Journal of Information Security and Applications 33 (2017) 16–29

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Affine Boolean classification in secret image sharing for progressive quality access control

Tapasi Bhattacharjee, Ranjeet Kumar Rout, Santi P. Maity*

Department of Information Technology, Indian Institute of Engineering Science and Technology, P.O. - Botanical Garden, Shibpur, Howrah 711 103, India

ARTICLE INFO

MSC:
00-01
99-00

Keywords:
Secret image sharing
Essential threshold
Affine Boolean functions
Kullback–Leibler divergence
Progressive quality access

ABSTRACT

Secret sharing plays an important role in confidential data protection by splitting the data into few noise-like shares or shadows. In the existing essential threshold based secret image sharing scheme, the decoding process depends on the essential as well as on the non-essential components. This paper proposes an essential threshold based progressive secret image sharing scheme. Affine Boolean functions are used to generate 2^i noise-like shares in 'i' levels, out of which at least 's' (2^{i-1}) shares are considered as essential and the rest are non-essential shares. Essential shares suffice to reconstruct/decode the secret image with a certain level of recognizability. The contribution of the non-essential part progressively aids on the quality of the reconstructed image. Robustness in term of decoding reliability of the proposed method is also studied against a set of common operations including random gain change on the share images. Extensive simulation results are also shown to validate the efficacy of the proposed method over a large number of existing works.

1. Introduction

Rapid advancement in computer and communication technologies have led to the wide spread use of digital media (audio, image, video data) in our day-to-day life. Transmission and retrieval of digital media are possible now almost in noise-free form over the wireless data communication network. Digital media can be easily captured, disseminated, sometimes even modified and duplicated without keeping any trace of such illegal operations [1]. Hence a serious concern in the form of various security related issues such as data misappropriation, illegal data usage, access control etc. are envisaged which in turn demand some form of protection and security in data transmission [2,3]. To offer security in transmission, several techniques such as cryptography (encryption), data hiding, secret sharing schemes etc. are developed and reported in the literature [4,5]. Contrary to the conventional data protection mechanisms (cryptography, data hiding etc.), secret sharing splits the secret data into several noise-like parts called shares. A group of authorized participants holding these shares can only read/retrieve the secret message, thus serves the purpose of access control in one way and in the other way it avoids intentional or accidental data loss [2].

Secret image sharing (SIS) scheme is a process of sharing a secret image into few noise-like shadow/ share images in the way that if shared images are combined in a specific way, the secret image can be decoded [6]. These shares are distributed among the group of legitimate participants. Only an authorized subset of participants can decode the secret image through cooperation. The forbidden subset of participants fail to retrieve any information about the secret image. All the authorized and the forbidden subset of users are the members of the access structure of the SIS scheme [7]. The concept of secret sharing was first independently investigated and reported by Blakley [8] and Shamir [9]. SIS schemes can be broadly classified into two categories: polynomial based secret image sharing (PSIS) and visual secret sharing (VSS) [10]. Both the schemes adopt different techniques and serve widely different applications [1]. PSIS schemes are based on Shamir's [9] scheme. Perfect reconstruction of the secret images are possible in these schemes using the Lagrange interpolation technique [11]. Thien and Lin [12] first proposed a (k, n) PSIS scheme based on [9] to generate image shares of reduced size. Here 'n' indicates the total number of shares, out of which 'k' number of shares are essential for decryption or decoding of the secret data. Later on many issues on PSIS schemes like smaller shadow images [13,14], smooth scalability [15], essentiality [10,16] etc. are extensively studied and developed to meet various requirements.

In VSS schemes, the decoding process requires neither any involvement of computation nor the use of any cryptography property [1]. The participants stack their shares to recognise visually

* Corresponding author.
E-mail addresses: tapasi.dgp@gmail.com (T. Bhattacharjee), ranjeetkumarrout@gmail.com (R.K. Rout), santipmaity@it.iiests.ac.in, spmaity@yahoo.com (S.P. Maity).

http://dx.doi.org/10.1016/j.jisa.2017.01.001
2214-2126/

the secret image using human visual system. The concept of VSS was first introduced by Shamir and Noar [17] for gray scale images. Pixel expansion and poor visual quality of the reconstructed images are the main disadvantages of their scheme. Later on different VSS schemes were proposed with the specific applications like region incrementing property [18,19], cheating prevention [20,21] etc. These methods use simple OR or X-OR operation in decoding process, and the visual quality of the reconstructed images are poor. Contrarily, in the PSIS schemes, higher quality secret images can be reconstructed more precisely without any pixel expansion.

Another form of SIS through bit-wise Boolean based operation is reported in [22,23]. Unlike simple stacking operation in VSS, Boolean based SIS uses some image manipulation techniques on bit-levels. Bit-wise Boolean operation based SIS schemes can reconstruct more precise (accurate) secret images as seen in PSIS schemes. However, PSIS schemes use Lagrange interpolation during reconstruction operation which is computation intensive. On the other hand, the computation requirement on the bit-wise Boolean-based operations is comparatively low and cost-effective [6]. Wang et al. [24] proposed a Boolean-based VSS scheme without any pixel expansion. Perfect reconstruction of the secret image is possible by introducing a little computation in the reconstruction process. Later on many bit-wise Boolean based SIS schemes were proposed [6,25,26]. The advantages of Boolean based SIS schemes lie on the simple operation for the generation of shares without any pixel expansion and distortionless reconstruction of images like PSIS schemes. Moreover, Boolean based SIS schemes require less computation involvement compared to PSIS schemes [6].

In most of the existing SIS schemes, each participant i.e. the individual share shows the same contribution or involvement in the reconstruction operation. But in many real life applications, all the shares hold by the respective participants may not expect to have same information content due to their status or importance in official or social fields [16]. Chen et al. [27] proposed a weighted SIS (WSIS) to generate the shadows according to the importance of the participants. Later on Lin et al. [28] proposed a WSIS scheme. The main disadvantage in WSIS scheme lies in determining the weights for the respective participants involved. To address such problem, an essential secret image sharing (ESIS) scheme was proposed by Li et al. [16]. In this scheme two groups of shares, namely as essential and non-essential are generated. The essential shares are distributed to the participants of higher importance, may be called a privilege group. Based on [16], Yang [10] proposed a new ESIS scheme. Reduction in essential shadow size is the main contribution of this scheme as it is suitable for modern visual communication. However, non-essential participants also contribute in the reconstruction process where without the use of the non-essential shares, the reconstruction of the secret image remains incomplete. Hence some form of dependency on the non-essential shares is a must to show the unambiguous decoding.

There may be some applications where essential shares seem to be enough for decoding without any ambiguity in the reconstruction of the secret images. Non-essential shares only aid in the quality improvement on the reconstructed image. Implementation process also sometimes demands low computational cost for the specific application to serve. Essential components with reduced size further offers the benefit of decoding from less amount of data. Hence, a hierarchical, cost effective SIS scheme with reduced share size needs its development and is considered in the present study. The essential components are good enough to decode the secret image to a certain quality of recognizability. The involvement of non-essential parts offers a relative improvement in the quality of the reconstructed secret image.

The organization of the paper is as follows: Section 2 presents the review works on some of the related SIS schemes with their limitations and the scope of the present work. Section 3 makes a brief discussion on mathematical preliminaries, first on classification of Boolean functions (since the present study is based on Boolean functions) and then on Kullback–Leibler divergence. Section 4 describes the proposed progressive SIS scheme. Section 5 presents performance evaluation with discussion. Conclusions are drawn in Section 6 along with scope of future works.

2. Literature review and scope of the present work

This section presents a brief literature review on SIS schemes with their relative strengths and weaknesses followed by the scope and contributions of the proposed work.

2.1. Essential SIS schemes

Relative importance of the shares (participants) in a WSIS was introduced by Chen et al. [27]. In this scheme, a group-based weighted SIS is proposed to assign different weights to the share images in such a way that a share with the higher weight can't be replaced by a share with the less weight in the decoding operation. However, in practical scenario, mathematical formulation followed by determining the weights of the participants, according to some hierarchical importance, sometimes becomes difficult and their calculation makes the method computationally expensive [16]. A hierarchical threshold secret image sharing scheme (HTSIS) to generate and distribute shares among a set of participants is proposed by Guo et al. [11]. But this scheme poses a serious security problem. Some illicit participants may reconstruct the secret image partially. The shortcoming of [11] was addressed and solved by Pakniat et al. [29]. The concept of cellular automata is used to propose a HTSIS scheme in which originality of the recovered image is checked by the participants.

Li et al. [16] propose a novel (t,s,k,n) ESIS scheme. In this scheme, the secret image is divided into 'n' shares using Shamir's secret sharing scheme [9]. The shares are divided into 's' essential and 'n-s' non-essential shares. The essential shadows are distributed to the participants with higher importance and non-essential shadows are distributed to less important participants. To reconstruct the secret image, the minimum 'k' shadows are required which include the minimum 't' essential shadows and the remaining non-essential shadows. In this scheme, threshold condition and essentiality conditions are satisfied. But the non-essential shares suffer from the problem of pixel expansion. The design of a (t,s,k,n) ESIS with reduced non-essential shadow size was kept as their future scope of work. Based on [16] and [29], a special kind of (t,s,k,n) HTSIS scheme with two security levels is proposed by Yang et al. [10]. In this scheme, the non-essential shadow sizes are less than the essential shadows sizes. This scheme may be treated as a type of PSIS as developed in [12]. Two layer hierarchical structures are followed for secret sharing. For successful reconstruction or decoding of the secret image, the mandatory involvement of both the essential and the non-essential shadows are required. However, two basic shortcomings in ESIS schemes are reported in [30]. These are unequal shadow size and concatenation of sub-shadows. These two problems may cause security vulnerability and make the decoding process more difficult. For concatenation of sub-shadows the location of each sub-shadow needs to be recorded. These two issues were addressed and reported by Li et al. [30]. In this scheme, each share image is generated using a single polynomial and no concatenation operation is required. They used derivative polynomial for share generation while Birkhoff interpolation technique was used for secret image reconstruction.

