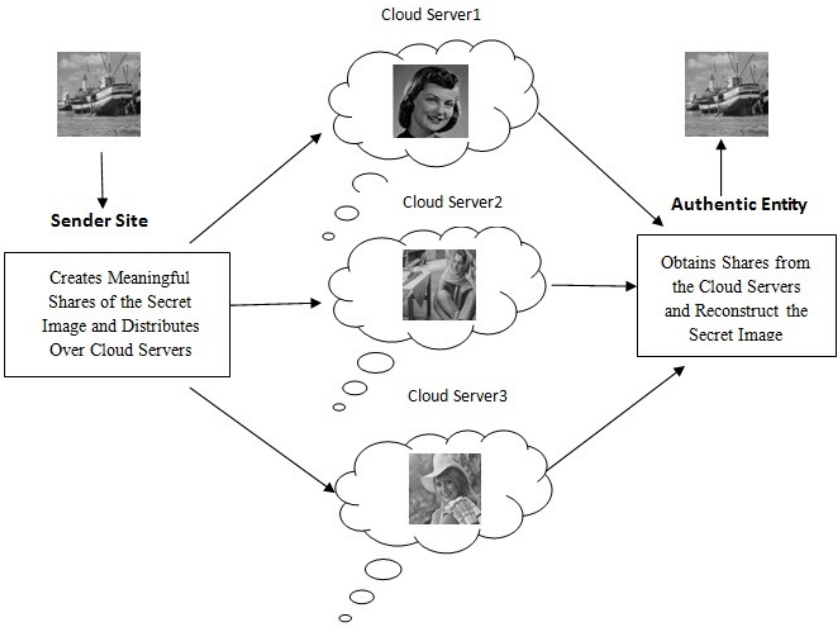

Figure 2: Architecture of proposed model

problem was resolved by introduction of meaningful shares based on n out of n XOR based scheme [40]. But the problems of poor visual quality in the obtained meaningful shares and recovered secret image could not be solved.

In this article, an effort has been made to propose a XOR based VC scheme that addresses the aforementioned challenges existing in the state-of-the-art approaches and provide a secure way of outsourcing the confidential information over remotely distributed cloud servers. The basic architecture of the proposed scheme is depicted in Fig. 2. Three novel algorithms have been designed for generation of basis matrices, generation of random shares and conversion of random shares to meaningful shares to attain these objectives. The main contributions of the proposed scheme can be summarized as follows:

- No pixel expansion: The proposed scheme encrypts the secret information into multiple shares of same size as the secret. It eradicates the pixel expansion problem, hence minimizing storage requirements and decreasing transmission time.

- No limit on number of shares: The proposed scheme is not restricted

to a specific number of participants or shares. Hence, it can be made applicable to a broad spectrum of real world problems.

- No explicit requirement of codebook: The scheme generates codebook implicitly at run time depending on the number of participants. Hence, there is no need to store the codebook, thus minimizing storage requirements.

- Unique meaningful shares: The proposed scheme obtains shares bearing unique meaningful cover information. It reduces the vulnerability of the shares to cryptanalysis and even assists handling of shares in case of tampering at the cloud servers as each share bears a unique cover information. So it is easy to identify which shares are corrupted and in case of deterioration exceeding acceptable limits, the particular share can be requested again.

- Perfect reconstruction of the secret: The scheme guarantees perfect reconstruction of the black/white pixels associated with the black/white pixels of the secret image in case the shares are not tampered. Hence, the contrast of the reconstructed secret is obtained to be 100% which enhances identification by the human visual system.

- Good visual quality of the shares and the recovered secret: The visual quality of the obtained meaningful shares and the recovered secret is quite good as verified by the various objective evaluation parameters.

The rest of the paper is organized as follows: section 2 gives a brief overview of the concepts used in the proposed scheme, section 3 discusses the proposed (n, n) XOR based VC scheme with meaningful shares. Experimental results along with analysis are presented in section 4, comparison with other state-of-the-art approaches in section 5 and finally, conclusions along with scope of future work are given in section 6.

2. Preliminaries

A brief overview of the concepts used in the proposed methodology is discussed as follows:

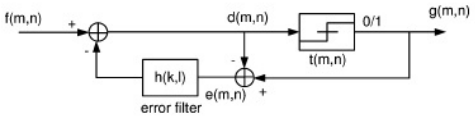

Figure 3: Block diagram for binary error diffusion

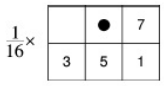

Figure 4: Floyd-Steinberg error filter. • indicates the current pixel.

2.1. Error Diffusion for Generation of Halftone Images

To obtain halftone version of a multitone image, error diffusion is often used as one of the efficient approaches. It is based on quantizing error at pixel level and fetching back to a set of future input samples as depicted in Fig. 3. Here, $f(m,n)$ and $g(m,n)$ represents the (m,n)th pixel of the input multitone and output halftone image respectively, $d(m,n)$ signifies the sum of diffused past errors and input pixel value $f(m,n)$ [24, 34].

It consists of two main components. First is the thresholding block where the output $g(m,n)$ is decided by

$$g(m,n) = \begin{cases} 1, & \text{if } d(m,n) \geq t(m,n) \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

The second component comprises of the error filter $h(k,l)$ whose input $e(m,n)$ is the difference between $d(m,n)$ and $g(m,n)$. Finally, we can compute $d(m,n)$ as

$$d(m,n) = f(m,n) - \sum_{k,l} h(k,l)e(m-k,n-l) \tag{2}$$

Floyd-Steinberg error filter is widely used as shown in Fig. 4, where • indicates the current processing pixel. The weights of the filter are given by $h(0,1) = 7/16$, $h(1,-1) = 3/16$, $h(1,0) = 5/16$ and $h(1,1) = 1/16$.

Here , the threshold $t(m,n)$ may be position-dependent.

The quantization error $e(m,n)$ not only depends on the current input and output but also on the entire past history as can be inferred from the

recursive structure depicted in Fig. 3. The low frequency difference between the input and output image must be minimized while designing an error filter to obtain an halftone version of an image from its multitone image.

2.2. Basic Definitions of VC Scheme

Definition 1 (Average light transmission ([29, 41]). Let the transmission of light through a pixel p of a binary image B of size $M \times N$ be denoted as $T(p)$. The probability of a pixel being white is represented as $Prob(p = 1)$. Thus, light transmission of a white pixel p is $T(p = 1)$ and that of a black pixel is $T(p = 0)$. The average light transmission of I is defined as follows:

$$T(I) = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} T(I_{i,j})}{M \times N} \tag{3}$$

Definition 2 (Area representation ([29, 41]). Let the area of all the white and black pixels in image L be denoted as $I(1)$ and $I(0)$ where $I = I(1) \bigcup I(0)$ and $I(1) \bigcap I(0) = \phi$. Hence, the total area of all the corresponding white and black pixels will be $L[I(1)]$ and $L[I(0)]$ in image L.

Definition 3(Contrast of the revealed secret image ([29, 41]). The contrast of the revealed secret image by stacking of shares $R_{\oplus,1\ldots n} = R_1 \oplus R_2 \ldots \oplus R_n$ with respect to the original secret image S is:

$$\alpha_x = \frac{T(R_{\bigoplus,1\ldots.n}[S(1)]) - T(R_{\oplus,1\ldots n}[S(0)])}{1 + T(R_{\bigoplus,1\ldots.n}[S(0)]} \tag{4}$$

The contrast of the revealed secret image obtained via XOR operation among the shares must be $\alpha_x > 0$ for the human visual system to identify clearly. Value of contrast must be as large as possible. The revealed pixels associated to the black secret pixels are definitely black when $T(R_{\bigoplus,1\ldots.n}[S(0)] = 0)$.

Definition 4 (Contrast of the share). The contrast of the share R with respect to the original cover image C is

$$\alpha_{sh} = \frac{T(R[C(1)]) - T(R[C(0)])}{1 + T(R[C(0)])} \tag{5}$$

The share R is said to have resemblance with the cover image C when the contrast of the share $\alpha_{sh} > 0$, otherwise when $\alpha_{sh} = 0$, the generated shares

become meaningless and hard to be identify.

Definition 5 (Security condition). A (n, n) XOR-based VC scheme is said to be secure if the XOR-result of any $(1 \leq k<n)$ shares out of n shares $R_1, \ldots R_n$ does not depend on the secret image

$$S : T(R_{\bigoplus, X_1 \ldots X_k}[S(1)]) = T(R_{\bigoplus, X_1 \ldots X_k}[S(0)]) \tag{6}$$

where $\{x_1 \ldots x_k\} \subsetneq \{1 \ldots n\}$

Definition 6 (Access structure). The proposed scheme is based on general access structure described as a set of qualified subsets Γ_{Qual} and forbidden subsets Γ_{Forb} on n participants $P = 1, 2, 3, \ldots, n$. The participants of any qualified subset can jointly decode the secret image, whereas those from a forbidden subset cannot. The pair $\Gamma_{Qual}, \Gamma_{Forb}$ is called the access structure of the scheme. Denote 2^P as the set of all subsets of P. We obtain $\Gamma_{Qual} \subseteq 2^P, \Gamma_{Forb} \subseteq 2^P$, and $\Gamma_{Forb} \bigcap \Gamma_{Qual} = \Phi$ since there is no participant subset that can be both qualified and forbidden simultaneously.

Example 2.1: The strong access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ of the $(3, 3)$ VC scheme can be written as $\Gamma_{Qual} = \{1, 2, 3\}$ and $\Gamma_{Forb} = \{\{\phi\}, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}$

3. Proposed Methodology

The proposed scheme provides a secure way of obscuring the confidential information into multiple meaningful shares prior to outsourcing at the cloud data centers. It eradicates the limitations existing in most of the state-of-the-art approaches, specifically problem of pixel expansion in obtained shares and recovered secret image, poor contrast, vulnerability of random shares to cryptanalysis and difficulty in management in case of a large number of participants. The proposed scheme is versatile and flexible enough to be applicable to many real world problems as it does not require predefining of parameters like specification of number of participants, codebook generation, etc which usually limit the application areas. Requirement of extra memory for storing and transmission of explicit codebook, expanded shares also poses as one of the major hindrances in designing a solution to the problem. The proposed methodology overcomes all such limitations and

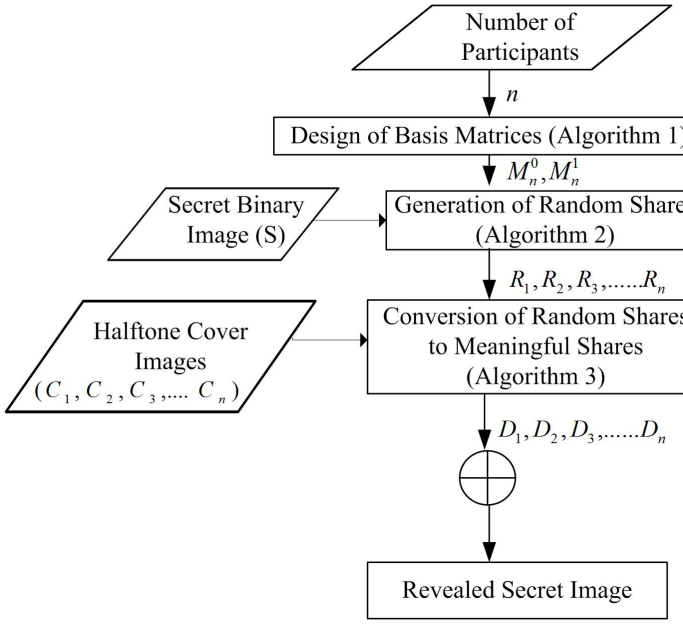

Figure 5: Basic flow of the proposed scheme

provides a precise solution designed in three novel algorithms towards the attainment of aforementioned objectives. The most important characteristic of the proposed scheme is the perfect reconstruction of the secret image and high contrast of the recovered secret image that is attained to 100 % in the above scheme. The visual quality of the generated meaningful shares is also maintained high. Thus, the scheme provides an appropriate feasible solution for outsourcing a confidential information over cloud-based paradigm with less computational overheads and efficient decryption of the recovered secret image. The basic flow of the proposed scheme is shown in Fig. 5.

