Journal of King Saud University – Computer and Information Sciences 34 (2022) 1246–1262

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

A new efficient TKHC-based image sharing scheme over unsecured channel

Mahmoud E. Hodeish [a,b,*], Linas Bukauskas [c], Vikas T. Humbe [d]

[a] School of Computational Sciences, S.R.T.M. University, Nanded, India
[b] Department of Computer, Faculty of Education-Zabid, Hodaidah University, Hodaidah, Yemen
[c] Faculty of Mathematics and Informatics, Vilnius University, Didlaukio 47, Vilnius, Lithuania
[d] School of Technology, S.R.T.M. University, Sub-Centre, Latur, India

ARTICLE INFO

Article history:
Received 20 February 2019
Revised 3 August 2019
Accepted 3 August 2019
Available online 13 August 2019

Keywords:
Visual cryptography (VC)
Secret sharing
Hill Cipher
Confidentiality
Histogram
Pixels correlations

ABSTRACT

The major problems of Visual Secret Sharing (VSS) are the pixel expansion and lossy recovery. The former creates large-sized shared images and makes their handling, storage, and speed transmission via networks challenging, whereas the latter leads to poor contrast of the recovered images. In addition, sharing a huge volume of images and transmitting the shared images through one less channel is a critical problem of VSS where any unauthenticated user can attack, discover the generated shares, and recover the secret image. In this paper, an efficient TKHC algorithm is proposed to augment the privacy and safety of the shared images. Moreover, the new TKHC-based VSS scheme is utilized to sharing a huge RGB and grayscale images which are subjected to be encrypted and decrypted by means of TKHC and providing strong security to transmit all the generated shares via one public channel. In comparison to the existing schemes, the proposed scheme shows significant improvement in encryption quality with lightweight computation cost. Furthermore, it withstands the known-plaintext and brute-force attacks and overall creates a balance between security, cost, and performance.

1. Introduction

Due to the rapid development in networking technologies, the transmission of sensitive information through Internet has become easy. Images specially those of visual information are widely used in various processes and applications. Hence, how to effectively protect an image from unauthorized access has become a critical issue nowadays. Therefore, network and information security have gained a great significance and importance in network technology for their vital role in storing, transmitting information, and protecting them from various attacks. In general, in network and information security there have been many techniques such as information hiding and cryptography which are commonly used to protect any type of information (Umamageswari et al., 2011).

Cryptography is an ancient encryption technique used to protect information by ensuring high-end communication between the sender and receiver (Mishra et al., 2015). In cryptography, the secret message becomes a disordered code after being encrypted and, then, it can be transmitted securely via a communication channel. The original message is decrypted by using a correct key. A common solution to the challenge of image protection is to use some standard data encryption algorithms such as AES, DES, IDEA, RSA, etc. However, complex mathematical calculations and large computational overheads over huge volume of multimedia data render the standard data encryption algorithms inefficient for the image encryption (Chen et al., 2015). Briefly, the most important problem of cryptography is that encryption and decryption processes certainly consume much time (Hou, 2003; Chen, 2013).

Therefore, VC or so-called VSS scheme is a new direction of the cryptography proposed by Moni Naor and Adi Shamir (Naor and Shamir, 1995) in 1994 as a subset of secret sharing used to encode visual information (images, texts, written materials, etc.) in a such way that the decoding process can be done by Human Visual System (HVS) without any complex computation. In general, the

* Corresponding author.
E-mail addresses: mah_hodeish@yahoo.com, mah.hodeish@gmail.com, mah_hodeish@srtmu.ac.in (M.E. Hodeish).

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2019.08.004
1319-1578/Production and hosting by Elsevier B.V. on behalf of King Saud University.