2.2. Boolean-based SIS schemes

A Boolean-based SIS scheme has been proposed by Chen and Wu [25] to share 'n−1' shadow images among 'n' shadows for decoding the secret image. Then X-OR operation is used for share generation and recovery. However, this scheme is not secure enough as simple X-OR operation is used and may leak some information about the secret data. The shortcomings of [25] are solved in the scheme by Chen et al. [26]. This scheme is a novel (n,n) multi-SIS (MSIS) scheme based on bit-wise Boolean operation. But some partial secret information may be decoded from 'n−1' or fewer share images. This compromises the threshold security of (n,n) MSIS scheme. To stop the information leakage in [26], a strong threshold MSIS scheme has been proposed in Yang et al. [6]. This is a (n,n) threshold scheme which does not leak any secret information from 'n-1' or fewer shadow images. This scheme adopts the same approach to generate random share images from even value of 'n' but the method is different for odd 'n'. In all the above schemes, each participant (share) plays (contributes) the same role (information) in the reconstruction process. However, as mentioned earlier there are many situations where some participants (shares) like company managers, head of government officials, high-level corporate officers etc. are accorded with special privilege according to their status or importance. This leads to the need of a hierarchy in SIS scheme. However, development of such prioritized SIS scheme has not been addressed much in the literature. This scheme attempts to explore the scope of Boolean-based prioritized SIS scheme.

2.3. Scope and contributions of the present work

Literature review of the previous works reveal that Boolean based schemes offer low computational cost. However, hierarchical approach is not addressed in Boolean based approach. On the other hand, WSIS schemes offer hierarchical approach with higher computational cost. Furthermore, in majority of the cases, involvement of the non-essential parts are mandatory to complete the decoding process. The objective of this study is to explore the scope of Boolean based approach, more specifically, the classification of the affine Boolean function to provide a hierarchical SIS scheme. Furthermore, essential components are of reduced size and do not keep any ambiguity in recognizability of the secret image without involvement of the non-essential share (s). The structure of Boolean function classification may be explored to meet some of these requirements and is briefly discussed below.

The classification of Boolean function offers benefits as follows: (a) equivalent functions in each class possess similar properties and (b) the number of representatives in each class is much less than that of Boolean functions.

The linear group and the affine Boolean function group of transformations are defined in [31]. This scheme proposed an algorithm for counting the number of classes under both the groups. Cryptographically strong balanced Boolean functions are envisioned in [32]. Later on classification of the affine equivalence classes of cosets of the first order Reed-Muller code with respect to cryptographic properties such as correlation immunity, resiliency, propagation characteristics have been discussed and reported in [33]. A systematic classification of all n-variable Boolean functions is studied and reported in [34,35]. In this scheme, only one affine Boolean function belongs to each class. Classification is achieved through a set of invariant bit positions with respect to an affine function of that class. The invariant bit positions also provide information regarding the size and symmetry properties of the classes/ sub-classes. The members of classes/ sub-classes satisfy certain similar properties. For each class of n-variable, the length of a Boolean function is 2^n, among which 'n+1' bits are fixed and remaining $2^n - (n+1)$ bits are changed with respect to the affine Boolean function of that class. The corresponding affine function is considered as the leader of a class. This can be considered as a kind of generating two shares: having leader in one share and non-linear Boolean functions or members in other share. The leader or priority class is mainly considered as essential part and the non-linear Boolean functions are considered as non-essential part of share images.

Based on the concepts of affine Boolean function on share generation, the present study proposes a progressive quality SIS scheme. The share images (2^i) are generate in 'i' levels. These shares are then distributed among two groups of participants: the privileged or higher priority participants are assigned with the essential shares (2^{i-1}) and the remaining shares are assigned to the less important participants. During the reconstruction process, the contribution of the complete set of essential components do not keep any ambiguity on recognizability. Non-essential shares progressively contribute on the quality of the reconstructed image. Involvement of all the participants decode the secret image precisely i.e. without loss of information. The total size of the generated shares is equal to the secret image size. In brief, the contributions of the work are summarized as follows:

(1) *Essential component requirement for decoding* - An essential threshold (2^{i-1}) is required to reconstruct the secret image from the share images (2^i). Essential components are sufficient for decoding the secret image to some certain degree of recognizability.
(2) *Quality access structure* - Progressive visual quality of the reconstructed secret image is possible through the involvement of all the essential participants and the variable number of non-essential components involved in the reconstruction operation.
(3) *Reduced shadow size* - The size of the generated shares are either $\frac{(n+1)}{2^n}^{\text{th}}$ or $\frac{(2^n-(n+1))}{2^n}^{\text{th}}$ times to that of the corresponding secret, thus reduced size shares are available which are advantageous for transmission and storage. Since, the present work is based on affine Boolean function classification, the next section makes a brief discussion on it.

3. Mathematical preliminaries

This section presents mathematical preliminaries on Classification of Boolean function and Kullback–Leibler divergence (KLD). The analysis is done to make the article self-understood.

3.1. Classification of Boolean function

The classification methodology of an n-variable affine Boolean function, as a representative one, is introduced here briefly. An n-variable Boolean function f is a mapping from the set of all possible n-bit strings $\{0, 1\}^n$ into $\{0, 1\}$. The number of different n-variable Boolean functions is 2^{2^n}, where each function can be represented by a truth table having output as a binary string of length 2^n. The decimal equivalent of the binary string starting from bottom to top (least significant bit) in the truth table is called the rule number of that function [36]. The complement of f is denoted as $\bar{f}$. A Boolean function with algebraic expression, where the degree is at most one is called an affine Boolean function. The general form for n-variable affine function is written below.

$$f_{affine}(x_1, x_2, x_3, \ldots, x_n) = k_n x_n \oplus k_{n-1} x_{n-1} \oplus \cdots \oplus k_2 x_2 \oplus k_1 x_1 \oplus k_0 \quad (1)$$

where the co-efficients are either zero or one. If the constant term k_0 of an affine function is zero, then the function is called a *linear Boolean function*. Thus, affine Boolean functions are either

linear Boolean function or their complements. The number of different n-variable affine Boolean functions is 2^{n+1}, out of which 2^n are linear. As an example, the '16' *affine Boolean functions* in 3-variables are 0, 60, 90, 102, 150, 170, 204, 240, 15, 51, 85, 105, 153, 165, 195, and 255. The first eight of them are linear and remaining Boolean functions are their corresponding complements [31].

If 'f' is a Boolean function of n-variables, the (n + 1)-variable Boolean functions can be represented as ff and $f\bar{f}$,

$$if\ f = \begin{pmatrix} 0 \\ 0 \end{pmatrix},\ then\ ff = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}\ and\ \ f\bar{f} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \tag{2}$$

Two different methods have been proposed for generating equivalence classes of Boolean functions with a precise objective that an exactly one affine Boolean function is present in a class [34,35]. Both the methods are discussed below in brief.

3.1.1. Recursive method to classify n-variable Boolean functions

This method is a recursive approach to classify n-variable Boolean functions starting from 1-variable to higher variables. Let $S_1 = \{(\mathbf{00}), (\mathbf{10}), (\mathbf{01}), (\mathbf{11})\}$ be a set of all 1-variable Boolean functions. These Boolean functions are affine.

Let $S'_1 = \{(\mathbf{00}), (\mathbf{10})\}$ be a set containing all linear Boolean functions of 1-variable. On the other hand, $S''_1 = \{(\mathbf{11}), (\mathbf{01})\}$ is a set that contains the complements of the set S'. The Cartesian product of the sets S_1 with S'_1 and S''_1 are defined as follows:

$S_1 \times S'_1 = \{(\mathbf{0000}, 0010), (\mathbf{1010}, 1000), (0100, \mathbf{0110}), (\mathbf{1100}, 1110)\}$ and

$S_1 \times S''_1 = \{(\mathbf{0011}, 0001), (1011, \mathbf{1001}), (0111, \mathbf{0101}), (\mathbf{1111}, 1101)\}$

Here, S_1 contains four classes each containing a 1-variable Boolean function where $(S_1 \times S'_1) \cup (S_1 \times S''_1)$ contains eight disjoint classes that exhaust all 2-variable Boolean functions. Each class contains exactly one affine Boolean function that is highlighted in Eqs. (2) and (3). The same process is repeated for the next higher variables using the recursive formula of Eq. (2).

$$S'_n = (S_{n-1}) \times (S'_{n-1}),\quad S''_n = (S_{n-1}) \times (S''_{n-1})\quad and$$
$$S_n = (S_{n-1}) \cup (S''_{n-1}) \tag{3}$$

S_n contains the classes of all n-variable Boolean functions. Each class contains the exactly one n-variable affine function. Both the sets S'_n and S''_n are complement to each other.

3.1.2. Non-recursive method to classify n-variable Boolean functions

In this method, the classification is done through the change in some variable bit positions with respect to the affine function belonging to that class. Let f_k^n is an n-variable affine Boolean function. An array 'A' is used to keep the fixed bit positions for a Boolean function with respect to f_k^n. This method keeps some of the bit positions fixed and changes the rest bits with respect to a Boolean function that corresponds to the classes of equal cardinality. If 'k' represents the number of fixed bit positions, then the number of equivalence classes is equal to 2^k. Different set of fixed positions generate different classes of Boolean functions. For a change in 'l' number of bit positions, the number of members in a particular class is 2^l where $0 \le l \le 2^n - k$. Any Boolean function, generated through this procedure, can be a representative for the class. Affine function is chosen as the representative of a class. The classification is done through the change in some variable bit positions with respect to the affine function belonging to that class.

In brief, the classification of Boolean function using recursive method works on Cartesian product, the usage of which in SIS schemes leads to an increasing the shadow size. On the contrary, non-recursive method works on the bit strings which generates the shadow images with reduced size. It is needless to mention that reduced size shares are preferred in SIS schemes for efficient transmission and storage. [12,16]. So the non-recursive method is more suitable for generating shares by considering a bit string of length bits as an n-variable Boolean function.

3.2. Kullback-Leibler divergence

In information theory, Kullback–Leibler (KL) divergence, or simply the KL divergence is used extensively to measure the difference between two probability distributions over the same variable 'x' [37–39]. The KL divergence, which is closely related to the relative entropy, information divergence, or information for discrimination, is a non-symmetric measure of the difference between two probability distributions. This measure also finds its use in application for security measure of the secret images. Let $p(x)$ and $q(x)$ are two probability distributions of a discrete random variable x. The KL divergence (KLD) can be defined as

$$KLD = (p \mid\mid q) = \sum_{x \in X} p_i\ log_2\ \frac{p_i}{q_i} \tag{4}$$

where, $p(x) > 0$ and $q(x) > 0$ for any x in X. The KL divergence measures the expected number of extra bits required to code samples from p(x) when using a code based on q(x), rather than using a code based on p(x). In SIS, it may be treated as a security measure between the original secret image and the reconstructed one as a measure of the number of extra bits required to generate the original secret $p(x)$ from the partial knowledge of $q(x)$. The larger the value of KLD is, better is the security.