The proposed scheme consists of three main phases: generation of basis access structure(as Algorithm 1), generation of random shares(as Algorithm 2) and lastly, conversion of random shares to multiple meaningful shares(as Algorithm 3). The block diagram for the proposed scheme has been presented in Fig.4.

3.1. Generation of Basis Access Structure

The proposed scheme is flexible enough to be applicable to any number of participants. So, depending on the requirement of the problem at hand,

the number of participants can be decided and accordingly, the basis access structure of the proposed VC scheme can be obtained. To represent the respective pixel values of the secret image '0' and '1', two basis matrices M_n^0 and M_n^1 are obtained. Depending on the number of participants(n), the size of the basis matrices M_n^0 and M_n^1 are decided as $t_j \times n$ where $j\epsilon(0,1)$ and $t_0 = \lfloor \frac{n}{2} \rfloor, t_1 = \lceil \frac{n}{2} \rceil$. M_n^0 and M_n^1 will be composed of row vectors whose hamming weight is even and odd respectively. The detailed methodology is given in *Algorithm* 1 and explained with example 2.1.

Algorithm 1 Generation of Basis Matrices

INPUT: n as number of participants or shares
OUTPUT: M_n^0 and M_n^1 as Basis Matrices of size $t_j \times n$
DEFINE: 1. M_n^0 and M_n^1 as Basis Matrices of size $t_j \times n$ where $j\epsilon(0,1)$ and $t_0 = \lfloor \frac{n}{2} \rfloor, t_1 = \lceil \frac{n}{2} \rceil$ initialized to zeros.
2. s_0 and s_1 are variables initialized with value as 1
3. u and v are null row vectors

for $i \leftarrow 1$ to n **do**
  $p \leftarrow i \bmod 2$
  if $p = 0$ **then**
    $u(s_0) \leftarrow i$
    $s_0 \leftarrow s_0 + 1$
  else
    $v(s_1) \leftarrow i$
    $s_1 \leftarrow s_1 + 1$
  end if
end for
for $i \leftarrow 1$ to $s_0 - 1$ **do**
  $M_n^0(i, 1:n) \leftarrow$ Assign u_i number of $1'$s in random positions varying from 1 to n
end for
for $i \leftarrow 1$ to $s_1 - 1$ **do**
  $M_n^1(i, 1:n) \leftarrow$ Assign v_i number of $1'$s in random positions varying from 1 to n
end for
return M_n^0, M_n^1

Example 2.1: Let us consider an example to demonstrate the generation of the basis matrices M_n^0 and M_n^1 where number of participants $n = 6$. As per the Algorithm 1, $t_1 = \lceil \frac{n}{2} \rceil = \lceil \frac{6}{2} \rceil = 3$,$t_0 = \lfloor \frac{n}{2} \rfloor = \lfloor \frac{6}{2} \rfloor = 3$, $v = [1, 3, 5], u = [2, 4, 6]$, $M_n^0 = \begin{bmatrix} 011000 \\ 111100 \\ 111111 \end{bmatrix}$,$M_n^1 = \begin{bmatrix} 100000 \\ 101010 \\ 101111 \end{bmatrix}$

3.2. Generation of Random Shares

The secret image S of size $H \times W$ is encrypted into multiple random shares of same size depending on the number of participants. The information of each pixel of the secret image S is distributed to the corresponding pixel positions of the multiple encrypted random shares. Depending on the pixel value of the secret image, a random row is selected from the basis matrix and its various column permutations. If secret pixel value is zero, a random row from basis matrix M_n^0 is chosen, else basis matrix M_n^1 is selected for filling the corresponding pixel positions in the random shares. The detailed procedure is given in *Algorithm* 2.

3.3. Conversion of Random Shares to Meaningful Shares

To reduce the vulnerability of the random shares to cryptanalysis and better management of the shares over the cloud servers, these random shares are converted to the meaningful shares. Depending on the number of participants or cloud servers involved, different cover images are taken up and their corresponding halftone versions are obtained via error diffusion method. Information of the cover images is embedded on block basis in two random positions of the corresponding blocks of random shares. Thereafter, XORing of these embedded shares is done to check whether the information of the original secret is intact or not. In case, information of any pixel position in the secret image is found to be altered, necessary changes are made in the corresponding pixel values of the random shares to obtain the original value of the secret image at the authentic entity end. The distribution of cover information is done randomly into the blocks of the random shares to make it meaningful. The intactness of the information of the secret image obtained after final decryption is also ensured by alteration of corresponding pixel value of randomly chosen share. This randomization introduced twice in the proposed scheme enhances the security of the scheme. The detailed

Algorithm 2 Generation of Random Shares

INPUT: Secret Image S of size $H \times W$, Basis Matrices M_n^0 and M_n^1
OUTPUT: Random Shares $R_1, R_2 \dots R_n$, each of size $H \times W$
DEFINE: 1. $R_k(i,j)$ represents the $(i,j)^{th}$ pixel of k^{th} share, where k varies from 1 to n.

for $i \leftarrow 1$ to H **do**
  for $j \leftarrow 1$ to W **do**
    if $S(i,j) = 0$ **then**
      $d \leftarrow$ Select random row from M_n^0 or its various column permutations
      for $k \leftarrow 1$ to n **do**
        $R_k(i,j) \leftarrow M_n^0(d,k)$
      end for
    else
      $d \leftarrow$ Select random row from M_n^1 or its various column permutations
      for $k \leftarrow 1$ to n **do**
        $R_k(i,j) \leftarrow M_n^1(d,k)$
      end for
    end if
  end for
end for
return $R_1, R_2 \dots R_n$

procedure is described in *Algorithm* 3 and explained in Example 2.3.

Example 2.3: Let us consider an example to demonstrate the working of proposed approach as shown in Fig. 6 where $n = 3$. As per the Algorithm 1, $t_1 = \lceil \frac{n}{2} \rceil = \lceil \frac{3}{2} \rceil = 2$,$t_0 = \lfloor \frac{n}{2} \rfloor = \lfloor \frac{3}{2} \rfloor = 1$, $v = [1,3], u = [2]$, $M_n^0 = \begin{bmatrix}011\end{bmatrix}$,$M_n^1 = \begin{bmatrix}100\\111\end{bmatrix}$, M_n^0 and M_n^1 are basis matrices and used as input to generate random shares via Algorithm 2 shown in Fig. 6(b) to 6(d). These random shares are then embedded with secret information of halftone cover images C_1, C_2, C_3 to generate meaningful shares as D_1, D_2, D_3 respectively via *Algorithm* 3.

Algorithm 3 Conversion of Random Shares to Meaningful Shares

INPUT: Secret Image S of size $H \times W$, Random Shares $R_1, R_2 \dots R_n$, each of size $H \times W$, Halftone cover Images $C_1, C_2 \dots C_n$, each of size $H \times W$

OUTPUT: Meaningful Shares $D_1, D_2 \dots D_n$, each of size $H \times W$

DEFINE:
1. $B^S_{j_k}$, $B^{R_i}_{j_k}$ and $B^{C_i}_{j_k}$ represents the k^{th} pixel of j^{th} block of secret image S, i^{th} random share and i^{th} halftone cover images respectively.
2. Block B is of size 2×2
3. b is a row vector of length equal to twice the number of blocks
4. $a = 1$

for $j \leftarrow 1$ to $\frac{H \times W}{4}$ **do**
  $k_w \leftarrow$ A random number between 1 to 4, where $w \in \{1, 2\}$ and $k_1 \neq k_2$
  for $i \leftarrow 1$ to n **do**
    $B^{R_i}_{j_{k_w}} \leftarrow B^{C_i}_{j_{k_w}} \quad \forall w$
    $b(a) \leftarrow k_w$, $a = a + 2$
  end for
end for
$Z \leftarrow XOR(R_1, R_2 \dots R_n)$
for $j \leftarrow 1$ to $\frac{H \times W}{4}$ **do**
  for $i \leftarrow 1$ to n **do**
    if $B^S_{j_{b(j)}} \neq Z_{j_{b(j)}}$ **then**
      if $B^S_{j_{b(j)}} = 1$ **then**
        $p \leftarrow$ A random number between 1 to n where $B^{R_p}_{j_{b(j)}} \neq 0$
        $B^{R_p}_{j_{b(j)}} = 0$
      end if
    end if
  end for
end for
return $D_1, D_2 \dots D_n$ ▷ $D_1, D_2 \dots D_n$ are composed of final shares $R_1, R_2 \dots R_n$

3.4. Recovery of the Secret Image

For recovery of the secret image at the authentic entity end, the meaningful shares are obtained from all the cloud servers and XORed together with corresponding pixel position values to decrypt the value of the secret

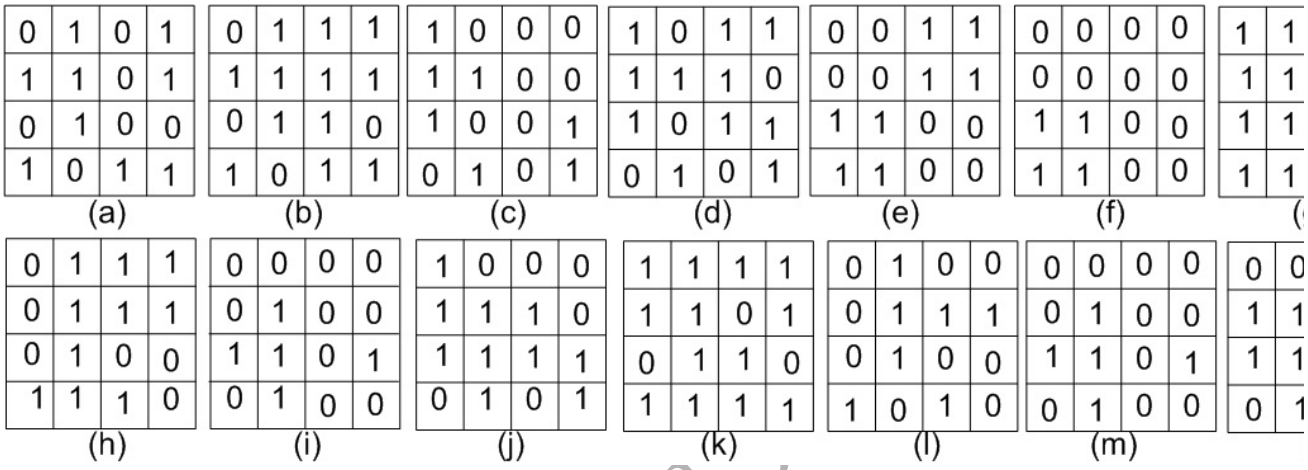

Figure 6: An example of proposed approach for $n = 3$ (a) Secret image S, (b)-(d) Random shares R_1, R_2, R_3 (e)-(g) Halftone cover images C_1, C_2, C_3 (h)-(j) Secret information embedded random shares R_1, R_2, R_3 (k) XORed secret image Z (l)-(n)Meaningful shares D_1, D_2, D_3

image S^R. The qualified set for recovery of the secret image contains only one possibility and that is, when all the meaningful shares are operated together. All other cases belonging to the forbidden set cannot reveal the information of the secret.

3.5. Verification and Analysis of the Proposed Approach

For a given VC scheme, it must satisfy the basic characteristics of visual cryptography. Theoretical analysis of the proposed algorithms has been discussed in this subsection on the basis of security condition, contrast condition of revealed secret image and meaningful shares to determine their validity for a (n, n) XOR based VC scheme.

3.5.1. Theoretical Analysis of Algorithm 2

Lemma 1: *Each of the n shares* R_1, R_2,...,R_n *generated from Algorithm 2 is totally random and does not give any information about the secret image* $S : T(R_k[S(0)]) = T(R_k[S(1)]) = 1/2$, *where* k=1,...,n.