VSS acts as a special approach in secret sharing and the secret is a concealed image. Its mechanism can be illustrated as follows: firstly, encodes an image into *n* shadow images - called shared images - according to basis matrices and; second, distributes these shadows to different *n* participants; then, for decryption process, any sufficient set of participants can superimpose their shares to retrieve the secret (original image) so that insufficient set of participants never retrieve any information (Shyu, 2009). For instance, the basis matrices for the *3-out-of-3* VSS scheme (Naor and Shamir, 1995) are:

$$C0 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \quad C1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$

Physically, the 3-out-of-3 VSS scheme can be implemented by column permutation of C^0 (C^1). The column permutation is performed when encoding every White (Black) pixel in *P* of the original image. For a comprehensive study on VSS schemes, ref. (Hodeish and Humbe, 2014) offers a descriptive and interpretative study on VSS, which covers the 'State-of-the-art' concept and classification of schemes based on some various measures.

Nevertheless, the major contribution of the current paper, a new version of Hill cipher algorithm called Two-Key Hill Cipher (TKHC) is proposed to produce TKHC-based VSS scheme to share a huge volume of gray and color images and to augment the privacy and safety of generated shared images. Unlike the traditional VC which require transmitting the shared images through different communication channels, the generated shares of the proposed scheme can be transmitted over unsecured public channel. The TKHC used two rounds of encryption by applying two different keys. What distinguishes the TKHC is that the dealer sends only one key to the combiner where the second key mathematically is generated on the basis of the first key at the decryption side.

However, the experimental results demonstrate that the proposed TKHC-based VSS scheme is an efficient scheme which satisfy the VC conditions in generating shared images with a quarter of the original image size and recovering the original image without any impairment of information, proved by obtaining the standard values of (MSE = 0, PSNR = ∞, UIQ = 1, MD = 0, AD = 0) and the equal values of entropy, SD, MSDR for the original and recovered images. The pixel correlation towards their ideal values and the encrypted shares content is random-like and perfectly have uniform histograms. Moreover, theoretical and security analysis along with time complexity proves the superiority of the proposed scheme that withstands the known-plaintext and brute-force attacks and has a high performance in term of time complexity, leading to increase the overall possibility for practical applications of VC.

2. Related works

Secret Sharing Scheme (SSS) was independently proposed by *Shamir* (Shamir, 1979) and *Blackly* (Blakley, 1979). The basic concept of SSS is to encode the secret message into *n* shares and distribute them to different participants. The secret can be recovered when any qualified set of participants stacked their shares together. Subsequently, *Shamir* (Shamir, 1979) generalized this problem to (k, n) threshold SSS and proposed a SSS on the basis of polynomial interpolation. Factually, *Shamir's* scheme (Shamir, 1979) has been utilized to solve such security problems in an unsecured environment like public cloud. For instance, *Marwan et al.* (Marwan et al., 2018) have used SSS along with homomorphic encryption and Secure Multi-party Computation (SMC) so as to protect medical data against any unauthorized usage when outsourcing computations to a public cloud and to maintain data privacy and confidentiality.

Marwan et al. (Marwan et al., 2019), too, have applied *Shamir's* scheme in his mechanism to improve the storage security of medical images. There are two main reasons for choosing SSS instead of other security approaches. The first reason is its ability to ensure fault-tolerance in cloud environment, the second is the fact that it does not demand complex computations.

The basic model of VSS was applied for binary images. However, it resulted in some important problems such as pixel expansion and image distortion. Recently, many researchers have proposed some methods to address such problems of VSS for black-and-white images (Ito et al., 1999, Yang, 2004, Tuyls et al., 2005; Yang and Chen, 2005; Ching-Nung and Tse-Shih, 2006; Liu et al., 2009; Pal et al., 2010; Hodeish and Humbe 2015; Hodeish et al., 2016). However, some recent studies have concentrated on gray-level and color images as in Lukac and Plataniotis (2005) B-bit image sharing scheme. This scheme is implemented by decomposing a secret gray-level image into 8 bit-planes where every bit-plane can be processed as a binary image. Then, each binary image is encoded into two shared images using the concept of traditional VC. After that, by combining the binary shared images, two gray-level shared images are obtained. Finally, the original secret image is recovered when the two gray-level shared images are decomposed into 8 bit-planes, respectively. Here, the original one can be recovered without distortion, but the shared images are expanded and this is an indication of the problem of pixel expansion.