With the brief introduction on recursive and non-recursive methods of Boolean classification and KLD, the next section presents the proposed SIS scheme.

4. The proposed method

This section describes the proposed hierarchical SIS scheme. A non-recursive affine Boolean function is used to generate share images. The access structure of the proposed method is shown in Fig. 1. The secret image 'SI' is partitioned into 'N' (2^i) share images through 'i' levels. The priority threshold condition is set as 's'. The value 's' contains (2^{i-1}) shares and are chosen as the essential shares based on their importance during the reconstruction operation. Rest of the shares are considered as non-essential shares. The relationship between 's','N' and 'i' are established below:

- i is an integer value greater than 1
- $N = 2^i$
- $s = 2^{i-1}$

The scheme can broadly be classified into two main procedures: share images generation and recovery of the secret image.

4.1. Share images generation procedure

This method generates 'N' number of share images from the secret image, 'SI' of size $R \times C$ in 'i' levels. The entire procedure of share generation is outlined in Algorithm 1. For each level the different steps are as follows:

Step 1 : *An n-variable affine Boolean function generation*

In case of n-variable, the bit positions which are fixed with respect to the affine functions of the corresponding class, are generated using a function as follows:

$$F(n) = P_n - 2^k,\quad where,\quad P_n = 2^n + 1\quad and\quad k = 0, 1, 2, \ldots, n \tag{5}$$

The present study uses 4-variable affine Boolean function to generate share images.

Step 2 : *Compute fixed bit positions for each class*

The fixed bit positions are used to provide the information regarding the non-linear Boolean functions and the affine function.

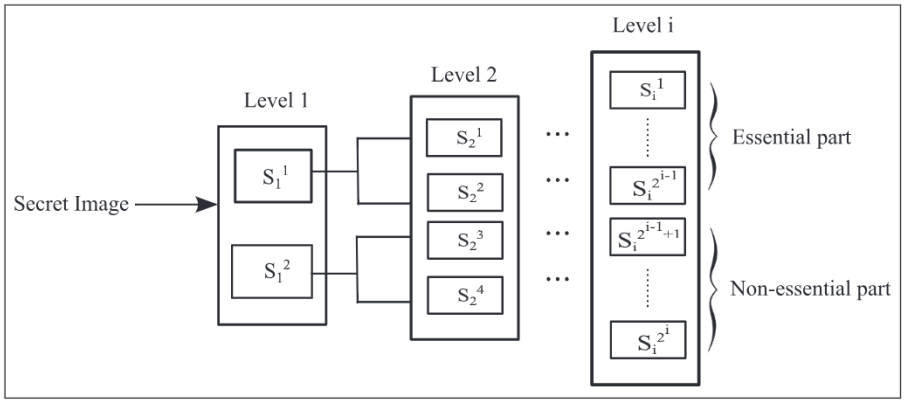

Fig. 1. Iterative scheme of share generation.

Algorithm 1 Share images generation procedure.

Input: Secret Image S of size $R \times C$ and the values *s, N, i.*
Output: Shadow images $Sh_i, 1 \le i \le N$

Compute the leader of each class (All 4-variable affine Boolean functions)
Compute the corresponding fixed bit positions of class
$p = 1$
Repeat until $p! = l$ /* l is the level
for $i = 1$ to 2^k **do**
    $sh_i = PPSIS_{cls}(S)$
    $sh_{i+1} = PPSIS_{sub-cls}(S)$
end for

$PPSIS_{cls}(S)$ /* **Procedure for generating class shares**

Repeat until $S[i,k] \in I$, where $S[i,k]$ as a 4-variable Boolean function.
If fixed positions of an affine function l and S are identical, then set sh_{cls} = index of the affine function l.

$PPSIS_{sub-cls}(S)$ /* **Procedure for generating sub-class shares**

Repeat until $S[i,k] \in I$, where $S[i,k]$ as a 4-variable Boolean function.
If fixed positions of an affine function l and S are identical, then set sh_{cls} = index of the affine function l.

The process to calculate the fixed bit positions B_{fix} for each class of n-variable is written below.

$X = 2^n$
for $i = 0$ to n **do**
    $B_{fix}[i] = X$
    $X = B_{fix}[i] - 2^i$
end for

Step 3 : *Secret image partition*

Any of the two cases may be considered at this stage based on the type of the secret image.

Case 1: For 8-bit/pixel secret image - The secret image is divided into non-overlapping blocks of pixels of size 2 × 1. Each pixel is converted into 8-bits/pixel to form a 16-bit binary stream.

Case 2 : For 1-bit/pixel secret image - The secret image is divided into non-overlapping blocks of pixels of size 16 × 1.

Step 4 : *Shares formation*

Let S' be the 2^n (n = 4) bit length binary bit stream and 'f' be an affine Boolean function of n-variable. Shares S'_1 and S'_2 are generated from S' using the steps written below.

if $S'[B_{fix}] == f[B_{fix}]$ **then**
    $S'_1 = f_{index}$
    S'_2 =Remaining 11-variable bit positions of S'
end if

4.2. Secret image recovery procedure

This scheme maintains a hierarchical structure in share generation procedure. During reconstruction/recovery of the secret image the same structure needs to be followed. It is already mentioned that the secret image can be reconstructed with a certain recognizability using the full contribution of essential shares. On the other hand, contribution of non-essential shares progressively increases the quality of the decoded secret image. The recovery procedure is demonstrated in Algorithm 2 and is discussed as follows:

Algorithm 2 Secret image reconstruction procedure.

Input: 'k' ($s \le k \le n$) share images including s essential shares ($I_1, I_2, \ldots, I_s$) and remaining non-essential shares ($I_{s+1}, I_{s+2}, \ldots, I_k$)
Output: The reconstructed image I'

$I_1 = O_1, I_2 = O_2, I_3 = O_3, \ldots, I_{k_1} = O_{k_1}$ /*O_1 to O_{k_1} are essential shadows
$I_{s+1} = O_{s+1}, I_{s+2} = O_{s+2}, I_{s+3} = O_{s+3}, \ldots, I_k = O_k$ are non-essential shadows
Let $j = 1$, $l = k$, is the number of essential and non-essential shares
Repeat until $l! = 1$
for $i = 1$ to l **do**
    Repeat until $p[a,b] \in I_i$, where $p[a,b]$ as a five bit index of the 4-variable affine Boolean function f_{affine}
    Repeat until $q[a,b] \in I_{i+1}$, where $q[a,b]$ as an eleven bit variable position of the 4-variable affine Boolean function f_{affine}
    $I_j = f_{affine}(q[a,b])$ /* put the eleven bit in the corresponding variable positions of the affine function
    $j+ = 1$
end for

Step 1 : *Generation of affine Boolean function*

An n-variable affine Boolean function is generated in this step. This process is same as discussed in the share image generation procedure.

Step 2 : *Computation of fixed bit positions of each class*

The fixed bit positions of each class need to be computed using the same process discussed in Step 1 of the share generation procedure.

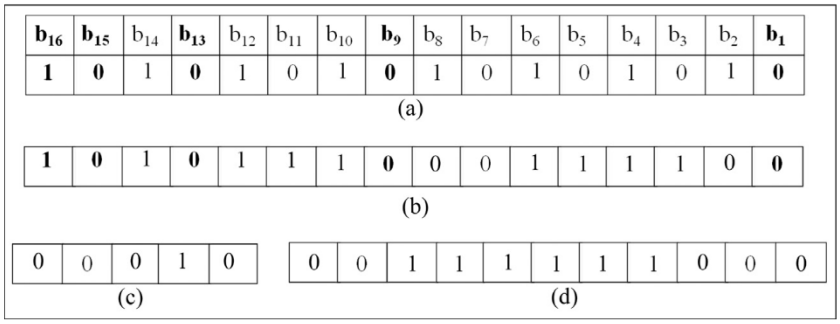

Fig. 2. Share generation (a) 4-variable affine function, fixed bit positions are represented by bold; (b)16 bit binary stream of input image; (c) Index of affine function as 1st share; (d) 11-variable bit position from 16 bit binary string as 2nd share.

Step 3 : *Data recovery from secret bit stream*

At each level, from two consecutive shares, the corresponding data recovery of the secret bit stream is done. The process of reconstruction is discussed below through an example.

1: Select 'n+1' (5) adjacent bits from $S_1^{'}$ as the index of the n-variable affine Boolean function f_{affine}
2: Compute the leader 'l' (2^4 bits length) as an n-variable affine Boolean function from the five consecutive bits of $S_1^{'}$
3: Select '$2^n - (n+1)$' (11) adjacent bits from the image $S_2^{'}$. The bits are stored in the corresponding variable bit positions of the affine function f_{affine}.
4: Reconstruct bit stream $S^{''} = f_{affine}$

Example. A class of Boolean functions can be achieved through a set of variable bit positions with respect to an affine function. For each class of n-variables, the length of a Boolean function is 2^n, among which 'n + 1' bits are fixed and the remaining $2^n - (n+1)$ bits are changing with respect to the affine Boolean function of that class [34,35]. It is considered as a way of generating two shares having leader in one share and the members in other share provided that there is a way for retrieving the original bit strings from the leader and its member.

This scheme considers 16 (2^4) adjacent bits of the secret image as a 4-variable Boolean function. In case of 4-variables, the bit positions which are fixed with respect to the affine functions of the corresponding classes are represented as '5' bit pattern. Let $S = 1000011011110000$ is the '16' consecutive bits of the secret image. The fixed bit positions are $b_{16} = 1$, $b_{15} = 0$, $b_{13} = 0$, $b_9 = 0$, $b_1 = 0$. A class having $f_{affine} = 1010101010101010$ is chosen as the leader of the class as the fixed bit positions of this class and S are same. So the string S belongs to the class having the above affine function. The share $S_1 = 00010$ is the index value of the corresponding affine function and the share $S_2 = 00111111000$ is the rest of the 11-bits from the string S. The share generation procedure is illustrated diagrammatically in Fig. 2.

During reconstruction, this method considers 5 adjacent bits from the share S_1 as the index of the affine Boolean function. As per the index, the corresponding affine function is selected. The fixed bits are placed accordingly to reconstruct the fixed bit positions (5 bits) of the secret bit stream S'. The other 11 adjacent bits are selected from share S_2. These bit values are placed in the corresponding variable bit positions to reconstruct S'.