Proof: For any $1 \times 2^{n-1}$ column vector in M_n^0 (M_n^1), its hamming weight is equal to $2^{n-2}(2^{n-2})$, and hence, the number of 1 is half of the vector length. According to *Algorithm* 2, the probability of randomly selecting row

vector from M_n^0 (M_n^1) for constructing n share pixels for secret pixel 0(1) is $1/2^{n-1}$. Thus, a bit 1 or 0 is assigned to share pixel $R_k(i,j)$ $(k = 1, \ldots, n)$ with probability 1/2. Hence, we can have $Prob(R_k(i,j) = 1|S(i,j) = 0) = Prob(R_k(i,j) = 1|S(i,j) = 1) = 1/2$ $(k = 1, \ldots, n)$, that implies R_k $(k = 1, \ldots, n)$ is a random liked image. By *Definitions* 1 and 2, we have $T(R_k[S(0)]) = T(R_k[S(1)])$=1/2 $(k = 1, \ldots, n)$. Therefore, each share is completely random and does not reveal any information about the secret image.

Lemma 2: *XOR result of any k out of n shares* $R_1, R_2, \ldots, R_n$, $(k < n)$ *generated from Algorithm 2,* $R_{(\oplus,x_1,\ldots,x_k)} = R_{x_1} \oplus \ldots \oplus R_{x_k}$ *does not reveal any information about the secret image* $S : T(R_{\oplus,x_1,\ldots,x_k}[S(1)]) = T(R_{\oplus,x_1,\ldots,x_k}[S(0)]) = 1/2$.

Proof: According to *Algorithm* 2, when $S(i,j) = 0$, a row vector is randomly selected from $M_n^0(1 : 2^{n-1}, [x_1, \ldots, x_k])$ with equal probability of $1/2^{n-1}$. In a simple matrix, the number of row vectors with odd hamming weight is same as that of row vectors with even hamming weight in matrix $M_n^0(1 : 2^{n-1}, [1, \ldots, k])$. The XOR result of row vector with even hamming weight is 0, while it is 1 in case of row vector with odd hamming weight, hence the probability of the result being a white pixel is 1/2, such that $Prob(R_{(\oplus,x_1,\ldots,x_k)}(i,j) = 1|S(i,j) = 0) = 1/2$. Same argument can be made when $S(i,j) = 1$ such that $Prob(R_{(\oplus,x_1,\ldots,x_k)}(i,j) = 1|S(i,j) = 1) = 1/2$. By *Definitions* 1 and 2, we have $T(R_{(\oplus,x_1,\ldots,x_k)}[S(1)]) = T(R_{(\oplus,x_1,\ldots,x_k)}[S(0)]) = 1/2$. Therefore, XOR result any k shares such that $k < n$ does not reveal any information about the secret image S.

Lemma 3: XOR result of the n shares $R_1, R_2, \ldots, R_n$ generated from *Algorithm* 2, $R_{\oplus,1,\ldots,n} = R_1 \oplus, \cdots \oplus R_n$ visually reveals the secret image $S : T(R_{\oplus,1,\ldots,n}[S(1)]) > T(R_{\oplus,1,\ldots,n}[S(0)])$.

Proof: According to *Algorithm* 2, when $S(i,j) = 0$, a row vector is randomly selected from M_n^0 with equal probability of $1/2^{n-1}$. In a simple matrix, the hamming weight of a row vector selected from M_n^0 is always even. Thus, XOR result is always 0. Hence, $T(R_{\oplus,1,\ldots,n}[S(0)]) = 0$. Similarly, hamming weight of row vector randomly selected from M_n^1 is always odd and XOR result is always 1. Hence, $T(R_{\oplus,1,\ldots,n}[S(1)]) = 1$. Thus, $T(R_{\oplus,1,\ldots,n}[S(1)]) - T(R_{\oplus,1,\ldots,n}[S(0)]) = 1 - 0 = 1$ and $T(R_{\oplus,1,\ldots,n}[S(1)]) > T(R_{\oplus,1,\ldots,n}[S(0)])$. Thus, the XOR result of n shares visually reveals the se-

cret image S.

Theorem 1. Let $R_1, R_2, \ldots, R_n$ be the n shares generated from *Algorithm* 2. Then, *Algorithm* 2 is valid for a (n, n) XOR-based VC scheme and meets the following conditions:

- Each of the n shares is completely random and does not give any information about the secret image $S : T(R_k[S(0)]) = T(R_k[S(1)]) = 1/2$, where $k = 1, \ldots, n$.
- XOR result of any k out of n shares such that $k < n$ $R_{(\oplus,x_1,\ldots,x_k)} = R_{x_1}\oplus, \ldots, \oplus R_{x_k}$ does not reveal any information about the secret image S: $T(R_{(\oplus,x_1,\ldots,x_k)}[S(1)]) = T(R_{(\oplus,x_1,\ldots,x_k)}[S(0)]) = 1/2$.
- XOR result of the n shares, $R_{\oplus,1,\ldots,n} = R_1\oplus, \ldots, \oplus R_n$ visually reveals the secret image $S : T(R_{\oplus,1,\ldots,n}[S(1)]) > T(R_{\oplus,1,\ldots,n}[S(0)]$.

Proof: The three conditions mentioned above are met from *Lemma* 1, 2, and 3, which proves the validity of *Algorithm* 2 for XOR-based VC scheme for (n, n) share generation.

Theorem 2: The contrast α_x of the XOR result of the n shares R_1, R_2,...,R_n generated from *Algorithm* 2 is 1.

Proof: From proof of *Lemma* 3, $T(R_{\oplus,1,\ldots,n}[S(0)]) = 0$ and $T(R_{\oplus,1,\ldots,n}[S(1)])$ =1. By $Definition$ 3, the contrast of XOR result is calculated as

$$\alpha_x = \frac{T(R_{\oplus,1,\ldots,n}[S(1)]) - T(R_{\oplus,1,\ldots,n}[S(0)])}{1 + T(R_{\oplus,1,\ldots,n}[S(0)])} = \frac{1-0}{1+0} = 1 \tag{7}$$

3.5.2. Theoretical Analysis of Algorithm 3

Lemma 4. Every share D_k $(k = 1, \ldots, n)$ generated from *Algorithm* 3 is a meaningful share that resembles the corresponding cover image C_k $(k = 1, \ldots, n) : T(D_k[C_k(1)]) > T(D_k[C_k(0)])$, but does not give any information about secret image $S : T(D_k[S(1)]) = T(D_k[S(0)])$.

Proof: Since half of the pixels in each share are generated directly from the secret S and in other half, the cover image information is embedded, when the cover image pixel $C_k(i, j) = 0$, then

$$Prob(D_k(i, j) = 1 | C_k(i, j) = 0) = \frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times 0 = \frac{1}{4} \tag{8}$$

When the cover image pixel $C_k(i,j) = 1$ then

$$Prob(D_k(i,j) = 1 | C_k(i,j) = 1) = \frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times 1 = \frac{3}{4} \tag{9}$$

From Equation 8 and Equation 9, it can be seen that $Prob(D_k(i,j) = 1|C_k(i,j) = 1) > Prob(D_k(i,j) = 1|C_k(i,j) = 0)$. By $Definition$ 1, we have $T(D_k[C_k(1)]) > T(D_k[C_k(0)])$, which implies the share D_k $(k = 1, \ldots, n)$ is a meaningful image which can resemble the cover image.

For pixels in which the cover image information is not embedded, from *Lemma* 1, the average light transmission of the share pixel $D_k(i,j)$ $(k = 1, \ldots, n)$ is always $1/2$ no matter the secret pixel $S(i,j)$ is white or black. In case of pixels in which the cover image information is embedded, the generation of the share pixel $D_k(i,j)$ $(k = 1, \ldots, n)$ does not depend on the secret pixel $S(i,j)$, either. Therefore, the share pixel $D_k(i,j)$ $(k = 1, \ldots, n)$ is generated independently of the secret pixel $S(i,j)$. Hence, $T(D_k[S(1)]) = T(D_k[S(0)])$ $(k = 1, \ldots, n)$, which implies the share S_k $(k = 1, \ldots, n)$ does not give any information about secret image.

Lemma 5: The XOR result of any $k < n$ shares of n meaningful shares $D_1, \ldots, D_n$ generated from *Algorithm* 3, $D_{(\oplus, x_1, \ldots, x_k)} = D_{x_1} \oplus \ldots \oplus D_{x_k}$ does not reveal any information about the secret image $S : T(D_{(\oplus, x_1, \ldots, x_k)}[S(1)]) = T(D_{(\oplus, x_1, \ldots, x_k)}[S(0)])$.

Proof: When k share pixels $D_1(i,j), \ldots, D_k(i,j)$ are constructed in which information of cover image is not embedded, then from *Lemma* 2, the average light transmission of the XOR result of k share pixels is always $1/2$ and does not depend on whether the secret pixel is black or white. When k share pixels $D_1(i,j), \ldots, D_k(i,j)$ are constructed in which information of cover image is embedded, their generation is independent of the secret pixel $S(i,j)$ and the average light transmission of their XOR result is assigned a fixed value ψ. Since half of the pixels in each share are generated directly from the secret S and in other half, the cover image information is embedded, we have

$$T(D_{(\oplus, x_1, \ldots, x_k)}[S(1)]) = \frac{1}{2} \times \frac{1}{2} + \frac{1}{2}\psi = \frac{1}{4} + \frac{1}{2}\psi \tag{10}$$

$$T(D_{(\oplus, x_1, \ldots, x_k)}[S(0)]) = \frac{1}{2} \times \frac{1}{2} + \frac{1}{2}\psi = \frac{1}{4} + \frac{1}{2}\psi \tag{11}$$

Hence, $T(D_{(\oplus,x_1,\ldots,x_k)}[S(1)]) = T(D_{(\oplus,x_1,\ldots,x_k)}[S(0)])$. Therefore, XOR result of any k shares does not reveal any information about the secret image.

Lemma 6: The XOR result of n meaningful shares $D_1, \ldots, D_n$ generated from *Algorithm* 3, $D_{(\oplus,1,\ldots,n)} = D_1 \oplus \ldots \oplus D_n$ visually reveals the secret image $S : T(D_{\oplus,1,\ldots,n}[S(1)]) > T(D_{\oplus,1,\ldots,n}[S(0)])$.

Proof: When n share pixels are constructed in which information of cover image is not embedded, then from *Lemma* 3, for white pixels of the secret image, the average light transmission for XOR result of n shares is $T(D_{\oplus,1,\ldots,n}[S(1)]) = 1$. For black pixels of the secret image, $T(D_{\oplus,1,\ldots,n}[S(0)]) = 0$. When n share pixels are constructed in which information of cover image is embedded, the pixels are XORed and if $T(D_{\oplus,1,\ldots,n}[S(1)]) \neq 1$ or $T(D_{\oplus,1,\ldots,n}[S(0)]) \neq 0$, then the value of the pixel in one of the shares is flipped. Hence, we have

$$T(D_{\oplus,1,\ldots,n}[S(1)]) = 1 \tag{12}$$

$$T(D_{\oplus,1,\ldots,n}[S(0)]) = \frac{1}{2} \times 0 + \frac{1}{2} \times 0 = 0 \tag{13}$$

Therefore, $T(D_{\oplus,1,\ldots,n}[S(1)]) > T(D_{\oplus,1,\ldots,n}[S(0)])$. Hence, XOR result of n shares visually reveals the secret image.

Lemma 7: The XOR result of n meaningful shares $D_1, \ldots, D_n$ generated from *Algorithm* 3, $D_{(\oplus,1,\ldots,n)} = D_1 \oplus \ldots \oplus D_n$ does not reveal any information about the cover images $C_1, \ldots, C_n$: $T(D_{(\oplus,1,\ldots,n)}[C_1(1), \ldots, C_n(1)]) = T(D_{(\oplus,1,\ldots,n)}[C_1(0), \ldots, C_n(0)])$.

Proof: Construction of n share pixels in which information of cover image is not embedded is done independent of the cover images $C_1, \ldots, C_n$, hence $T(D_{(\oplus,1,\ldots,n)}[C_1(1), \ldots, C_n(1)]) = T(D_{(\oplus,1,\ldots,n)}[C_1(0), \ldots, C_n(0)]) = 1/2$. When n share pixels are constructed in which information of cover image is embedded, the XOR result of n share pixels is always equal to 0. Since half of the pixels in each share are generated directly from the secret S and in other half, the cover image information is embedded, we have

$$T(D_{(\oplus,1,\ldots,n)}[C_1(1), \ldots, C_n(1)]) = \frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times 0 = \frac{1}{4} \tag{14}$$

$$T(D_{(\oplus,1,\ldots,n)}[C_1(0),\ldots,C_n(0)]) = \frac{1}{2}\times\frac{1}{2}+\frac{1}{2}\times 0 = \frac{1}{4} \tag{15}$$

Hence, $(D_{(\oplus,1,\ldots,n)}[C_1(1),\ldots,C_n(1)]) = T(D_{(\oplus,1,\ldots n)}[C_1(0),\ldots,C_n(0)])$. Therefore, XOR result does not reveal any information about the cover images.