However, the traditional VCS can also be raised to as OR-based VCS (OVCS). Factually, the monotone property of OR operation destroys the display quality of recovered images in OVCS. Accordingly, XOR-based VCSs (XVCSs) have been proposed (Tuyls et al., 2005; Wang and Dong, 2011) so as to enhance the visual quality by allowing participants to apply XOR operation for stacking purpose which permits the complete restoration of the secret image. (Yang and Wang 2014) investigated the relation between OVCS and XVCS by providing a theoretical prove that the basic matrices of OVCS can be used in XVCS with (k, n) general access structure. In other words, they provided a theoretical analysis to prove that the basic matrices in (k, n)-OVCS also satisfy the security and contrast conditions of (k, n)-XVCS. Meantime, the XOR operation enhanced the contrast to be $2^{\wedge(k-1)}$ times.

On the basis of DNA-XOR truth table, *Tuncer et al.* proposed a probabilistic DNA-XOR VSS scheme for color images in order to be used reversible data hiding algorithm (Tuncer and Avci, 2016). Their VSS scheme used DNA-XOR operator to split the secret data into three shares. Thereafter, each share is embedded into each channel of color image. The idea of using DNA-XOR operator was extracted from Watson–Crick complement rule (Enayatifar et al., 2014) where a color image firstly splitted to RGB channels. These channels are converted to binary code. Then, each pixel of the generated channels expressed as a DNA sequence. As example, the DNA binary code of the pixel value of the blue channel expressed as (11001001) which equivalent to [TACG] according to definition of eight kinds of schemes encoding map rule of DNA sequence (King and Gaborit, 2007). Furthermore, XOR operator has been extensively employed in DNA computing.

On the basis of Random Grid (RG) concept suggested by (Kafri and Keren, 1987), (Shyu, 2007) has proposed VSS scheme to deal with binary, gray-level, and color images. In the first stage of this scheme, random images with values belonging to [0,1] are generated. Then, two random images with the same size of the original one are obtained. This scheme refutes the pixel expansion whereas the recovered image has poor contrast. Moreover, a progressive VC scheme was proposed by (Fang, 2008) which encodes an expanded secret and a cover image into *n* meaningful shared images. Here, superimposing two shared images only leads to obtaining the recovered image with distortion, whereas stacking all shared

images leads to retrieve the original image without distortion. Regardless, the problem of the pixel expansion is still unaddressed. (Chen and Tsao, 2009) proposed two RG algorithms where the secret image is recovered clearly when only more shared images are superimposed together.

To improve the security of the VC, some schemes have merged between the VC and the Cryptography techniques. (Yadar and Ojha, 2013) have proposed a scheme based on Caser Cipher algorithm and the concept of RG for gray-level images. In this scheme, the generated shares had the same size of the original one and the retrieved image was lossless. Moreover, Shetty and Abraham (2015) proposed a VC scheme which could be applied to both binary and color images. It was implemented on the basis of the traditional VC concept to generate two shares from the secret image after being converted to a binary-valued image. Then, RSA algorithm was performed to encrypt the generated shares. Here, the generated shares and the recovered image had the same size of the original one. However, the recovered image was lossy, and the use of the RSA algorithm led to time consumption.

Recently, to ensure a confidentiality of image transmission, Shankar and Eswaran (2015) have proposed a (2, 2) VC scheme with a combination of AES algorithm. This combined scheme is suggested to secure and share color images that can be transmitted over a public channel. Whatsoever, AES algorithm needs more processing and requires more key rounds. Each round further in the AES algorithm needs round key from the key expansion algorithm. On the whole, when the size of images increases, the time of this scheme also increases. As well, Shankar and Eswaran (2017) have proposed an Elliptic Curve Cryptography (ECC)-based VSS scheme in order to be applied on RGB images. This scheme is secure in spite of its requirement for additional verification of the public key to be performed, yet the quality of the recovered image has to be improved. In addition, it is more complex and more difficult to be implemented since it is ECC-based VSS scheme.