5. Performance evaluation and discussion

This section presents performance results of the proposed scheme in terms of perceptual quality of the reconstructed image and robustness against various common and deliberate signal processing operations including random gain operation. Performance of the proposed method is studied for a large number of binary and gray scale secret images [40] (over 100 images). Some of them are Lena, Pepper, Cameraman, Opera, F161, Baboon, Fishing boat, Zelda, Barbara, Zebra, Logo etc. The test images are of different sizes. Few of them are shown in Fig. 3. Fig. 3(a)–(c) are the binary images and Fig. 3(d)–(g) are the gray scale images with intensity values of 8 bits/pixel. The present study uses Peak-Signal-to-Noise-Ratio (PSNR) and Structural SIMilarity index (SSIM) [41] as distortion measure to quantify the visual quality of the reconstructed images with respect to the original gray scale secret images under inspection. On the other hand, to quantify the quality of the binary secret images, normalized cross-correlation (NCC) values are used as a distortion measure between the original secret image and the reconstructed secret image. Mathematical form of NCC is written as follows:

$$NCC = \frac{\sum_{i=1}^{L} b_i b_i'}{\sum_{i=1}^{L} b_i^2} \tag{6}$$

where, b_i and b_i' indicate the ith bit for the original and the decoded secret images, respectively and L is the length of the original/the decoded secret images.

The range of the NCC value is between 0 and 1. When the NCC value is close to 1, the degree of similarity between the two images is high. In contrast, when the NCC value is close to 0, the degree of similarity between the images is quite low.

5.1. Performance evaluation

Performance of the proposed scheme is evaluated in terms of the following attributes:

- Reduced shadow size
- Progressive quality access

In the following, few studies are reported to demonstrate the efficacy of the proposed scheme.

Case 1: *Results for binary secret image*

Fig. 4 shows the experimental results of the proposed scheme for $i = 3$, $N = 2^3 = 8$, and $s = N/2 = 4$ for a binary secret image 'Zebra' as shown in Fig. 3(b). It is already mentioned that this scheme uses a 4-variable affine Boolean function to generate the share images. Hence the size of the share images are 5/16 th or 11/16 th times smaller than the corresponding secret image. Fig. 4(a)–(h) show the eight share images generated in three levels. First four share images are essential shares which are distributed to the relatively high priority participants as essential group and the rest are distributed to the less important participants as non-essential group. It is shown (in Fig. 4(i)) that a complete decoding of the secret image is possible with the involvement of

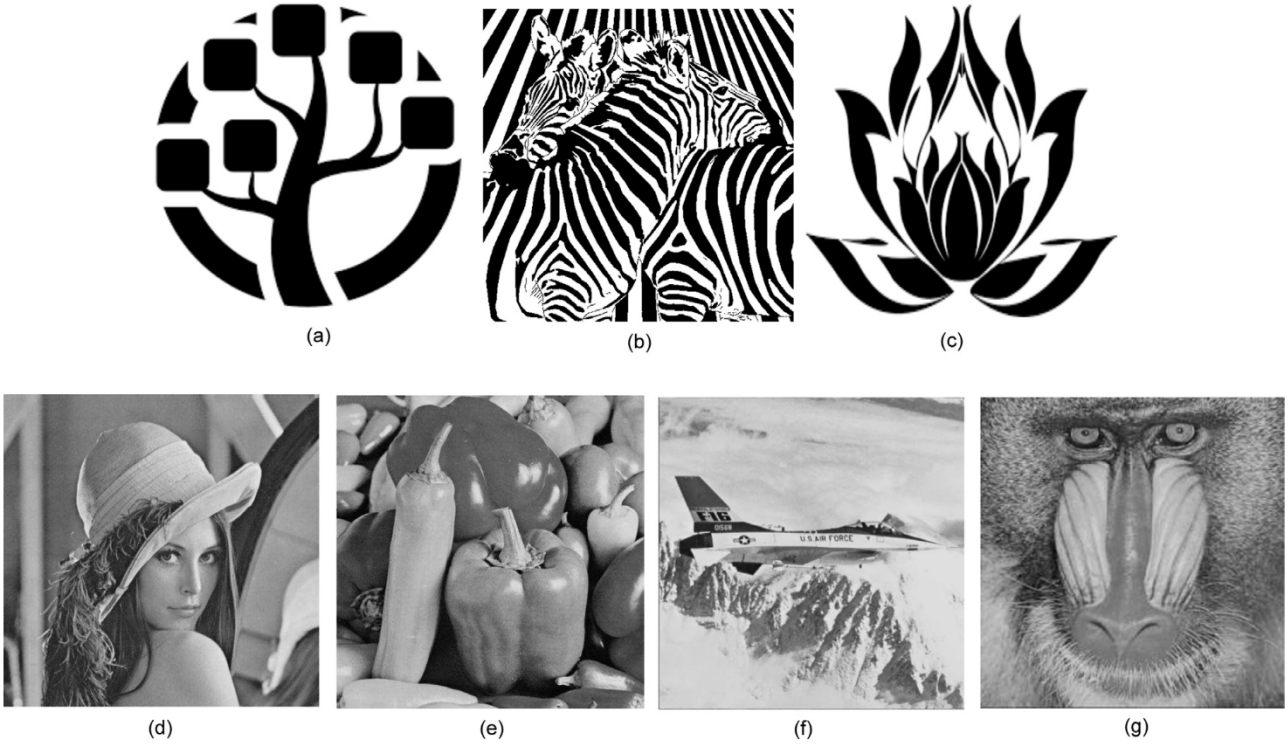

Fig. 3. Test images: (a)–(c) binary images; (d)–(g) gray scale images.

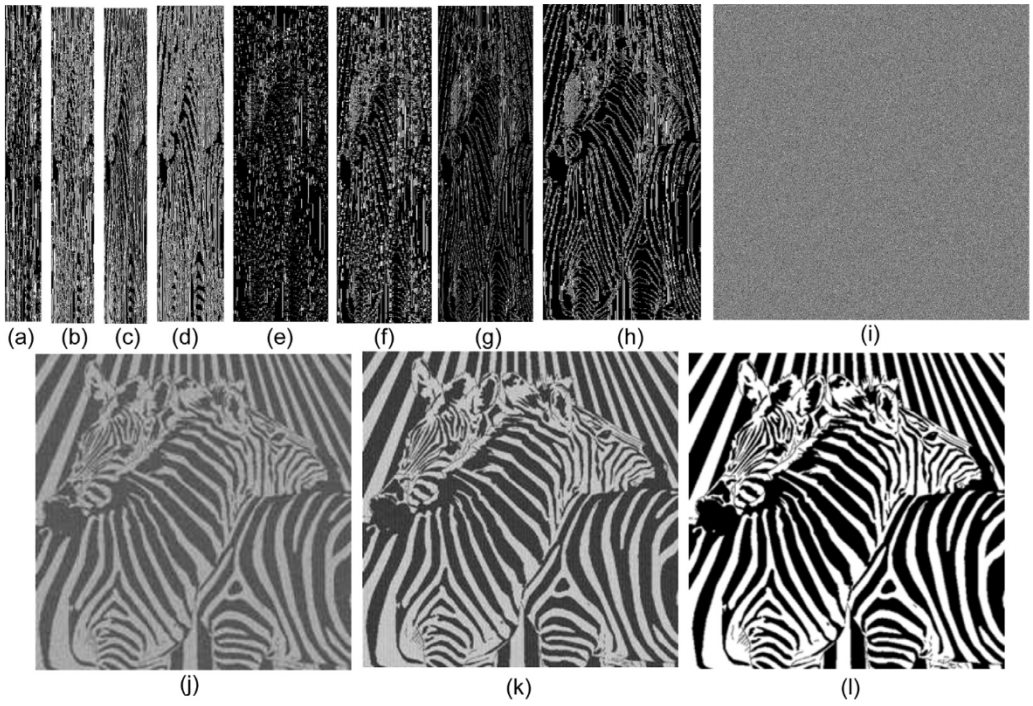

Fig. 4. Share images and the reconstructed images for binary secret image, Zebra : (a)–(h) share images; (i) reconstructed secret image from all the essential and the non-essential shares (NCC = 1) (j) reconstructed secret image with all the non-essential shares and the random values for the essential shares (NCC = 0.00053); (k) reconstructed secret image with all the essential shares and the random values for the non-essential shares (NCC = 0.63); (l) reconstructed secret image with all the essential shares and the two non-essential shares (NCC = 0.75).

required number of the essential and the non-essential shares. However, here it is also studied the decoding reliability when partial knowledge for the essential or non-essential shares are used. It is expected that the remaining parts (essential or non-essential shares) to be filled, in one way (they may be developed many other ways), by some random values to reconstruct the secret image. Fig. 4(j) shows the decoded secret image with the full contribution of the non-essential parts and random values for the essential part. On the other hand, Fig. 4(k) shows the decoded secret image with the full participation of the essential part and the random values as the non-essential part. From these two figures, Fig. 4(i) and (j), it is clear that the essential components (shares)

Table 1
Correlation values of a (4, 8) scheme for a binary secret image.

No. of essential shares	No. of non-essential shares	NCC
0	4	0.00053
1	4	0.0033
2	4	0.0289
3	4	0.0536
4	0	0.63
4	1	0.69
4	2	0.75
4	3	0.82
4	4	1

Table 2
SSIM and PSNR values of a (4, 8) scheme for a gray scale secret image.

No. of essential shares	No. of non-essential shares	SSIM	PSNR
0	4	0.000126	9.87
1	4	0.0011	15.54
2	4	0.0053	28.13
3	4	0.0587	20.56
4	0	0.59	31.56
4	1	0.65	35.87
4	2	0.76	39.28
4	3	0.84	45.01
4	4	1	Infinity

are good enough to reconstruct the secret image to maintain a certain recognizable quality. Fig. 4(l) shows the decoded secret image from all the essential shares and any two non-essential shares (considering remaining two shares as random). It is clear that the contribution of the essential shares are mandatory for faithful reconstruction of the secret image. On the other hand, progressive contribution of the non-essential shares enhances the quality of the reconstructed image.

The NCC values for the reconstructed images shown in Fig. 4(i)–(l) are 1, 0.00053, 0.63, 0.75, respectively. Numerical values in Table 1 demonstrate that with the involvement of the more number of the non-essential shares (with essential shares), the quality of the reconstructed image increases progressively.

Case 2: *Results for gray scale (8 bits/pixel) secret image*

Performance is also studied for large number of gray scale secret images. One such image F161 of size 512 × 512 with intensity value 8 bits/pixel is shown in Fig. 3(f). It is divided into 8 shares ($i = 3$) as shown in Fig. 5(a)–(h). The decoded secret image with the contribution of all the non-essential shares and the random values for the essential shares is shown in Fig. 5(i). On the other hand, the decoded secret image with the contribution of all the essential shares and the random values for the non-essential shares is shown in Fig. 5(j). Fig. 5(k) shows the reconstructed secret image with the contribution of all the essential and the non-essential shares. The PSNR and SSIM values achieved in these three figures (Fig. 5(i)–(k)) are (9.87 dB, 0.000126), (31.56 dB, 0.59), (Infinity, 1), receptively.