Theorem 3: Let $D_1, D_2, \ldots, D_n$ be the n shares generated from *Algorithm* 3. Then, *Algorithm* 3 is valid for a (n, n) XOR-based VC scheme for meaningful shares and meets the following conditions:

- Every share D_k $(k = 1,\ldots,n)$ is a meaningful share that resembles the corresponding cover image $C_k(k = 1,\ldots,n) : T(D_k[C_k(1)]) > T(D_k[C_k(0)])$, but does not give any information about secret image $S : T(D_k[S(1)]) = T(D_k[S(0)])$.
- The XOR result of any $k < n$ shares of n meaningful shares, $D_{\oplus,x_1,\ldots,x_k} = D_{x_1}\oplus\ldots\oplus D_{x_k}$ does not reveal any information about the secret image $S : T(D_{(\oplus,x_1,\ldots,x_n)}[S(1)]) = T(D_{(\oplus,x_1,\ldots,x_n)}[S(0)])$.
- The XOR result of n meaningful shares,$D_{(\oplus,1\ldots n)} = D_1\oplus\ldots\oplus D_n$ visually reveals the secret image $S : T(D_{(\oplus,1,\ldots,n)}[S(1)]) > T(D_{(\oplus,1,\ldots,n)}[S(0)])$, but does not reveal any information about the cover images $C_1,\ldots,C_n$: $T(D_{(\oplus,1,\ldots,n)}[C_1(1),\ldots,C_n(1)]) = T(D_{(\oplus,1,\ldots,n)}[C_1(0),\ldots,C_n(0)])$.

Proof: The three conditions mentioned above are met from *Lemma* 4, 5, 6 and 7, which proves the validity of *Algorithm* 3 for XOR-based VC scheme for (n, n) share generation for meaningful shares.

Theorem 4: The contrast α_x of the XOR result of n meaningful shares $D_1,\ldots,D_n$ generated from *Algorithm* 3 is 1.

Proof: From proof of *Lemma* 6, $T(D_{\oplus,1,\ldots,n}[S(1)])$=1 and $T(D_{\oplus,1,\ldots,n}[S(0)])$=0. By *Definition* 3, the contrast of XOR result is calculated as

$$\alpha_x = \frac{T(D_{\oplus,1,\ldots,n}[S(1)]) - T(D_{\oplus,1,\ldots,n}[S(0)])}{1+T(D_{\oplus,1,\ldots,n}[S(0)])} = \frac{1-0}{1+0} = 1 \tag{16}$$

Theorem 5: The contrast α_{sh} of a share $D_k(k = 1,\ldots,n)$ generated from *Algorithm* 3 is 2/5.

Proof: From proof of *Lemma* 4 (Equation 8 and Equation 9),

$$T(D_k[C_k(0)]) = \frac{1}{4} \tag{17}$$

$$T(D_k[C_k(1)]) = \frac{1}{4} + \frac{1}{2} = \frac{3}{4} \tag{18}$$

From $Definition$ 4, the contrast of a share D_k is calculated as

$$\alpha_{sh} = \frac{T(D_k[C_k(1)]) - T(D_k[C_k(0)])}{1 + T(D_k[C_k(0)])} = \frac{3/4 - 1/4}{1 + 1/4} = \frac{2}{5} \tag{19}$$

where $k = 1, \ldots, n$.

3.6. Performance Analysis

The performance of the proposed XOR based VC scheme has been evaluated based on several properties desired in an efficient VC scheme. The foremost property needed is less storage requirements and fast transmission time. As in traditional VC schemes, it usually takes n share images to encode a given secret binary image. So storage requirements will be $n \times n$ for encrypting n secret images. The storage requirements are minimized in our proposed scheme as just n shares are required for transmitting n cover images plus one additional secret image that will be revealed by the combination of these shares. No extra storage requirements are demanded apart from these n shares. Second big hurdle in real time application is the pixel expansion problem that persists in most of the state-of-the-art approaches. Pixel expansion refers to number of pixels used in the encoded shares to represent a pixel of the secret image. Accordingly, the transmission time and storage requirements depend on it and increase proportionately with it. In our proposed scheme, we have taken care of pixel expansion and maintained the size of the encoded shares to be same as size of the secret image.

Next comes the sharing capacity which is an estimate of number of secret images shared over the number of shares. Mathematically, it can be defined as follows:

$$\eta = \frac{S}{D \times p} \tag{20}$$

where, S, D and p represent the number of secret images, number of shares and pixel expansion respectively. For our proposed scheme $p = 1$, hence the number of shares required for hiding n number of secrets will also

be n. The scheme can also be used as one of stenographic approaches for image based data hiding, where the hiding capacity is taken to be the ratio of size of the secret image to the size of cover image.

4. Experimental Results and Analysis

4.1. Experimental Results

Experiments have been performed on large set of standard images of different sizes. Results for some of the cover and secret images have been illustrated. Fig. 7 shows the various intermediate images generated at different steps while generation of meaningful shares.

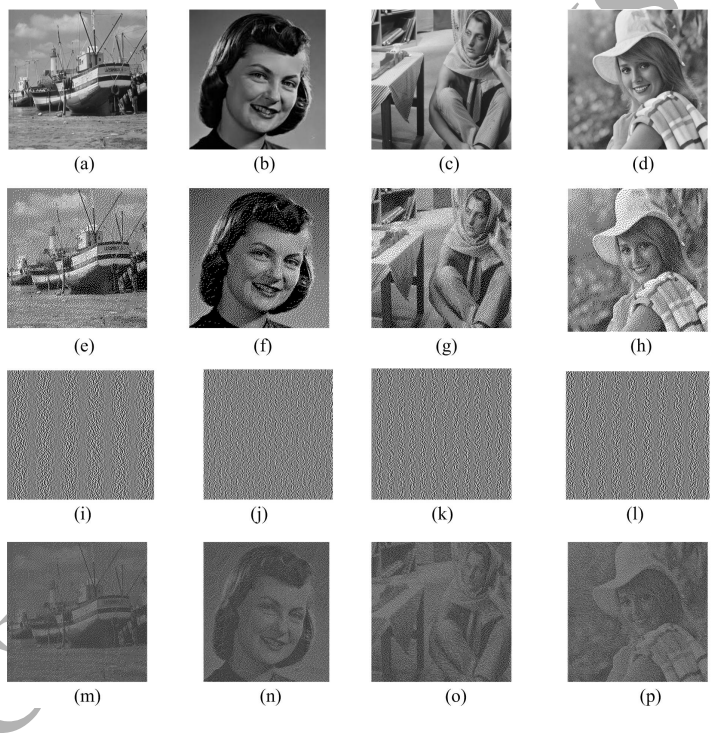

Figure 7: Different phases from original cover image to meaningful share, (a)-(d) Original Cover Images (e)-(h) Halftone Cover Images $C_1, C_2 \dots C_n$ (i)-(l) Random shares $R_1, R_2 \dots R_n$ (m)-(p) Meaningful shares $D_1, D_2 \dots D_n$

First of all, set of all original gray scale cover images are converted into halftone images by using existing error diffusion technique. By using proposed *Algorithm* 1 and 2, n random shares are formed with the help of

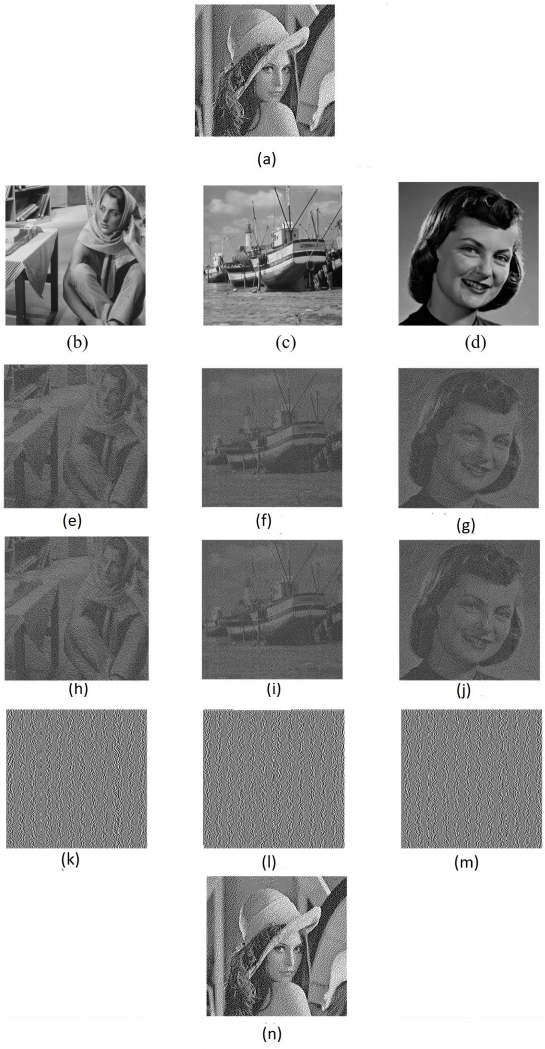

Figure 8: Experimental results for proposed approach where $n = 3$:(a) Secret image (b)-(d) Grayscale Cover Images (e)-(g) Halftone Grayscale Images (h)-(j)Meaningful shares (k)-(m) Results of XORing less than n shares ($(k) = (h) \oplus (i)$, $(l) = (i) \oplus (j)$, $(m) = (j) \oplus (h)$) (n)Revealed Secret Image via XORing all the shares

secret image. Ultimately n meaningful shares are generated using halftone cover images and random shares. All these transitions of images can be visualized by Fig. 7.

To understand the scheme better, the proposed visual cryptography scheme

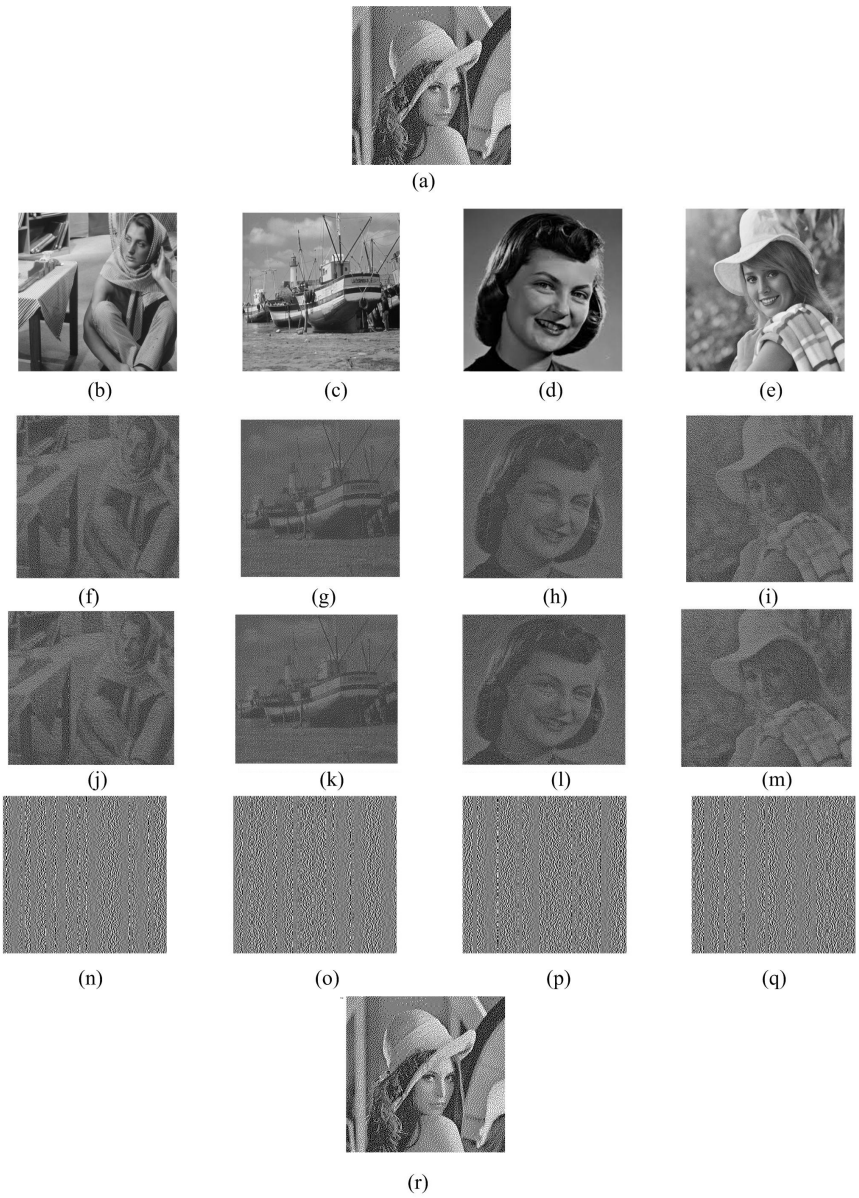

Figure 9: Experimental results for proposed approach where $n = 4$:(a) Secret image (b)-(e) Grayscale Cover Images (f)-(i) Halftone Grayscale Images (j)-(m)Meaningful shares (n)-(q) Results of XORing less than n shares ($(n) = (j) \oplus (k), (o) = (j) \oplus (k) \oplus (l), (p) = (k) \oplus (l) \oplus (m), (q) = (l) \oplus (m) \oplus (j)$) (r)Revealed Secret Image via XORing all the shares