It is worth noting that the classic Hill Cipher algorithm was not used with VSS. It is only Chen (2013) who used a linear equation Hill Cipher to construct two sub-images in his VSS method proposed for gray-level images. In this method, the RG concept was applied to the two sub-images to construct the final shared images. To recover the original image, the reverse process was applied with the inverse Hill Cipher. Here, the recovered image was lossless. Yet, one of the problems faced in using classic Hill Cipher in Chen (2013) method is that the inverse of a matrix may not exist due to the impossibility of decryption (Muttoo et al., 2011). Approximately, the schemes discussed above have various problems such as pixel expansion, image distortion, time and storage consumption, and weak security.

The current paper tackles this line of problems further by proposing an image sharing scheme integrated with a new cryptographic algorithm called Two-Key Hill Cipher (TKHC), which is also proposed in this paper in order to provide fast and secure transmission via networks, time and storage saving, and a balance between security, cost, and performance. In addition, it is looking at testing such valid and reliable metrics empirically.

The rest of this paper is organized as follows. An overview of Hill Cipher concept is given in Section 3. The proposed scheme is presented in Section 4. Experimental results and performance analysis of the proposed scheme are discussed in in Section 5 and Section 6, respectively. Finally, conclusion is drawn in Section 7.

3. An overview of Hill Cipher

Hill Cipher, as one of the famous symmetric encryption systems, was proposed by *Laster S. Hill* in 1929. It is considered as a good example of data encryption in blocks or streams. The main idea of Hill Cipher is based on the multiplication of matrices in which every block of characters (more than one character) in the plaintext is substituted by a block of characters in the ciphertext. In such that each character is coded with a unique integer value belonging to [0,25] and the modular is 26 (Bibhudendra, 2008). It is assumed that the plaintext message and the secret key consist of 4 and 16 values, respectively, and, then, the encryption side can be performed as:

$$C = k\ p \bmod 26 \quad (1)$$

where C is the ciphertext, p is the plaintext, and k is the key matrix. For decryption side, the inverse of the matrix k can be used to decrypt the ciphertext as:

$$p = k^{-1}\ C \bmod 26 \quad (2)$$

where; k^{-1}refers to inverse of matrix k. Moreover, the Hill Cipher according to Archarya et al. (2009) can be used for gray-level images encryption but, with modular of 256.

4. The proposed schemes

4.1. The proposed Two-Key Hill Cipher (TKHC) algorithm

The classic Hill Cipher has many merits. Some of these merits include the following: (1) it is resistant to the frequency letter analysis, (2) it is easily implemented, and (3) it provides high speed and high throughput. In spite of these merits, the noninvertible key matrix is the main demerit of Hill Cipher because the encrypted text can't be decrypted. Another demerit is the linear nature which can make it succumb to known-plaintext-attack (Bora and Ojha, 2015). Therefore, the first contribution of this paper is to develop a new Hill Cipher-based algorithm in order to overcome the problem of the non-invertible key matrix and to strengthen the security level. The idea of the new Hill Cipher-based algorithm (TKHC) is based on the use of two key matrices. The first key matrix is generated randomly and should satisfy the conditions of the invertible matrix. Moreover, the key matrix values should belong to two integer numbers *a, b* belonging to [0,255] for an images encryption and to [0,25] for characters encryption. The second key matrix is generated depending on the first key matrix by mathematically computing its cofactor matrix.

The detailed steps of TKHC algorithm can be described as follows:

TKHC-KeyGen()
Input: Two numbers *a, b* belonging to the range of [0,255].
Output: 1- *k1* (invertible matrix with the size of 4×4). 2- *k2* (invertible matrix with the size of 4×4).
Procedure:
Begin

- To generate the first key (*k1*),

1. Generate a random matrix (key) with size of 4×4 and elements belonging to [a,b]

$key = random([ab], 4, 4)$

2. Multiply the generated matrix (key) with its inverse

$test = key * floor(inv(key))$

3. If $test == I(Identicalmatrix)$

$k1 = test$

Else

Repeat the steps 1–3

- To generate the second key (*k2*),

$k2 = (\text{adj}\ (k1))^{T}$ (3)