Numerical values in Table 2 demonstrate the secret image and the decoded image quality (PSNR and SSIM values) with the contribution of different number of the essential and the non-essential shares involved in the reconstruction operation. The results also support our earlier findings that

(i) the secret image can be reconstructed to a certain recognizable quality with the contribution of the essential shares only.
(ii) the contributions from the relatively more number of non-essential shares progressively increases the quality of the reconstructed image.

5.2. Robustness results

This section presents the results of the reconstructed/decoded secret images after applying various operations on the shares. Performance study is done over a large numbers of images. Numerical values shown in Fig. 6 and the other graphical plots are obtained by taking average on the samples of 100 such secret images.

Fig. 6 presents a graphical representation of the quality of the reconstructed secret image indicated by NCC values versus different percentage of bit error rate (BER) applied on each of the share image using a (4,4) scheme (considering i = 2, N = 4 and s = 2). The word BER here implies the error in the share images when transmitted through the noisy channels or any manipulation like flipping of the bits for binary shares done by some user. This case considers the first two shares as essential share images (Share 1 and share 2) and the other two shares as non-essential share images. The graph shows the reconstructed image quality (indicated as NCC value) with the contribution of all the shares. Each plot in Fig. 6 indicates that the flipping is done on the bit pattern of the respective share only, while the other shares remain unchanged. The reconstruction is done using all the shares. After applying error flipping operation on Share 3 or Share 4, the reconstructed image quality looks quite good. However, after applying the same operation on Share 1 or Share 2, the reconstructed images are affected more and consequent degradations on the quality of the reconstructed images are seen. Simulation results show that any manipulation (deliberate or unintentional) on essential shares causes more degradation on the decoded secret image than the same degree of manipulation on the non-essential shares.

Robustness performance of the proposed scheme is studied against various signal processing operations or due to transmission over noisy channels. The proposed method is capable to withstand a large variations in the additive noise intensity. Even at high variance, the reconstructed image maintains its recognizability. Fig. 7(a)–(d) show the reconstructed secret images after applying AWGN on all the share images of a (4,4) scheme (considering i = 2, N = 4 and s = 2) on binary secret image, 'Zebra' with different variance values. Fig. 8 graphically represents that the reconstructed image quality decreases with the increase in variance of AWGN. As expected, increase in noise variance i.e. decrease in SNR value shows the degradation in reconstruction (robustness) performance. Furthermore, involvement of the less number of shares i.e. a (2,4) or a (3,4) scheme offer lower visual quality of the decoded images than a (4,4) scheme. Fig. 9 graphically represents the decoded image after AWGN contamination on individual share image of a (4,4) scheme. Share 1 and Share 2 are the essential components, other two are the non-essential components. As expected the effect of AWGN on essential components degrade the quality of the reconstructed image more than the non-essential components.

Fig. 10(a)–(d) represent the decoded images after AWGN operation with zero mean and a variance value of 0.1 on the individual share image of a (4,4) scheme on binary secret image (Zebra). NCC values for the reconstructed secret images shown in Fig. 10(a)–(d) are 0.65, 0.69, 0.81, 0.86, respectively. On the other hand, Fig. 10(e)–(h) represent the reconstructed images after AWGN operation with a variance value of 0.05 on the individual share image of a (4,4) scheme on gray scale (8 bits/pixel) secret image (Lena). The decoded secret image quality is effected more when AWGN of a particular variance is applied on the non-essential shares. PSNR values for the reconstructed images of Fig. 10(e)–(h) are 26.31 dB, 28.8 dB, 31.47 dB and 34.27 dB, respectively.

Performance of the proposed scheme is also studied against random scaling gain operation. It is very much relevant for multimedia data transmission over radio mobile channel. To study the similar operation, the share images are transmitted using multi-carrier code division multiple access (MC-CDMA) [42] over

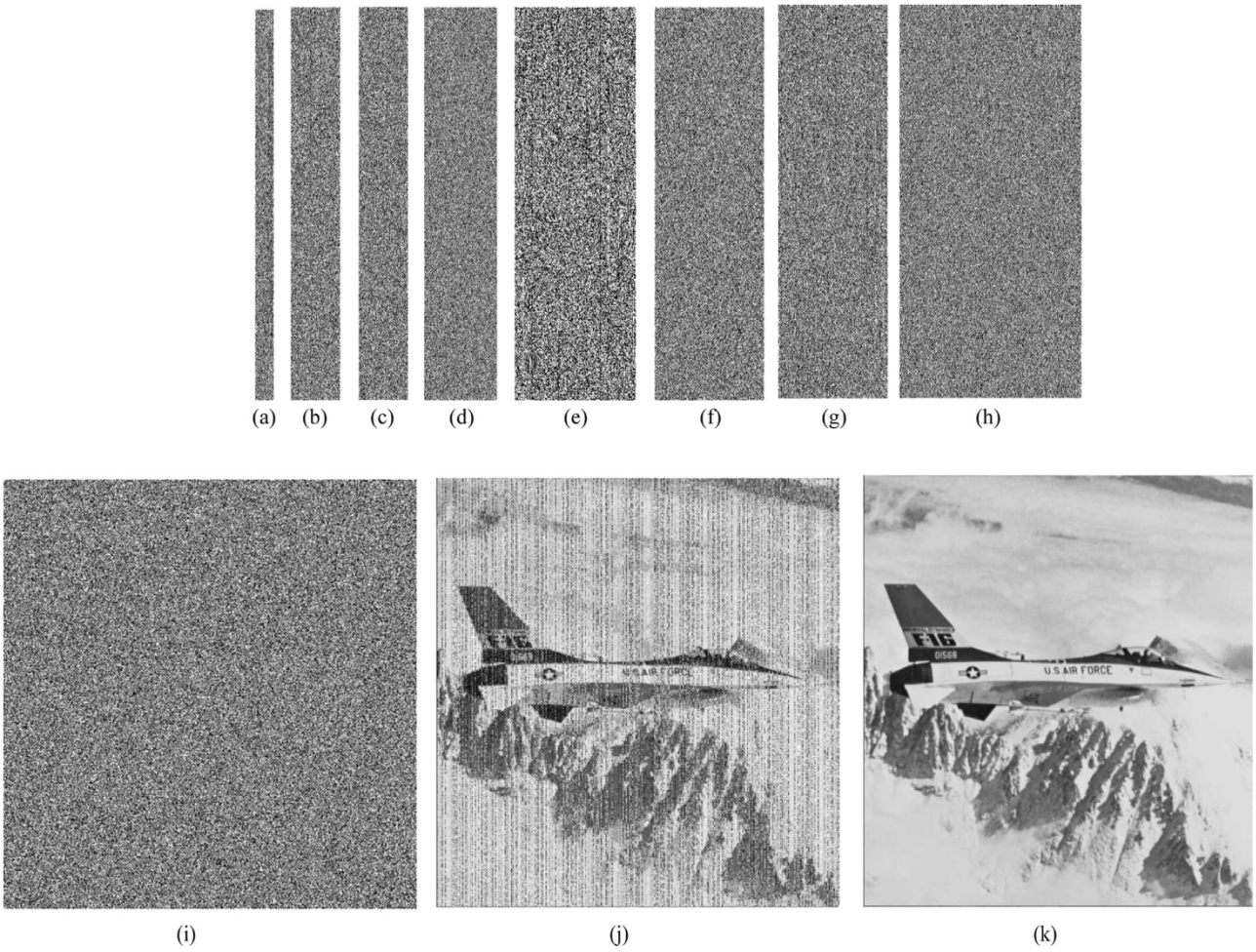

Fig. 5. Share images and the decoded images for the gray scale secret image, F161 : (a)–(h) share images; (i) reconstructed secret image with all the non-essential shares and the random values for the essential shares (PSNR = 9.87 dB); (j) reconstructed secret image using the essential components and the random values for the non-essential components (PSNR = 31.56 dB); (k) reconstructed secret image from all the shares (PSNR = Infinity).

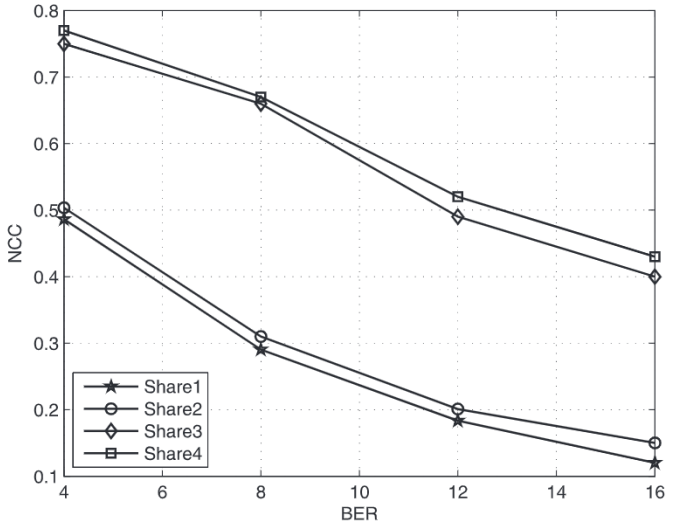

Fig. 6. Reconstructed secret image quality vs bit error rate applied on individual share image.

Rayleigh fading channel at different SNR values. This is analogous to the effect of independent slow fading when shares are transmitted through radio mobile channel. Rayleigh fading is considered as it is the widely used frequency selective fading model. The small SNR value represents that the channel is under deep fade, while the high value of SNR represents the reverse. Fig. 11(a)–(c) represent the reconstructed binary secret images of a (4,4) scheme at different SNR values. NCC values for the reconstructed secret images shown in Fig. 11(a)–(c) are 0.84, 0.68, 0.36, respectively. Fig. 11(d)–(f) show the same for gray scale (8 bits/pixel) secret image 'Lena'. It is observed that the proposed scheme is capable to retain the recognizability of the secret image, even when the share images undergo the frequency selective fading-like random gain operation. PSNR values for the reconstructed images shown in Fig. 11(d)–(f) are 31.7 dB, 28.36 dB and 24.52 dB, respectively.