has been illustrated for two cases when number of participants are three ($n = 3$) and four ($n = 4$) in Fig. 8 and Fig. 9 respectively. One can see that all shares are meaningful in nature and do not reveal the secret image when less than n shares are stacked together. Only random looking images will be obtained is all such cases until all the shares are stacked together to reveal the original secret image. The proposed scheme can easily handle shares even when number of participants is very large as a unique meaningful share is obtained for each participant. Even when one of these shares is tampered, the owner of the share can be easily identified and the tampered share can be identified accordingly. Hence, it reduces the vulnerability of the scheme towards cryptanalysis. The visual quality of the obtained meaningful shares and revealed secret image via XORing of all the shares is quite good. To measure the similarity between the meaningful shares with respect to their halftone versions, various objective error metrics have been employed.

4.2. Objective Evaluation Parameters

Objective evaluation parameters are more suitable for assessing similarity of binary images as compared to the subjective parameters like Peak Signal to Noise Ratio (PSNR), Signal to Noise Ratio (SNR) and Mean Square Error (MSE) etc [23], [46],[11]. They are based on mutual relations between pixels (i.e neighborhood), their locations and pixel values respectively. For instance, a binary image with its various distorted versions with variations in their neighboring pixel values is depicted in Fig. 10. They can be distinguished by different objective error metrics, but not by the subjective parameters like PSNR, SNR, MSE, etc. which will be close to their ideal values and will not signify any distortion. Various error metrics are available for performing objective evaluation. Some of them are described in this subsection.

Let I and G be the input and output image. The total number of true positive, false positive, true negative and false negative pixels with respect to I and G be denoted by N_{TP}, N_{FP}, N_{TN} and N_{FN} respectively. The white pixels are assumed to be positive in an image while the black pixels are assumed to be negative. Hence, a true positive is marked when a pixel is white in both the output image and input image. A false positive is when the output image has a white pixel where the input image has black pixel. True negatives and false negatives can be defined in similar ways.

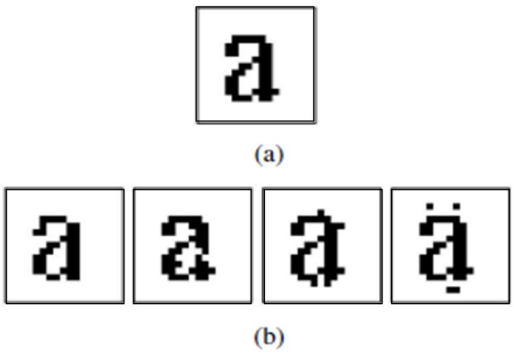

Figure 10: Variations in a binary image (a) Original binary image (b) Distorted binary images

4.2.1. Precision

Precision is also referred to as positive predictive value (PPV). It is the ratio of white pixels in the input image I to all the pixels that have been identified as white in the output image G, including the ones that were black in the input image I.

$$Precision = \frac{N_{TP}}{N_{TP} + N_{FP}} \tag{21}$$

For identical images value of Precision will be 1.

4.2.2. Recall/Sensitivity

Sensitivity or recall, also known as true positive rate, is the proportion of white pixels in the input image I that have been correctly identified as white pixels in output image G.

$$Recall = \frac{N_{TP}}{N_{TP} + N_{FN}} \tag{22}$$

For identical images the value of recall will be 1.

4.2.3. F-Measure

F-measure considers both precision and recall by calculating the harmonic mean of precision and recall.

$$FM = \frac{2 \times Recall \times Precision}{Recall + Precision} \tag{23}$$

For identical images the value of F-Measure will be 1.

4.2.4. Structural Similarity Index (SSIM)

SSIM is the measure of structural similarity between the output image G and input image I that compares the two images on the basis of luminance, contrast and structure. SSIM is Human Visual System (HVS) based measure defined as follows:

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_1)} \tag{24}$$

Where μ_x, μ_y, σ_x^2, σ_y^2 and σ_{xy} are the average, variance and covariance for x and y respectively. The resultant SSIM index is a decimal value between -1 and 1, and value 1 is attained when the two sets of data are exactly identical.

4.2.5. Specificity

Specificity, also known as true negative rate, is the proportion of black pixels in the input image I that have been correctly identified as black pixels in output image G.

$$Specificity = \frac{N_{TN}}{N_{TN} + N_{FP}} \tag{25}$$

For identical images value of specificity will be 1.

4.2.6. Balanced Classification Rate (BCR)/Area Under the Curve (AUC)

Balanced Classification Rate is the average of the proportion of white pixels and black pixels in the input image I that have been correctly identified as such in the output image G.

$$BCR = 0.5 \times (Specificity + Sensitivity) \tag{26}$$

For identical images the value of BCR/AUC will be 1.

4.2.7. Balanced Error Rate (BER)

Balanced Error Rate (BER) is the average of the proportion of white pixels and black pixels in the input image I that have been incorrectly identified as black pixels and white pixels respectively in the output image G.

$$BER = 100 \times (1 - BCR) \tag{27}$$

For identical images value of Precision will be 0.

4.2.8. Negative Rate Matrix (NRM)

Negative Rate Matrix (NRM) is based on the pixel wise mismatch between I and G. It is the average of false negative rate NR_{fn} and false positive rate NR_{fp}. NRM is based on pixel wise mismatch between I and G.

$$NRM = \frac{NR_{fn} + NR_{fp}}{2} \tag{28}$$

where

$$NR_{fn} = \frac{N_{FN}}{N_{FN} + N_{TP}} \tag{29}$$

$$NR_{fp} = \frac{N_{FP}}{N_{FP} + N_{TN}} \tag{30}$$

For identical images, value of NRM will be 0.

4.2.9. Distance-Reciprocal Distortion Measure (DRDM)

Distance-Reciprocal Distortion Measure (DRDM) is an objective distortion measure for two binary images. It is derived from the observation that distance between two pixels plays an important role in their mutual interference as perceived by human eyes. The distortion or flipping of one pixel (white pixel is changed to black and vice-versa) in the output image G with respect to input image I is more visible when it is in field of view of the pixel in focus.

Let W_m is the weight matrix and i_c and j_c are the center pixel.

$$W_m(i,j) = \begin{cases} 0, & \text{if } i_c = j_c \\ \frac{1}{\sqrt{(i-i_c)^2+(j-j_c)^2}}, & \text{otherwise} \end{cases} \tag{31}$$

This matrix is Normalized by.

$$W_{Nm}(i,j) = \frac{W_m(i,j)}{\sum_{i=1}^{m}\sum_{j=1}^{m} W_m(i,j)} \tag{32}$$

Now

$$DRD_k = \sum_{i,j}[D_k(i,j) \times W_{Nm}(i,j)] \tag{33}$$

Where D_k is given by $(B_k(i,j) - g[(x,y)_k])$. Thus DRD_k equals to he weighted sum of the pixels in the block B_k of the original image.

$$DRD = \frac{\sum_{k=1}^{s} DRD_k}{NUBN} \tag{34}$$

Where NUBN is the nonuniform blocks in $F(x,y)$. For identical Image DRDM will be 0.

To assess the similarity of the meaningful shares with respect to the halftone versions of cover images qualitatively, various objective error metrics have been calculated with values listed in Table 1 and Table 2 for number of participants $n = 3$ and $n = 4$ respectively.

Table 1: Various objective evaluation measures for meaningful shares with respect to the halftone versions of the cover images for (3,3) case

Objective Evaluation Methods	Meaningful Shares			
	Barbara	Boat	Face	Ideal Value
Precision	0.6915	0.7724	0.6823	1
Recall	0.7128	0.6299	0.8432	1
F-measure(%)	74.65	70.44	75.11	100
SSIM	0.8079	0.7123	0.8477	1
Specificity	0.7912	0.8352	0.7445	1
BCR	0.8944	0.8954	0.8056	1
BER(%)	10.56	10.46	19.44	0
NRM	0.1056	0.1046	0.1944	0
DRD	0.1989	0.1734	0.1311	0

Table 2: Various objective evaluation measures for meaningful shares with respect to the halftone versions of the cover images for (4,4) case

Objective Evaluation Methods	Meaningful Shares				
	Barbara	Boat	Face	Girl	Ideal Value
Precision	0.7153	0.7994	0.6617	0.6827	1
Recall	0.7079	0.6079	0.8579	0.7639	1
F-measure(%)	75.78	69.36	74.71	81.14	100
SSIM	0.8079	0.7235	0.8579	0.9645	1
Specificity	0.7811	0.8252	0.7329	0.5674	1
BCR	0.8995	0.8876	0.7954	0.7526	1
BER(%)	10.05	11.24	20.16	24.74	0
NRM	0.1005	0.1124	0.2016	0.2474	0
DRD	0.1849	0.1534	0.1102	0.0869	0

4.3. Attack on Shares

The shares of the secret image residing at the cloud servers may be altered intentionally or unintentionally. In case of an attack, the shares must be fragile enough to reflect the changes in itself as well as the recovered image obtained at the authentic entity end via XORing of the shares. Possible attacks may be categorized as follows:

- Brute force attack: No attacker can estimate the value of the secret pixel by looking at the insufficient number of shares. It implies that the bitstreams constituting the basis matrices for representing the secret pixel values '0' and '1' are indistinguishable. Both the basis matrices satisfy the contrast and security conditions of the basic visual cryptographic scheme which ensures that no matter how much computation power an attacker has, he cannot predict the value of the secret pixel [26]. Hence, no brute force attack is possible. For the proposed scheme, as there is no pixel expansion, let us suppose that the size of the secret image is $m \times m$. Then there will be, say n shares of size equal to that of the secret image i.e. $m \times m$. As the secret image is binary, it can have either of the two values '0' or '1' and each value is equi-probable i.e. 0.5. The possible number of combinations for a single share will be $2^{m \times m}$ and for n shares, it will become $2^{m \times m \times n}$. Hence, an attack need to apply $2^{m \times m \times n}$ number of attacks in order to reveal the value of the secret pixel.