Where *adj* denotes the *adjoint* or *adjugate* of square matrix

(*continued*)

TKHC-KeyGen()
and T is the transpose of the matrix.
End
TKHC-Encrypt()
Input: Plain text, M
Output: Cipher text, C
Procedure:
Begin
1. Divide the plain text M into blocks of size 4.
2. Encrypt the first block (p):

$C{=}E(k2, E(k1, p))$

Where E is an encryption function that encrypt four plain text, p of message in turn as:

C1=k1 ∗ p mod Modular

$C{=}k2 * C1$ *mod Modular*

Where Modular is equal to 26 for text and 256 for images.

3. Repeat the step 2 till all blocks of M being encrypted and get the cipher text C.

End
TKHC-Decrypt()
Input: Cipher text, C
Output: Plain text, M
Procedure:
Begin
1. Divide the cipher text C into blocks of size 4.
2. Decrypt the first block (c) by using the invers of keys ($k1^{-1}$ and $k2^{-1}$):

$M{=}D(k1^{-1}, D(k2^{-1}, c))$

Where D is a decryption function that decrypt four cipher text, c of message in turn as:

M1=$k2^{-1}$∗c mod Modular

$M{=}k1^{-1} * M1$ *mod Modular*

3. Repeat the step 2 till all blocks of C being decrypted and get the plain text M.

End

4.1.1. The mathematical proof

The following mathematical proof proves that the cofactor matrix of an invertible matrix is invertible.

If A matrix is an invertible matrix and B = *cofactor (A)*, then B is an invertible matrix.

Proof. *Suppose that* ***A*** *is an invertible matrix, which means that*

$A^{-1}{=}\frac{adj(A)}{|A|}{=}\frac{(co(A))^T}{|A|} \rightarrow (1)$, Where $(co(A))^T$ is a transpose of (A). Since $B{=}co(A)$, then by (1) we have $A^{-1}{=}\frac{B^T}{|A|}, \rightarrow (2)$

Now, put $|A|{=}\lambda$, since A is an invertible matrix, then, $\lambda{\neq}0$. According to (2), we obtain

$$A^{-1}{=}\frac{B^T}{\lambda}, \rightarrow (3)$$

By using cross-multiplication, then the equation (3) leads to $B^T{=}\lambda A^{-1}$

From the properties of the determinants, we get

$$\left|B^T\right|{=}\left|\lambda A^{-1}\right|{=}\lambda^n|A^{-1}|$$

Since, $\left|B^T\right|{=}|B|$ and $\left|A^{-1}\right|{=}\frac{1}{A}$, then. $|B|{=}\lambda^n\frac{1}{|A|}{=}\lambda^{n-1}{\neq}0$.

Therefore, ***B*** is invertible matrix.

4.2. The proposed TKHC-based VSS scheme

4.2.1. The mathematical model

Let $P = \{1, 2, \ldots, n\}$ be a set of participants, and 2^P refers to the set of all subsets of P. let $\Gamma_{Qual} \subseteq 2^P$ and $\Gamma_{Forb} \subseteq 2^P$, where $\Gamma_{Qual} \cap \Gamma_{Forb} = \phi$. The members of Γ_{Qual} referred as qualified sets, whereas the members of Γ_{Forb} are referred as forbidden sets. The pair $(\Gamma_{Qual}, \Gamma_{Forb})$ is defined as access structure. The set of the minimal qualified sets can be defined as $\Gamma_0 = \{Q \in \Gamma_{Qual} : Q' \notin \Gamma_{Qual}, \forall Q' \subset Q\}$. The qualified and forbidden set refers to the sufficient and insufficient number of shareholders. The proposed method is conducted for gray-level and color images by considering the following access structure:

Γ_{Qual}={{1,2,3,4}},and Γ_{Forb}={{1},{2},{3},{4},{1,2},{1,3},{1,4},{2,3},{2,4},{3,4},{1,2,3},{1,2,4},{1,3,4},{2,3,4}}.