5.3. Performance comparisons

A summary of comparative study of the proposed scheme with the other recently reported SIS schemes are listed in Table 3. The comparative study is based on the following properties: 'Decryption method', 'Reduced shadow size', 'Essential threshold', 'Progressive quality access', 'Secret image recognizability without non-essential part'. Performance results include a wide variation in the working principles for the techniques used with the involvement of different parameters. Methods also include different diverse issues and in true sense does not represent a comparison. However, the relative merits and the demerits of different works are shown to highlight the status of the related

Table 3
Performance comparison study with the existing works.

Schemes	Decryption method	Reduced shadow size	Essential threshold	Progressive quality access	Secret image recognizability without non-essential part
[5]	Lagrange interpolation	Yes	No	Yes	–
[10,16]	Lagrange interpolation	Yes	Yes	No	Not possible
[30]	Birkhoff interpolation	Yes	Yes	No	No
[1]	Stacking (OR)	No	No	Yes	–
Proposed	Boolean	Yes	Yes	Yes	Possible

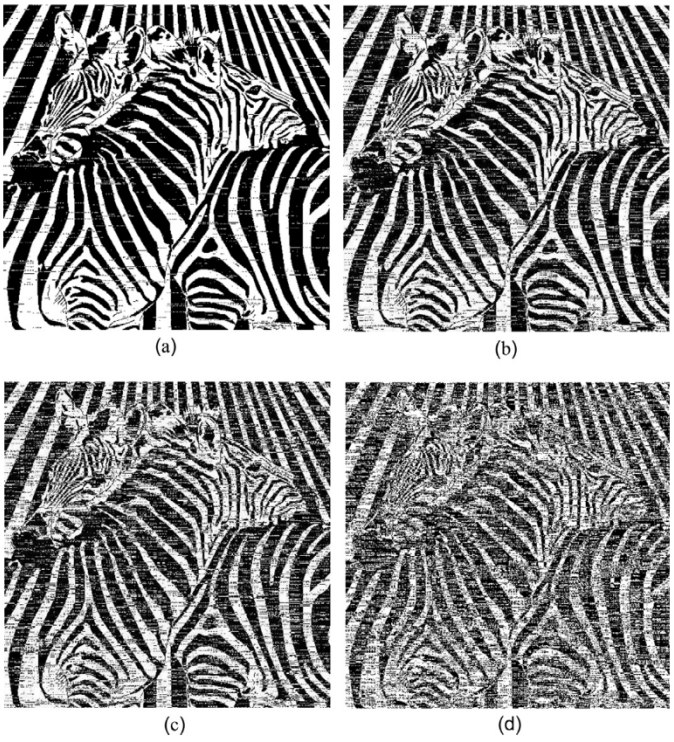

Fig. 7. Reconstructed images after AWGN operation: (a) with variance 0.01 (NCC = 0.82); (b) with variance 0.05 (NCC = 0.65); (c) with variance 0.07 (NCC = 0.45); (d) with variance 0.1 (NCC = 0.32).

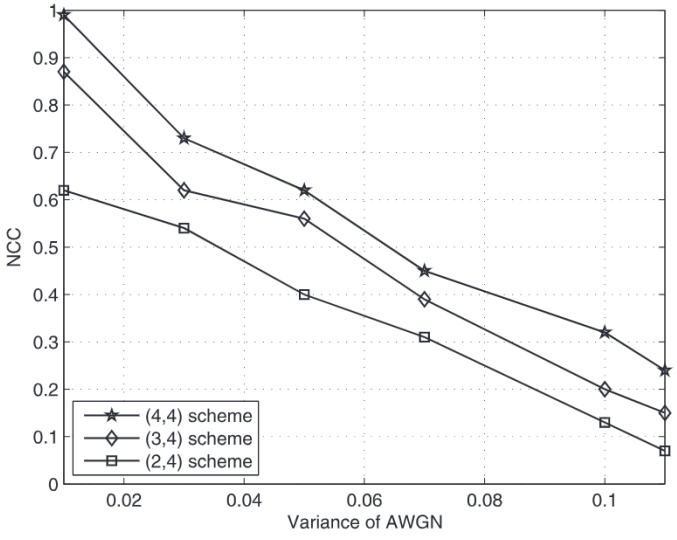

Fig. 8. NCC vs variance of AWGN.

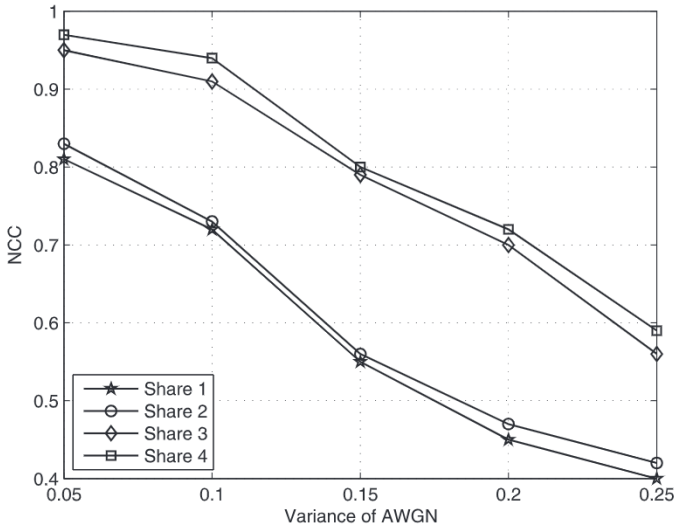

Fig. 9. Reconstructed secret quality (NCC value) vs variance of AWGN.

recent SIS schemes. The column 'Decryption method' represents the process of secret image reconstruction from the respective set of share images. It is needless to mention that reduced size shares are always preferred in SIS schemes. So the parameter 'Flexible shadow size' is considered in the third column of Table 3. The next column 'Essential threshold' is used here to show the importance of one set of participants (essential) in the decoding process. The next column 'Progressive quality access' indicates the quality of the reconstructed secret image with the involvement of more amount of data (shares) in the reconstruction process. The last field (column) compares the requirement of non-essential shares during the reconstruction operation.

Table 3 highlights some merits of the proposed scheme over some recent related schemes [1,5,10,16,30]. The schemes reported in [1,5] do not offer any hierarchical access structure in secret image reconstruction process. All the participants (share holders) play an identical role in secret reconstruction. Contrarily, the SIS schemes reported in [10,16,30] maintain an access structure to decode the secret image from the respective set of shares. The image secret reconstruction without the involvement of non-essential shares and progressive quality access of the decoded secret images are not possible in these schemes.

Progressive quality access property of the proposed scheme is also studied against two schemes reported in [1,5]. The scheme reported in [5] is studied here to have a performance comparison for gray scale images. The graphical representation of the same is shown in Fig. 12(a). On the other hand, the scheme reported in [1] is used for similar performance comparison for binary secret images. It is shown in Fig. 12(b). Fig. 12(a) and (b) show the visual quality (SSIM/NCC values) for the reconstructed secret images with respect to progressive involvement of the respective share images. The average reconstructed secret image quality values (SSIM) for different gray scale secret images are 0.65, 0.8, 1, respectively with progressive involvement of share images (50%, 75%, 100%). On the

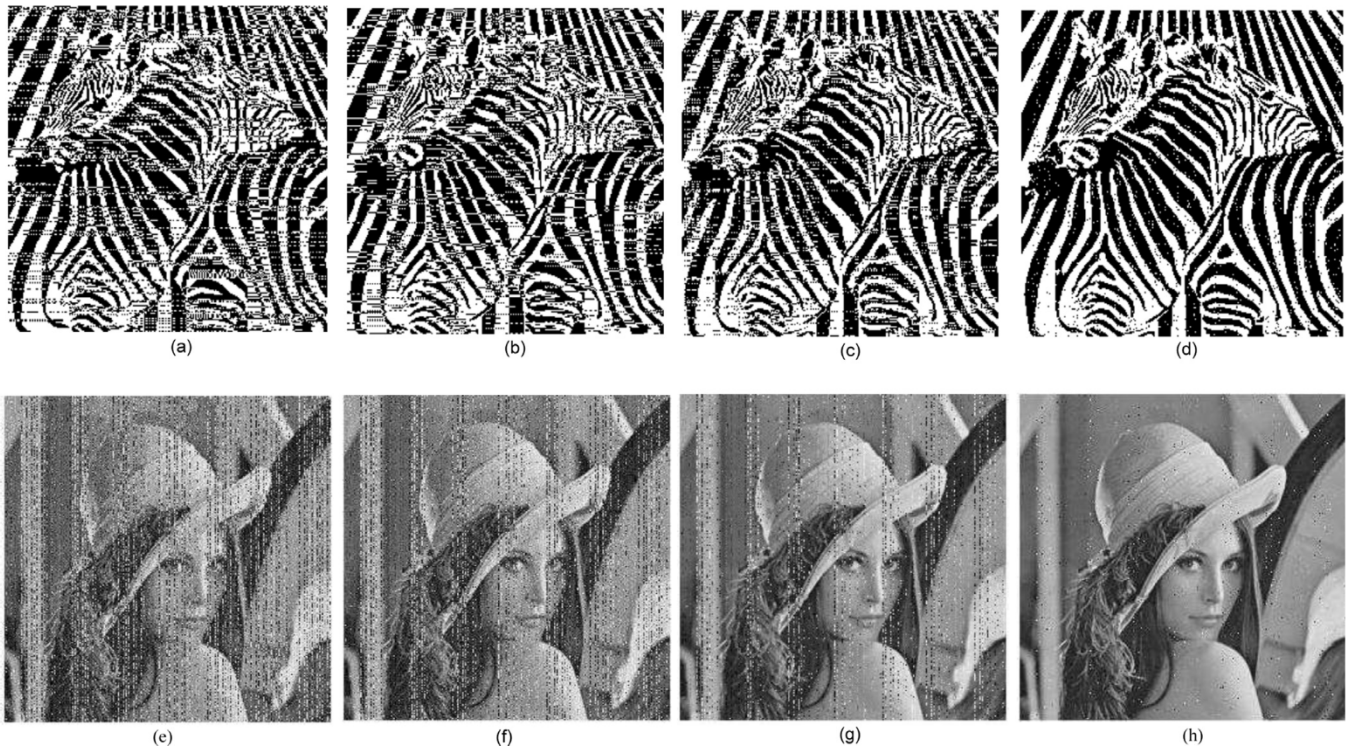

Fig. 10. Reconstructed images after AWGN operation: (a)–(d) for binary secret image (with variance 0.1): (a) on Share 1 (NCC = 0.65); (b) on Share 2 (NCC = 0.67); (c) on Share 3 (NCC = 0.84); (d) on Share 4 (NCC = 0.86) (e)–(h) for gray scale (8 bits/pixel) secret image (with variance 0.05): (a) on Share 1 (PSNR = 27.31 dB); (b) on Share 2 (PSNR = 27.8 dB); (c) on Share 3 (PSNR = 34.05 dB); (d) on Share 4 (PSNR = 34.27 dB).