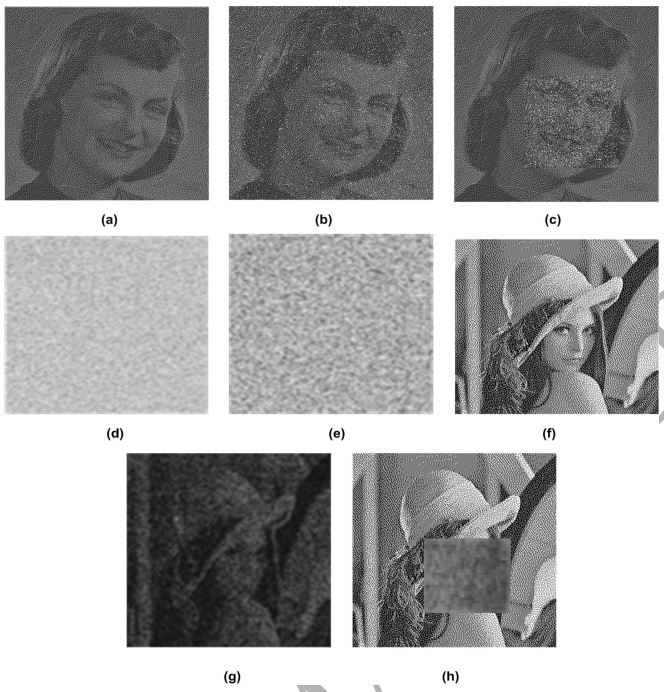

Figure 11: Attack scenarios on shares for proposed approach where $n = 4$:(a) One of the meaningful shares (b) Unintentional attack via addition of Salt & Pepper noise with density=0.3 (c)Intentional attack via tampering a region of interest (d) Random share (e) Random share with noise (f)Recovered secret image with unaltered share in (a) (g) Recovered secret image with altered share in (b)(h)Recovered secret image with altered share in (c)

- Unintentional attack on shares: The shares may get corrupted while transmission to the cloud servers via noises caused by the interferences occurring in the channel. One of such cases has been depicted in Fig.11(b) where one of the meaningful shares is corrupted with salt & pepper noise of density 0.3. The number of pixels getting affected by this noise will be approximately 0.3× (size of image). As the probability of black and white pixels is 0.5, the chances of adding more black pixels will be around 0.15× (size of image) and hence it would cause contrast loss in the share and the recovered image with the same factor of noise density. The result is depicted in Fig.11(g).

- Intentional attack on shares: The shares could be attacked intentionally in some regions of interest as depicted in Fig.11(c) via adding noises to

it or the whole share in itself could be tampered. The alterations due to the attack will be reflected back in the recovered image as depicted in Fig.11(h). If the quality of the recovered images deteriorates beyond an acceptable limit, the authentic entity can request for resending of the tampered share as it can be easily identified by the meaningful information on the shares.

4.4. Computational complexity

The computational complexity of the XORed based decryption in the proposed scheme is assessed and compared with the other state-of-the-art approaches. In a XORed based decryption, the computational complexity is directly proportional to the number of participants involved. Let us suppose we have n participants, then complexity of our proposed scheme will be $O(n)$. A comparative study of the computational complexity of some of the existing state of art approaches with the proposed scheme is presented in Table 3 [33, 21, 13, 31, 43, 20, 44].

Table 3: Comparative performance based on decryption of schemes

Scheme	Computational Complexity
Ours	O(n)
[27]	O(n)
[40]	O(n)
[33]	O(n)
[21]	O(n)
[13]	O(1)
[31]	O(1)
[43]	O(1)
[20]	O($nlog^2n$)
[44]	O($nlog^2n$)

Schemes based on Shamir's method have more computational complexity as they involve interpolation and polynomial evaluations [20, 44, 28] whereas OR based schemes require no computation at all while decrypting the secret image [13, 31, 43]. The proposed XOR based VC scheme lies intermediate between these two extremes along with other XOR based VC schemes [40, 33, 21, 27] but it provides other benefits like superior visual quality of shares and

recovered secret image, no pixel alignment problems, no pixel expansion and multiple meaningful shares which reduces the vulnerability to cryptanalysis.

5. Comparison with the state-of-the-art approaches

A comparative study of the proposed scheme with other state-of-the-art schemes has been done and depicted in Fig. 12-16 and Table 4-8. Fig. 12 shows the visual quality of the revealed secret images for our scheme, Ou et al. scheme [27] and Guo et al. scheme [13] for different number of shares. It can be seen that our scheme generates an identical secret image while in Ou et al. scheme [27], the white pixels are not constructed properly. The visual quality of Guo et al. scheme [13] is much worse. Moreover, the quality of secret image keeps on degrading as the number of shares is increased, which is not the case with our scheme.

Fig. 13 shows the comparison of our scheme with other schemes for different cases. From Fig. 13, it can be observed that our scheme provides better visual quality of the secret image and cover image for different number of shares. For assessment of visual quality of the shares and revealed images of Fig. 13, their contrasts have been given in Table 5. Our scheme provides higher contrast than Ou et al. scheme [27] and Wu et al. [41]. For odd number of shares, contrast for Ou et al. scheme [27] is even lower. Moreover, $T(S^R[S(1)])$ and $T(S^R[S(0)])$ in our scheme is always equal to 1 and 0, which is not the case in other schemes. Hence, our scheme provides perfect reconstruction of secret image, whereas other schemes do not.

The comparison of effect of number of shares on the contrast of revealed image has been depicted in Fig. 14. Our scheme provides better contrast than Ou et al. scheme [27] and Guo et al. scheme [13] and moreover, the contrast of the revealed secret image is independent of the number shares. Fig. 15 and Fig. 16 depict the comparison of contrast of the revealed images and shares respectively between our scheme and other approaches for different cases. From Fig. 15, it can be seen that the contrast of the revealed secret image provided by our scheme is very high (equal to 1) as compared to other schemes for different number of shares. Also, from Fig. 16, it can be observed that the contrast of shares provided by our scheme is higher than other that provided by other schemes. It is lower than the contrast for Ou et al. scheme [27] when $\beta = 0.2$. However, in that case the contrast of the revealed secret image provided by their scheme is very low. Table 4 tabulates the contrast of revealed image and secret image for different cases when β and P are equal to

Figure 12: The revealed secret images by our scheme, Ou et al. scheme [27] and Guo et al. scheme [13] for different number of shares, β and P are set to 0.5 (a) Secret image, (b) Cover image, (c) Guo et al. [13] (3,3) case, (d) Ou et al. [27] (3,3) case, (e) our (3,3) case, (f) Guo et al. [13] (4,4) case, (g) Ou et al. [27] (4,4) case, (h) our (4,4) case, (i) Guo et al. [13] (5,5) case, (j) Ou et al. [27] (5,5) case, (k) our (5,5) case, (l) Guo et al. [13] (6,6) case, (m) Ou et al. [27] (6,6) case, (n) our (6,6) case, (o) Guo et al. [13] (7,7) case, (p) Ou et al. [27] (7,7) case, (q) our (7,7) case

0.5 in case of Ou et al. scheme [27] and Guo et al. scheme [13] respectively. It can be observed that there is perfect reconstruction of the secret image in our scheme and higher contrast than other schemes.

Comparison of objective evaluation measures for meaningful shares with respect to the halftone versions of cover images has been done in Table 6 and Table 7 for (3,3) case and (4,4) case respectively. From Table 6 and

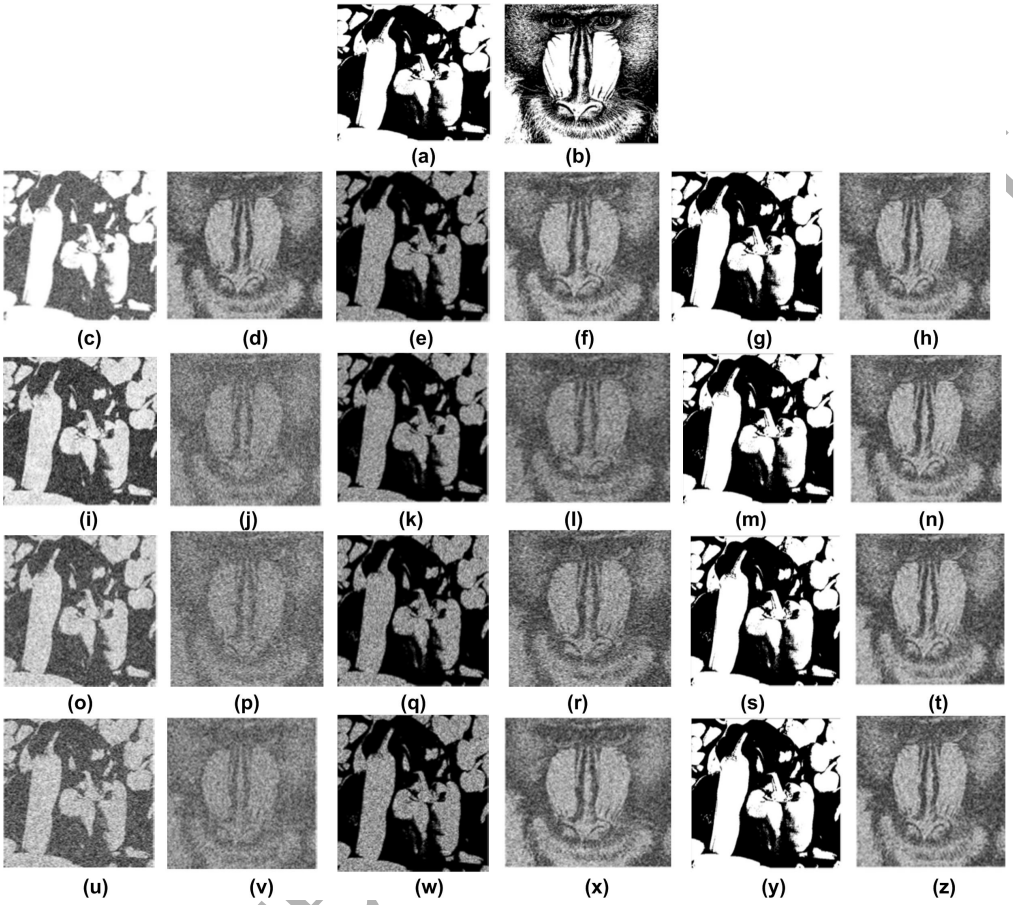

Figure 13: Visual quality for our scheme, Ou et al. scheme [27] and Wu et al. scheme [41] (a) Secret image, (b) cover image, (c)-(d) Wu et al. [41] (2,2) case, (e)-(f) Ou et al. [27] (2,2) case (g)-(h) our (2,2) case, (i)-(j) Wu et al. [41] (3,3) case, (k)-(l) Ou et al. [27] (3,3) case (m)-(n) our (3,3) case, (o)-(p) Wu et al. [41] (4,4) case, (q)-(r) Ou et al. [27] (4,4) case (s)-(t) our (4,4) case, (u)-(v) Wu et al. [41] (5,5) case, (w)-(x) Ou et al. (5,5) [27] case (y)-(z) our (5,5) case

Table 7, it can be inferred that for different parameters, our scheme provides better results than Ou et al. scheme [27], Guo et al. scheme [13], and Wu et al. [41]. Hence, it can be inferred that the numbers of true positives and true negatives for our scheme are higher than those of other schemes and the numbers of false positives and false negatives are lower in case of our scheme.

To further evaluate the efficacy of the proposed scheme, it has been com-

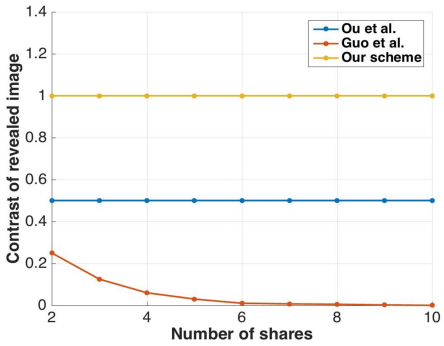

Figure 14: Contrast curves of our scheme, Ou et al. scheme [27] and Guo et al. scheme [13] for share numbers from 2 to 10.