4.2.2. The general framework

The general framework of the proposed scheme consists of two procedures, shares generation, and secret recovery. The block diagram of shares generation procedure is used to generate four shares by using two keys (*k1* & *k2*) that are generated by the *TKHC-keyGen*() procedure and one random master grid (RG) as shown in Fig. 1(a). In secret recovery procedure, as shown in Fig. 1(b), the participants are only holding their own shares, whereas the *k1* is held by the combiner along with the master random grid. The *k2* is generated on the basis of *k1*.

However, the detailed steps of the procedures of the proposed scheme are described as follows:

SharesGen()
Input:

1- Original image with the size of $n \times n$ (*GI with form of* (gray or color)).
2- The first generated key (*k1*).

Output:

1- Four encoded sub-images (shares) (E1, E2, E3, and E4).

Procedure:

1. Using equation (3) generate k2.
2. By raster scan order, split the original image *GI* with the size of $n \times n$ into blocks where each block (P) consisting of four pixels.
3. $P = (p1, p2, p3, p4)$
4. $I \leftarrow TKHC - Encrypt(P, k1)$

$$\begin{bmatrix} I1 \\ I2 \\ I3 \\ I4 \end{bmatrix} = \begin{bmatrix} k1_{11} & k1_{12} & k1_{13} & k1_{14} \\ k1_{21} & k1_{22} & k1_{23} & k1_{24} \\ k1_{31} & k1_{32} & k1_{33} & k1_{34} \\ k1_{41} & k1_{42} & k1_{43} & k1_{44} \end{bmatrix} \begin{bmatrix} p1 \\ p2 \\ p3 \\ p4 \end{bmatrix} \text{mod} 2^8. \quad (4)$$

5. $I = (I1, I2, I3, I4)$
6. $EI \leftarrow TKHC - Encrypt(I, k2)$

$$\begin{bmatrix} EI1 \\ EI2 \\ EI3 \\ EI4 \end{bmatrix} = \begin{bmatrix} k2_{11} & k2_{12} & k2_{13} & k2_{14} \\ k2_{21} & k2_{22} & k2_{23} & k2_{24} \\ k2_{31} & k2_{32} & k2_{33} & k2_{34} \\ k2_{41} & k2_{42} & k2_{43} & k2_{44} \end{bmatrix} \begin{bmatrix} I1 \\ I2 \\ I3 \\ I4 \end{bmatrix} \text{mod } 2^8 \quad (5)$$

7. $EI = (EI1, EI2, EI3, EI4)$

where *I1* to *I4* are the encoded pixels, $k1_{11}$ to $k1_{44}$ denote the encryption key and *p1* to *p4* are the original pixels.