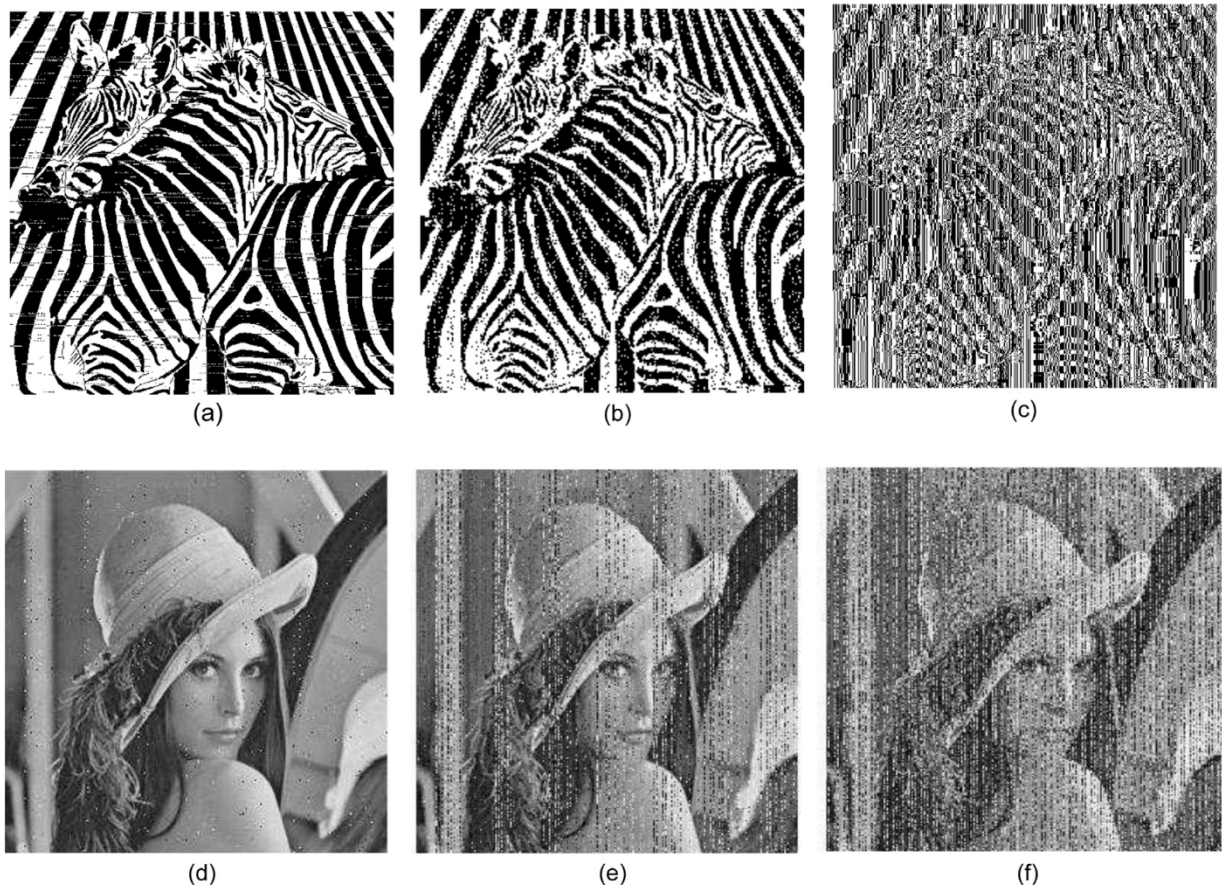

Fig. 11. Reconstructed image after random gain Rayleigh operation: (a)–(c) for binary secret image (a) low (NCC = 0.84); (b) mild (NCC = 0.68); (c) sever (NCC = 0.36) (d)–(f) for gray scale (8 bits/pixel) secret image (a) low (PSNR = 31.7 dB); (b) mild (PSNR = 28.36 dB); (c) sever (PSNR = 24.52 dB).

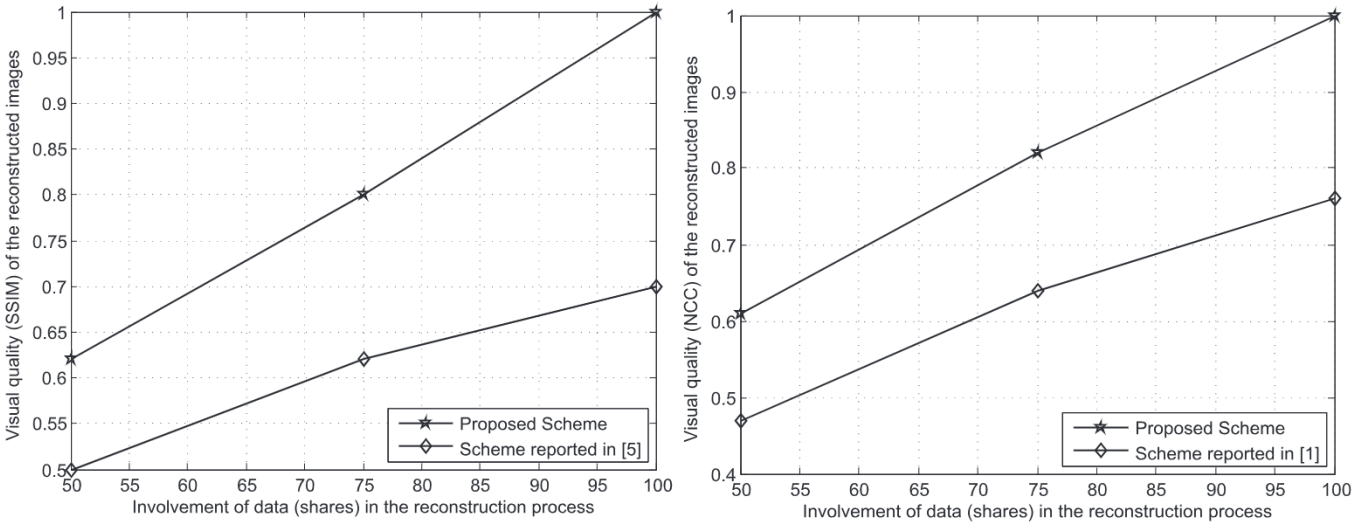

Fig. 12. Progressive involvement of data (shares) in the reconstruction process versus reconstructed secret image quality (a) for gray scale secret images (8 bits/pixel) (b) for binary secret images.

other hand, with the same requirement, the SSIM values for different secret images are 0.5, 0.62, 0.7, respectively using the scheme reported in [5]. The NCC values for binary secret images achieved using the proposed scheme and the scheme reported in [1] are (0.6, 0.82, 1) and (0.47, 0.64, 0.76), respectively. In brief, the major advantages of the proposed scheme may be highlighted as follows: (i) reduced size share images are generated, (ii) an essential threshold is maintained and the secret image can be reconstructed to a certain visual recognizability without the involvement of the non-essential shares, (iii) involvement of the non-essential shares progressively enhances the quality of the decoded secret image.

5.4. Security analysis

The security of the proposed scheme can be shown from two different perspectives. Each one is discussed in brief.

(i) An n-variable Boolean function 'f' is a mapping from the set of all possible n-bit strings $(0, 1)^n$ into 0 or 1. The number of different n-variable Boolean functions is 2^{2^n}. It is already mentioned that a Boolean function with algebraic expression, where the degree is at most one is called an affine Boolean function. The general form for n-variable affine function is written in Eq. (1). It is already mentioned that affine Boolean functions are either linear Boolean functions or their complements. In Boolean algebra, a linear function is a function f for which $f(X \oplus Y) = f(X) \oplus f(Y)$, where X and Y are any two vectors from the domain. To identify the linearity property of an n-variable Boolean function, the worst case time complexity is $O(n.2^n_{C_2}.2^{2^n})$ where 'n' is the time taken for X-OR operation of the binary string having the length 'n' for n-variable, $2^n_{C_2}$ is the number of pairs taken from the domain and 2^{2^n} is the total number of Boolean function.

Illustration: Table 4 shows two 4-variable Boolean functions as f_{43690} and f_{43691}. The linear property of the function, $f_{43690}(1010101010101010_2)$ can be determined by considering any two vectors from the domain. For example, $f(0000 \oplus 0001) = f(0001) = 1$ and $f(0000) \oplus f(0001) = 0 \oplus 1 = 1$. So the function, f_{43690} is a linear function as $f(0000 \oplus 0001) = f(0000) \oplus f(0001)$. Similarly, the linear properties can be verified by considering any two vectors from the domain. For any 4-variable Boolean function the same is possible in 16_{C_2} possible ways (or for one function of n-variable it is $2^n_{C_n}$). On the other hand, the linear properties of the function $f_{43691}(1010101010101011_2)$ can be determined by considering any two vectors from the domain, like $f(0000 \oplus 0001) = f(0001) = 1$ and $f(0000) \oplus f(0001) = 1 \oplus 1 = 0$. So the function, f_{43691} is not a linear function as $f(0000 \oplus 0001) \neq f(0000) \oplus f(0001)$.

Table 4
Truth table of 4-variable Boolean function.

A	B	C	D	f_{43690}	f_{43691}
0	0	0	0	0	1
0	0	0	1	1	1
0	0	1	0	0	0
0	0	1	1	1	1
0	1	0	0	0	0
0	1	0	1	1	1
0	1	1	0	0	0
0	1	1	1	1	1
1	0	0	0	0	0
1	0	0	1	1	1
1	0	1	0	0	0
1	0	1	1	1	1
1	1	0	0	0	0
1	1	0	1	1	1
1	1	1	0	0	0
1	1	1	1	1	1

Table 5
Reconstructed secret image quality (statistical distance and visual quality values).