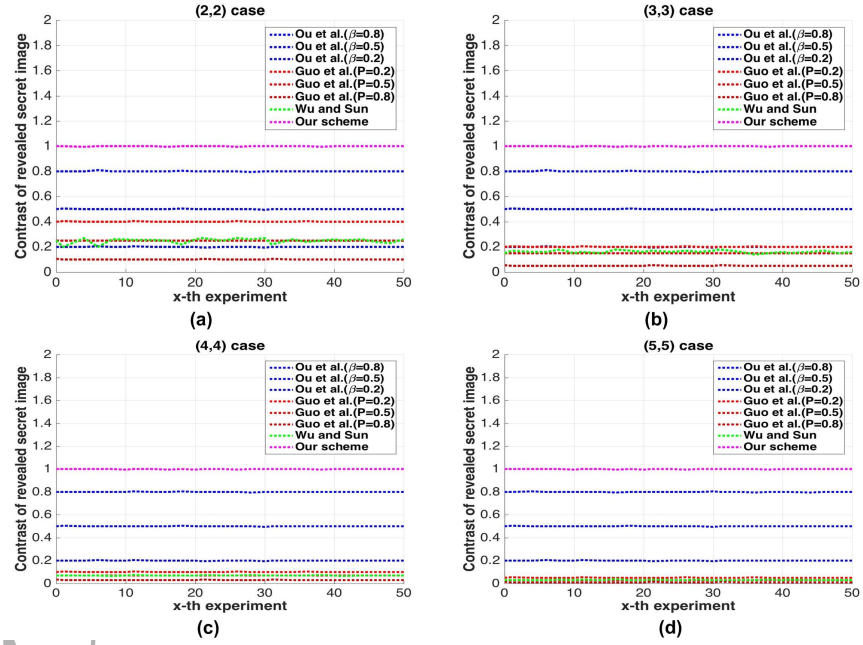

Figure 15: Contrast comparisons of the revealed images among our scheme, Ou et al. scheme [27] Guo et al. scheme [13] and Wu et al. scheme [41] for (a) (2,2) case, (b) (3,3) case, (c) (4,4) case, (d) (5,5) case

pared with the other existing state-of-the-art approaches tabulated in Table 8. To assist evaluation, some of these criteria are described as follows:

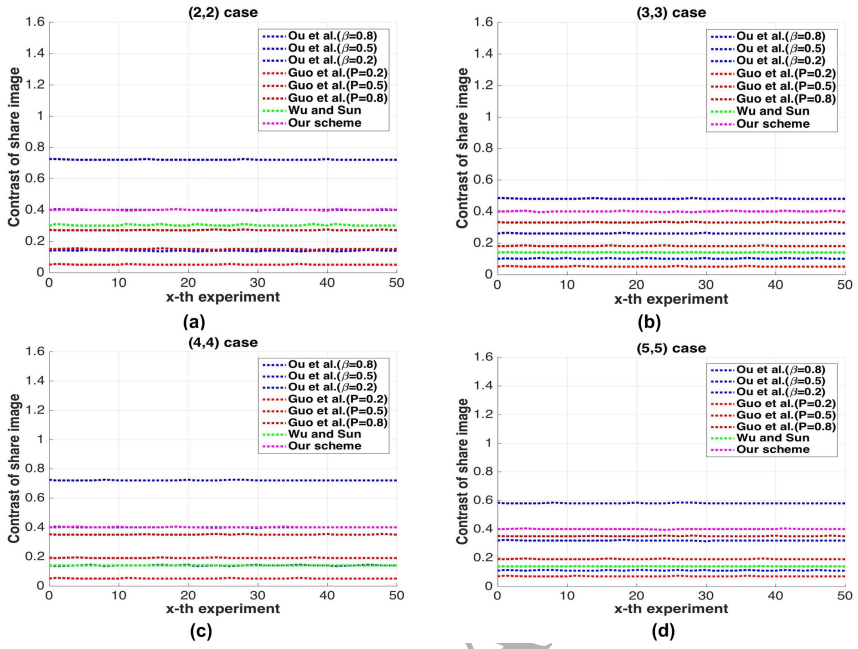

Figure 16: Contrast comparisons of the shares among our scheme, Ou et al. scheme [27], Guo et al. scheme [13] and Wu et al. scheme [41] for (a) (2,2) case, (b) (3,3) case, (c) (4,4) case, (d) (5,5) case

1. **Pixel expansion p:** It refers to number of sub-pixels used for encoding one pixel of secret information p. It must be as small as possible to minimize the transmission time and increase bandwidth utilization. In our proposed scheme as there was no pixel expansion in the obtained shares so $p = 1$.
2. **Decoding process:** Decoding of secret image can be done either by direct identification by human visual system (HVS) via stacking of transparencies or through small computational devices or high resource requirement. In the proposed scheme, it was maintained in between the two extremes and secret information could be recovered by simple XORing using small computational devices.
3. **Content of shares:** The content of shares can be either meaningful or random. Meaningful shares are preferred over random ones as they reduce the vulnerability of random shares to cryptanalysis and in case of attacks, tampered share can be identified. If the visual quality of the secret information recovered by the attacked share is beyond the

Table 4: Average contrasts of both revealed image and share for our scheme, Ou et al. scheme [27], Guo et al. scheme [13] and Wu et al. scheme [41] under different cases

Cases	Schemes	Average			
		$T(S^R[S(1)])$	$T(S^R[S(0)])$	α for revealed image	α for share
(2,2)	[13]	0.2502	0	0.2502	0.1502
	[27]	0.5003	0	0.5003	0.3996
	[41]	0.4831	0.1829	0.2547	0.3073
	Ours	1.000	0	1.000	0.4126
(3,3)	[13]	0.1251	0	0.1251	0.1832
	[27]	0.4996	0	0.4996	0.2668
	[41]	0.2645	0.0976	0.1525	0.1428
	Ours	1.000	0	1.000	0.3983
(4,4)	[13]	0.0626	0	0.0626	0.1941
	[27]	0.4998	0	0.4998	0.3999
	[41]	0.1431	0.1347	0.0690	0.1431
	Ours	1.000	0	1.000	0.4002
(5,5)	[13]	0.0313	0	0.0313	0.1976
	[27]	0.4998	0	0.4998	0.3200
	[41]	0.0735	0.0478	0.0245	0.1426
	Ours	1.000	0	1.000	0.4089

acceptable limit, resending of that particular share can be demanded at the authentic entity end. In the proposed scheme, we have obtained unique meaningful shares for storing at the cloud servers.

4. **Contrast $\alpha(m)$ of decoded image:** It ranges from 0 to 1. The contrast of the decoded image must be as high as possible. In the proposed scheme, it is obtained as 1 if no tampering is done with the shares at the cloud servers.
5. **Security criteria:** Any subset of shares from the forbidden set must not reveal the information of the secret image. In the proposed scheme, the meaningful shares obey the security criteria and reveal no information of the secret image if all the shares are not stacked.
6. **Codebook requirement:** Codebook is a pattern of all combinations of the basis matrices M_n^0 and M_n^1 and can be required either explicitly or implicitly. Implicit codebook is preferred as it saves storage requirement. In the proposed scheme, it is implicitly obtained at run

Table 5: Comparisons of contrast for the (2,2), (3,3), (4,4) and (5,5) case between our scheme, Ou et al. scheme [27], and Wu et al. scheme [41].

Cases	Schemes	Contrasts						
		D_1	D_2	D_3	D_4	D_5	Revealed Image S^R	$T(S^R[S(0)])$
(2,2)	[27]	0.3078	0.3067	-	-	-	0.5983	0
	[41]	0.3060	0.3080	-	-	-	0.4276	0.4009
	Ours	0.4010	0.4055	-	-	-	1.0000	0
(3,3)	[27]	0.2070	0.2056	0.2062	-	-	0.5990	0
	[41]	0.1424	0.1455	0.1423	-	-	0.5114	0.2578
	Ours	0.3995	0.4005	0.4015	-	-	1.0000	0
(4,4)	[27]	0.3096	0.3091	0.3079	0.3089	-	0.5982	0
	[41]	0.1456	0.1423	0.1410	0.1411	-	0.3915	0.3110
	Ours	0.4140	0.4048	0.4042	0.4012	-	1.0000	0
(5,5)	[27]	0.2481	0.2463	0.2459	0.2452	0.2478	0.6019	0
	[41]	0.1421	0.1427	0.1393	0.1416	0.1428	0.3073	0.3475
	Ours	0.4056	0.3996	0.4045	0.3990	0.4180	1.0000	0

Table 6: Comparison of objective evaluation measures for meaningful shares with respect to the halftone versions of the cover images between our scheme, Ou et al. scheme [27], Guo et al. scheme [13] and Wu et al. scheme [41] for (3,3) case.

Objective Evaluation Methods	Meaningful Shares			
	[13]	[27]	[41]	Ours
Precision	0.4032	0.5034	0.2934	0.7154
Recall	0.4109	0.5194	0.3127	0.7286
F-measure(%)	0.4290	52.87	0.3012	73.40
SSIM	0.4923	0.5792	0.4493	0.7893
Specificity	0.4198	0.5845	0.3198	0.7903
BCR	0.5298	0.6376	0.4274	0.8651
BER(%)	47.12	36.38	57.48	13.49
NRM	0.4714	0.4637	0.5748	0.1348
DRD	0.7326	0.3832	0.6238	0.1678

time.

7. **Limit of shares:** It is pre-defining of the number of participants for which the scheme is applicable. In the proposed scheme, there is no

Table 7: Comparison of objective evaluation measures for meaningful shares with respect to the halftone versions of the cover images between our scheme, Ou et al. scheme [27], Guo et al. scheme [13] and Wu et al. scheme [41] for (4,4) case.

Objective Evaluation Methods	Meaningful Shares			
	[13]	[27]	[41]	Ours
Precision	0.4235	0.7034	0.3198	0.7148
Recall	0.4428	0.7194	0.3012	0.7344
F-measure(%)	0.4327	72.87	0.3498	75.25
SSIM	0.5235	0.7923	0.4298	0.8385
Specificity	0.4255	0.7845	0.3210	0.7267
BCR	0.5385	0.8376	0.4355	0.8338
BER(%)	46.48	16.38	56.23	16.55
NRM	0.4548	0.1637	0.5624	0.1655
DRD	0.5476	0.1832	0.6365	0.1339

such restriction on the number of shares and so it can be applied to a broad spectrum of real world problems.

8. **Identical meaningful shares:** n identical meaningful shares are equivalent to n random shares as still one cannot identify the desired share in case of some attack. The proposed scheme obtains unique meaningful shares and hence, no dispute problem exists as the attacked share can be traced easily.

Table 8: Comparison of relative reports on VC

Method	Pixel Expansion	Identical Meaningful Share	Meaningful Share	Decryption	$\alpha(m)$	CodeBook Generation	Limit of Shares
Naor and Shamir [26]	Yes(2 times)	—	No	Stack	1/2	Explicit	n
Fang and Lin [9]	Yes (4 times)	No	No	Stack	1/2	Explicit	n
Ateniese *et al.* [1]	Yes	No	No	Stack	1/2	Explicit	n
Giuseppe *et al.* [2]	Yes(4 times)	No	Yes	Stack	1/4	Explicit	n
Jin *et al.* [17]	Yes(4 times)	—	No	Stack & Compute	1/4	Explicit	n
Zhi Zhou *et al.* [48]	Yes(16 times)	No	Yes	Stack	1/16	Explicit	2
Wen Pim *et al.* [10]	Yes(4 times)	No	Yes	Stack	1/4	Implicit	n
Zhongmin Wang *et al.* [38]	Yes(12 times)	No	Yes	Stack	1/12	Explicit	n
Young Chang *et al.* [15]	No	No	No	Stack	(k-1)/2	Explicit	n
Young-Chang Hou *et al.* [15]	No	No	Yes	Stack	1/4	Explicit	2
Young-Chang Hou *et al.* -1 [10]	No	No	No	Stack	1/2	Implicit	n
Young-Chang Hou *et al.* -2 [10]	No	No	Yes	Stack	1/4	Implicit	n
Tzung-Her Chen *et al.* [36]	No	No	No	Stack	7/17	Implicit	n
Shyong Jian Shyu *et al.* [30]	No	No	No	Stack	1/4	Implicit	2
Wu *et al.* [39]	No	Yes	Yes	Compute	1	Implicit	n
Wu *et al.* [40]	No	Yes	Yes	Compute	7/17	Implicit	n
Wu *et al.* [33]	Yes	—	No	Compute	1	Explicit	n
Proposed Approach	**No**	**No**	**Yes**	**Compute**	**1**	**Implicit**	n

6. Conclusion and Future Scope

For secure hosting of media information over the cloud based architecture, a novel XOR based visual cryptography approach with unexpanded multiple meaningful shares has been proposed in this paper. It obscures the confidential information into multiple shares and reduces their vulnerability to cryptanalysis by turning them into shares carrying some meaningful information. This deceives the third party cloud data servers as some unimportant information is residing while in fact these combine to produce a confidential information at the authentic entity end. The storage requirements of the proposed scheme are minimized as there is no pixel expansion in the obtained shares favoring fast transmission over cloud architecture. Further, there is a huge boost in storage capacity as the scheme can transmit $n+1$ information with just n shares. Other existing demerits in the state-of-the-art algorithms like explicit requirement of codebook, random pattern on shares, predefining of number of participants, poor contrast of meaningful shares and recovered secret image are well taken care of. In fact, the recovered secret image is lossless. Hence this scheme is very efficient for scenarios which require transmission of secure confidential information over cloud. Three novel algorithms were proposed to accomplish aforementioned objectives. The comparative study of the proposed scheme with existing state-of-the-art approaches validate its efficacy.