Parameter	Statistical distance (KL divergence)	Visual quality (PSNR)
Random values of essential components (share images)	100.3	9.56

(ii) It is worth to mention that the presence of the essential components (shares) are sufficient to decode the secret image. Contrarily, non-essential components are not good enough to reconstruct the secret image. Fig. 13(a) shows the reconstructed secret image, 'Lena' with the involvement of all the non-essential shares and the random values for the essential shares (considering i = 2, N = 4 and s = 2). Fig. 13(b) shows the decoded secret image, 'F161' with the involvement of all the non-essential shares and 's − 1' essential shares (considering i = 3, N = 8 and s = 4). The results show that the full participation of all the essential shares are mandatory in the decoding process. Table 5 shows the average (taken over 100 images) KLD values (as statistical measure) and PSNR values (as visual quality measure) of the reconstructed secret

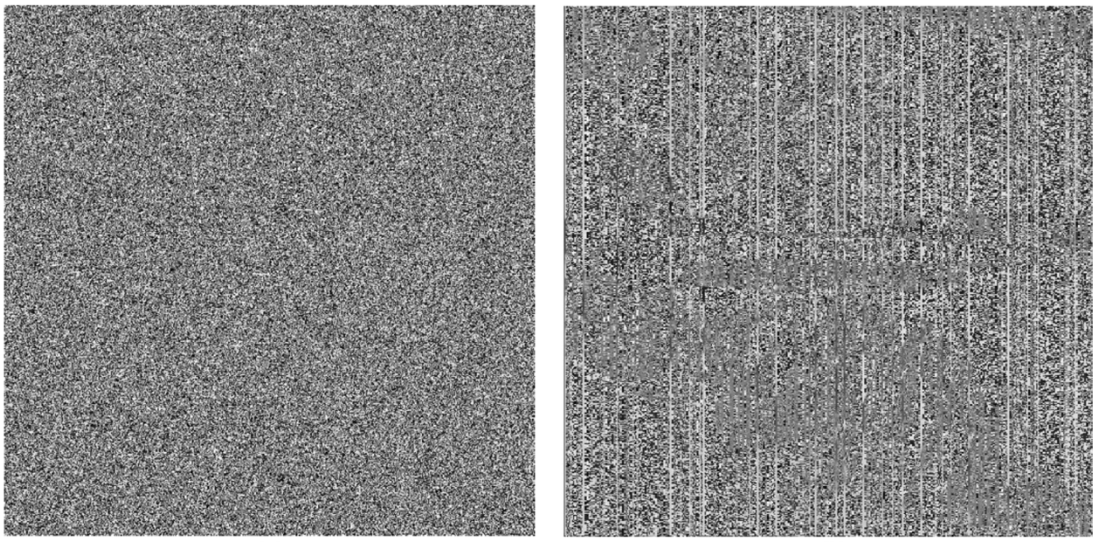

Fig. 13. (a) Reconstructed secret image, Lena with the involvement of two number of non-essential shares and random values of essential shares (PSNR 9.56 dB) (b) Reconstructed secret image, Airplane with the involvement of four number of non-essential shares, three essential shares (PSNR 16.12 dB).

images when the essential shares are filled with random values. High KLD values and low PSNR values prove that the quality of the reconstructed secret images are quite poor which in turn indicates the high security value for the proposed scheme.

6. Conclusions and scope of future work

This work proposes an affine Boolean function based essential threshold SIS scheme. An n-variable $(n = 4)$ affine Boolean function is used to generate the share images (2^i) in 'i' levels. This scheme maintains an essential threshold (2^{i-1}) to reconstruct the secret image to a certain degree of recognizability. On the other hand, involvement of the non-essential components progressively improves the quality of the reconstructed image. Improved performance on progressive quality access highlights the feasibility and effectiveness of the proposed scheme that includes robustness against some common signal processing operations. Affine Boolean function classification not only offers simple computation but also provides a significant reduction in share image sizes. Simulation results of a (4,4) (i = 2, N = 4 and s = 2) scheme considers two shares as the essential components and the rest two as the non-essential components. For binary secret images, the average reconstructed image qualities (NCC values) are 0.79 and 1, respectively with the involvement of only the essential components and both the essential and the non-essential components, respectively. On the other hand, for gray scale secret images (8 bits/pixel) the average reconstructed image quality (PSNR values) is 32.5 dB with the involvements of the essential components in the decoding process. The modification of this scheme as a general (k,n) SIS scheme may be considered as possible extension of the current work.

References

[1] Hou YC, Quan ZY, Tsai CF. A privilege-based visual secret sharing model. J Visual Commun Image Represent 2015;33:358–67.
[2] Ou D, Sun W. Reversible AMBTC-based secret sharing scheme with abilities of two decryptions. J Visual Commun Image Represent 2014;25(5):1222–39.
[3] Bhattacharjee T, Maity SP. An image-in-image communication scheme using secret sharing and m-ary spread spectrum watermarking. Microsyst Technol 2016:1–14. doi:10.1007/s00542-016-3104-z.
[4] Wei SC, Hou YC, Lu YC. A technique for sharing a digital image. Comput Stand Interfaces 2015;40:53–61.
[5] Liu L, Wang A, Chang CC, Li Z. A novel real-time and progressive secret image sharing with flexible shadows based on compressive sensing. Signal Process 2014;29(1):128–34.
[6] Yang CN, Chen CH, Cai SR. Enhanced boolean-based multi secret image sharing scheme. J Syst Software 2016;116:22–34.
[7] Jin J, hong Wu Z. A secret image sharing based on neighbourhood configurations of 2-d cellular automata. Opt Laser Technol 2012;44(3):538–48.
[8] Blakley G. Safeguarding cryptographic keys. In: Proceedings of the 1979 AFIPS national computer conference; 1979. p. 313–17.
[9] Shamir A. How to share a secret. Commun ACM 1979;22(11):612–13.
[10] Yang CN, Li P, Wu CC, Cai SR. Reducing shadow size in essential secret image sharing by conjunctive hierarchical approach. Signal Process 2015;31:1–9.
[11] Guo C, Chang CC, Qin C. A hierarchical threshold secret image sharing. Pattern Recognit Lett 2012;33(1):83–91.
[12] Thien CC, Lin JC. Secret image sharing. Comput Graphics 2002;26(5):665–70.
[13] Wang RZ, Su CH. Secret image sharing with smaller shadow images. Pattern Recognit Lett 2006;27(6):551–5.
[14] Lin YY, Wang RZ. Scalable secret image sharing with smaller shadow images. IEEE Signal Process Lett 2010;17(3):316–19.
[15] Yang CN, Chu YY. A general (k, n) scalable secret image sharing scheme with the smooth scalability.. J Syst Software 2011;84(10):1726–33.
[16] Li P, Yang CN, Wu CC, Kong Q, Ma Y. Essential secret image sharing scheme with different importance of shadows.. J Visual Commun Image Represent 2013;24(7):1106–14.
[17] Naor M, Shamir A. Visual cryptography. In: Advances in cryptology-EUROCRYPTO94, 950. Springer-Verlag; 1995. p. 1–12.
[18] Zhou Z, Arce G, Di Crescenzo G. Halftone visual cryptography. IEEE Trans Image Process 2006;15(8):2441–53.
[19] Wang Z, Arce G, Di Crescenzo G. Halftone visual cryptography via error diffusion. IEEE Trans Inf Forensics Secur 2009;4(3):383–96.
[20] Chen TH, Tsao KH. Threshold visual secret sharing by random grids. J Syst Software 2011;84(7):1197–208.
[21] Wu X, Sun W. Random grid-based visual secret sharing for general access structures with cheat-preventing ability. J Syst Software 2012;85(5):1119–34.
[22] Lukac R, Plataniotis KN. Bit-level based secret sharing for image encryption. Pattern Recognit 2005;38(5):767–72.
[23] Chao KY, Lin JC. Secret image sharing: a Boolean-operations-based approach combining benefits of polynomial-based and fast approaches. Int J Pattern Recognit Artif Intell 2009;23(2):263–85.
[24] Wang D, Zhang L, Ma N, Li X. Two secret sharing schemes based on boolean operations. Pattern Recognit 2007;40(10):2776–85.
[25] Chen TH, Wu CS. Efficient multi-secret image sharing based on boolean operations. Signal Process 2011;91(1):90–7.
[26] Chen CC, Wu WJ. A secure boolean-based multi-secret image sharing scheme. J Syst Software 2014;92(0):107–14.
[27] Chen CC, Chen CC, Lin YC. Weighted modulated secret image sharing method. J Electron Imag 2009;18(4):043011.
[28] Lin SJ, Chen LST, Lin JC. Fast-weighted secret image sharing. Opt Eng 2009;48(7):1–7. 077008
[29] Pakniat N, Noroozi M, Eslami Z. Secret image sharing scheme with hierarchical threshold access structure. J Visual Commun Image Represent 2014;25(5):1093–101.
[30] Li P, Yang CN, Zhou Z. Essential secret image sharing scheme with the same size of shadows. Digital Signal Process 2016;50:51–60.
[31] Harrison MA. On the classification of boolean functions by the general linear and affine groups. J Soc Ind Appl Math 1964;12(2):285–99.

[32] Millan W, Clark A, Dawson E. Heuristic design of cryptographically strong balanced boolean functions.. In: EUROCRYPT. In: Lecture Notes in Computer Science, 1403. Springer; 1998. p. 489–99.
[33] Stănică P, Hak Sung S. Boolean functions with five controllable cryptographic properties. Des Codes Cryptography 2004;31(2):147–57.
[34] Rout RK, Choudhury PP, Sahoo S. Classification of boolean functions where affine functions are uniformly distributed. CoRR 2013. abs/1303.3527.
[35] Rout RK, Choudhury PP, Sahoo S, Ray C. Partitioning 1-variable boolean functions for various classification of *n*-variable boolean functions. Int J Comput Math 2015;92(10):2066–90.
[36] A new kind of science. Champaign, Ilinois, US, United States: Wolfram Media Inc.; 2002. ISBN 1-57955-008-8.
[37] Kullback RLS. On information and sufficiency. Ann Math Stat 1951;22(1):79–86.
[38] Lefebvre G, Steele R, Vandal AC. A path sampling identity for computing the kullback leibler and j divergences. Comput Stat Data Anal 2010;54(7):1719–31.
[39] Zhao X, Turk M, Li W, chin Lien K, Wang G. A multilevel image thresholding segmentation algorithm based on two-dimensional KL divergence and modified particle swarm optimization. Appl Soft Comput 2016;48(C):151–9.
[40] http://www.imageprocessingplace.com/root_files_V3/image_databases.htm.
[41] Wang Z, Bovik AC, Sheikh HR, Simoncelli EP. Image quality assessment: From error visibility to structural similarity. IEEE Trans Image Process 2004;13(4):600–12.
[42] Maity SP, Maity S, Sil J. Multicarrier spread spectrum watermarking for secure error concealment in fading channel. Telecommun Syst 2012;49(2):219–29.