Acknowledgements
This work was supported by Information Security Education and Awareness (ISEA) Project (phase II) MIT-867-CSE, DeitY, New Delhi, INDIA

References

[1] Ateniese, G., Blundo, C., Santis, A. D., Stinson, D. R., 1996. Visual cryptography for general access structures. Information and Computation 129 (2), 86 – 106.
URL http://www.sciencedirect.com/science/article/pii/S0890540196900760

[2] Ateniese, G., Blundo, C., Santis, A. D., Stinson, D. R., 2001. Extended capabilities for visual cryptography. Theoretical Computer Science 250 (1), 143 – 161.

URL http://www.sciencedirect.com/science/article/pii/S0304397599001279

[3] BBC, 2014. Apple to tighten icloud security after celebrity leaks.
URL http://www.bbc.com/news/technology-29076899

[4] Blundo, C., Bonis, A. D., Santis, A. D., 2001. Improved schemes for visual cryptography. Designs, Codes and Cryptography 24 (3), 255–278.
URL http://dx.doi.org/10.1023/A:1011271120274

[5] Blundo, C., D'Arco, P., Santis, A. D., Stinson, D. R., 2003. Contrast optimal threshold visual cryptography schemes. SIAM Journal on Discrete Mathematics 16 (2), 224–261.
URL http://dx.doi.org/10.1137/S0895480198336683

[6] Chen, F., Zhang, C., Wang, F., Liu, J., Wang, X., Liu, Y., Sept 2015. Cloud-assisted live streaming for crowdsourced multimedia content. IEEE Transactions on Multimedia 17 (9), 1471–1483.

[7] Chen, T. H., Tsao, K. H., Jul. 2011. Threshold visual secret sharing by random grids. J. Syst. Softw. 84 (7), 1197–1208.
URL http://dx.doi.org/10.1016/j.jss.2011.02.023

[8] Chen, Y. C., Horng, G., Tsai, D. S., July 2012. Comment on x201c;cheating prevention in visual cryptography x201d;. IEEE Transactions on Image Processing 21 (7), 3319–3323.

[9] Fang, W., Lin, J., 2006. Progressive viewing and sharing of sensitive images. Pattern Recognition and Image Analysis 16 (4), 632–636.
URL http://dx.doi.org/10.1134/S1054661806040080

[10] Fang, W. P., Apr. 2008. Friendly progressive visual secret sharing. Pattern Recogn. 41 (4), 1410–1414.
URL http://dx.doi.org/10.1016/j.patcog.2007.09.004

[11] Furht, B., Muharemagic, E., Socek, D., 2005. Multimedia Encryption and Watermarking (Multimedia Systems and Applications). Springer-Verlag New York, Inc., Secaucus, NJ, USA.

[12] Gao, G., Zhang, W., Wen, Y., Wang, Z., Zhu, W., Aug 2015. Towards cost-efficient video transcoding in media cloud: Insights learned from

user viewing patterns. IEEE Transactions on Multimedia 17 (8), 1286–1296.

[13] Guo, T., Liu, F., Wu, C., 2014. k out of k extended visual cryptography scheme by random grids. Signal Processing 94, 90 – 101.
URL http://www.sciencedirect.com/science/article/pii/S0165168413002211

[14] Hofmeister, T., Krause, M., Simon, H. U., 2000. Contrast-optimal k out of n secret sharing schemes in visual cryptography. Theoretical Computer Science 240 (2), 471 – 485.
URL http://www.sciencedirect.com/science/article/pii/S0304397599002431

[15] Hou, Y. C., Wei, S. C., Lin, C. Y., May 2014. Random-grid-based visual cryptography schemes. IEEE Transactions on Circuits and Systems for Video Technology 24 (5), 733–744.

[16] Hu, C. M., Tzeng, W. G., 2007. Cheating prevention in visual cryptography. IEEE Transactions on Image Processing 16 (01), 36–45.

[17] Jin, D., Yan, W. Q., Kankanhalli, M. S., 2005. Progressive color visual cryptography. Journal of Electronic Imaging 14 (3), 033019–033019–13.
URL http://dx.doi.org/10.1117/1.1993625

[18] Koga, H., Ueda, E., 2006. Basic properties of the (t, n)-threshold visual secret sharing scheme with perfect reconstruction of black pixels. Designs, Codes and Cryptography 40 (1), 81–102.
URL http://dx.doi.org/10.1007/s10623-005-6700-y

[19] Lee, Y. S., Chen, T. H., Mar. 2012. Insight into collusion attacks in random-grid-based visual secret sharing. Signal Process. 92 (3), 727–736.
URL http://dx.doi.org/10.1016/j.sigpro.2011.09.015

[20] Lin, C. C., Tsai, W. H., Nov. 2004. Secret image sharing with steganography and authentication. J. Syst. Softw. 73 (3), 405–414.
URL http://dx.doi.org/10.1016/S0164-1212(03)00239-5

[21] Liu, F., Wu, C., 2010. Optimal xor based (2,n)-visual cryptography schemes. IACR Cryptol. 545.

[22] Liu, F., Wu, C., June 2011. Embedded extended visual cryptography schemes. IEEE Transactions on Information Forensics and Security 6 (2), 307–322.

[23] Lu, H., Kot, A. C., Shi, Y. Q., Feb 2004. Distance-reciprocal distortion measure for binary document images. IEEE Signal Processing Letters 11 (2), 228–231.

[24] Myodo, E., Sakazawa, S., Takishima, Y., Oct 2006. Visual cryptography based on void-and-cluster halftoning technique. In: 2006 International Conference on Image Processing. pp. 97–100.

[25] Naor, M., Pinkas, B., 1997. Visual authentication and identification. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 322–336.
URL http://dx.doi.org/10.1007/BFb0052245

[26] Naor, M., Shamir, A., 1995. Visual cryptography. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 1–12.
URL http://dx.doi.org/10.1007/BFb0053419

[27] Ou, D., Sun, W., Wu, X., Mar. 2015. Non-expansible xor-based visual cryptography scheme with meaningful shares. Signal Process. 108 (C), 604–621.
URL http://dx.doi.org/10.1016/j.sigpro.2014.10.011

[28] Shamir, A., Nov. 1979. How to share a secret. Commun. ACM 22 (11), 612–613.
URL http://doi.acm.org/10.1145/359168.359176

[29] Shyu, S. J., Mar. 2007. Image encryption by random grids. Pattern Recogn. 40 (3), 1014–1031.
URL http://dx.doi.org/10.1016/j.patcog.2006.02.025

[30] Shyu, S. J., Mar. 2007. Image encryption by random grids. Pattern Recogn. 40 (3), 1014–1031.
URL http://dx.doi.org/10.1016/j.patcog.2006.02.025

[31] Shyu, S. J., 2009. Image encryption by multiple random grids. Pattern Recognition 42 (7), 1582 – 1596.
URL http://www.sciencedirect.com/science/article/pii/S003132030800335X

[32] Tuyls, P., Hollmann, H. D., Lint, J. H., Tolhuizen, L., Oct. 2005. Xor-based visual cryptography schemes. Des. Codes Cryptography 37 (1), 169–186.
URL http://dx.doi.org/10.1007/s10623-004-3816-4

[33] Tuyls, P., Hollmann, H. D. L., Lint, J. H. V., Tolhuizen, L., 2005. Xor-based visual cryptography schemes. Designs, Codes and Cryptography 37 (1), 169–186.
URL http://dx.doi.org/10.1007/s10623-004-3816-4

[34] Ulichney, R. A., 1993. Void-and-cluster method for dither array generation. In: Human Vision, Visual Processing, and Digital Display IV. pp. 332–343.

[35] Vinton, K., 2014. Data breach bulletin: Staples, needmytranscript, icloud, sourcebooks.
URL http://www.forbes.com/sites/katevinton/2014/10/24/databreach-bulletin-staples-needmytranscript-com-icloudsourcebooks

[36] Wang, S., Gu, K., Ma, S., Lin, W., Liu, X., Gao, W., Feb 2016. Guided image contrast enhancement based on retrieved images in cloud. IEEE Transactions on Multimedia 18 (2), 219–232.

[37] Wang, Z., Arce, G. R., Di Crescenzo, G., Sep. 2009. Halftone visual cryptography via error diffusion. Trans. Info. For. Sec. 4 (3), 383–396.
URL http://dx.doi.org/10.1109/TIFS.2009.2024721

[38] Wang, Z., Arce, G. R., Di Crescenzo, G., Sep. 2009. Halftone visual cryptography via error diffusion. Trans. Info. For. Sec. 4 (3), 383–396.
URL http://dx.doi.org/10.1109/TIFS.2009.2024721

[39] Wu, X., Ou, D., Dai, L., Sun, W., 2013. Xor-based meaningful visual secret sharing by generalized random grids. In: Proceedings of the First ACM Workshop on Information Hiding and Multimedia Security. IH&MMSec '13. ACM, New York, NY, USA, pp. 181–190.
URL http://doi.acm.org/10.1145/2482513.2482515

[40] Wu, X., Sun, W., Sept 2013. Generalized random grid and its applications in visual cryptography. IEEE Transactions on Information Forensics and Security 8 (9), 1541–1553.

[41] Wu, X., Sun, W., Sept 2013. Generalized random grid and its applications in visual cryptography. IEEE Transactions on Information Forensics and Security 8 (9), 1541–1553.

[42] Wu, X., Sun, W., Jan. 2013. Random grid-based visual secret sharing with abilities of or and xor decryptions. J. Vis. Comun. Image Represent. 24 (1), 48–62.
URL http://dx.doi.org/10.1016/j.jvcir.2012.11.001

[43] Yang, C. N., Mar. 2004. New visual secret sharing schemes using probabilistic method. Pattern Recogn. Lett. 25 (4), 481–494.
URL http://dx.doi.org/10.1016/j.patrec.2003.12.011

[44] Yang, C. N., Chen, T. S., Yu, K. H., Wang, C. C., Jul. 2007. Improvements of image sharing with steganography and authentication. J. Syst. Softw. 80 (7), 1070–1076.
URL http://dx.doi.org/10.1016/j.jss.2006.11.022

[45] Yang, C. N., Wang, D. S., Feb 2014. Property analysis of xor-based visual cryptography. IEEE Transactions on Circuits and Systems for Video Technology 24 (2), 189–197.

[46] Young, D. P., Ferryman, J. M., 2005. Pets metrics: On-line performance evaluation service. In: Proceedings of the 14th International Conference on Computer Communications and Networks. ICCCN '05. IEEE Computer Society, Washington, DC, USA, pp. 317–324.
URL http://dl.acm.org/citation.cfm?id=1259587.1259810

[47] Yue, H., Sun, X., Yang, J., Wu, F., June 2013. Cloud-based image coding for mobile devices x2014;toward thousands to one compression. IEEE Transactions on Multimedia 15 (4), 845–857.

[48] Zhou, Z., Arce, G. R., Crescenzo, G. D., Aug 2006. Halftone visual cryptography. IEEE Transactions on Image Processing 15 (8), 2441–2453.

[49] Zhu, W., Luo, C., Wang, J., Li, S., May 2011. Multimedia cloud computing. IEEE Signal Processing Magazine 28 (3), 59–69.