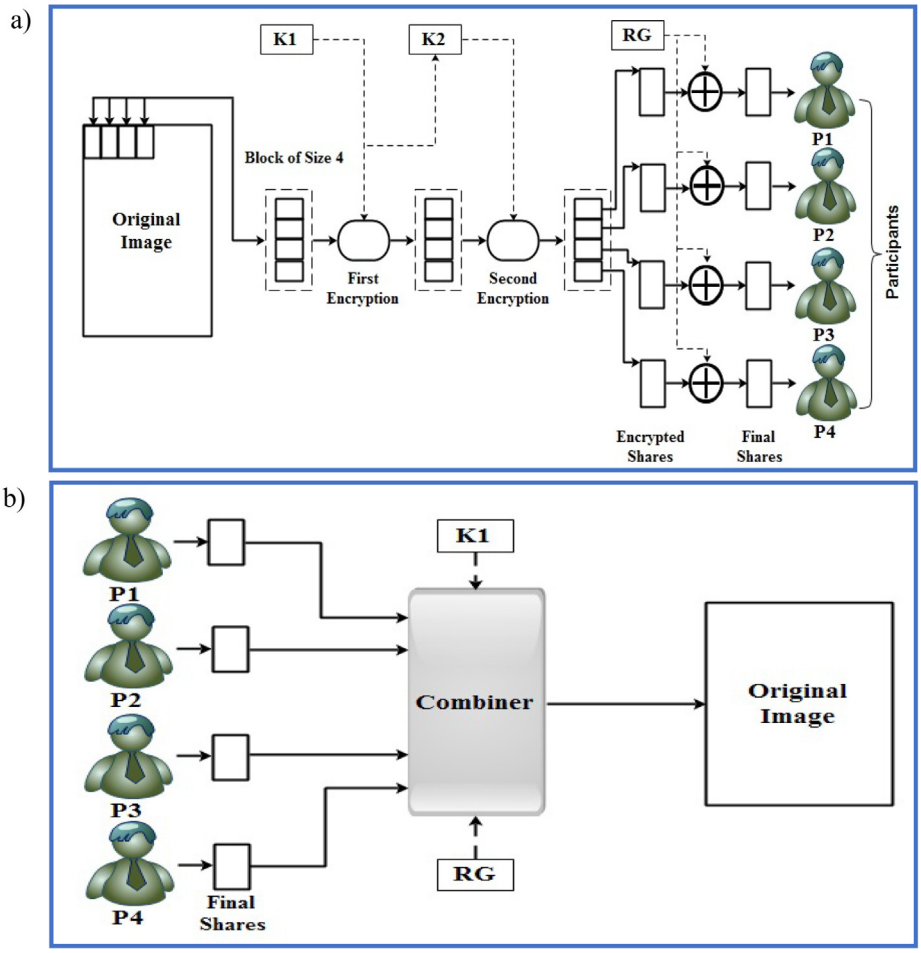


Fig. 1. Block diagrams of the proposed scheme, (a) shares generation procedure, (b) secret recovery procedure.

8. Successively repeat the steps 3 and 6 until all pixels of blocks scanned to construct the four sub-images (*EI1*, *EI2*, *EI3*, and *EI4*) with the size of n × n/4.
9. Construct a random master grid *M* with pixels belonging to [0,255] with the same size of the sub-images.

$$M = random([0255], n, n/4)$$

10. Collect the Master grid M and the four sub-images (*EI1*, *EI2*, *EI3*, and *EI4*) to generate four encoded shares (*E1*, *E2*, *E3*, and *E4*) into equation (6).

$$\begin{aligned} E1 &= M \oplus EI1 \\ E2 &= M \oplus EI2 \\ E3 &= M \oplus EI3 \\ E4 &= M \oplus EI4 \end{aligned} \tag{6}$$

where ⊕ denotes XOR operation.

11. Transmit the four encoded shares (*E1*, *E2*, *E3*, and *E4*) through one channel.

Secret-Recovery()
Input:

1- First generated key (*k1*).
2- Final four encoded shares (*E1*, *E2*, *E3*, and *E4*) and *M*.

Output: -

- The original image.

Procedure:

1. Gather *M*, *E1*, *E2*, *E3*, and *E4* into equation (7) in order to reconstruct four sub-images (*EI1′*, *EI2′*, *EI3′*, and *EI4′*).

$$\begin{aligned} EI1' &= M \oplus E1 \\ EI2' &= M \oplus E2 \\ EI3' &= M \oplus E3 \\ EI4' &= M \oplus E4 \end{aligned} \tag{7}$$

2. Using equation (3) generate k2.
3. Take the first pixel of each reconstructed four sub-images (*EI1′*, *EI2′*, *EI3′*, and *EI4′*) by raster scan order and *k2* into equation (8) to obtain *I1′*, *I2′*, *I3′*, and *I4′*.

$$\begin{bmatrix} I1' \\ I2' \\ I3' \\ I4' \end{bmatrix} = \begin{bmatrix} k2_{11} & k2_{12} & k2_{13} & k2_{14} \\ k2_{21} & k2_{22} & k2_{23} & k2_{24} \\ k2_{31} & k2_{32} & k2_{33} & k2_{34} \\ k2_{41} & k2_{42} & k2_{43} & k2_{44} \end{bmatrix}^{-1} \begin{bmatrix} EI1' \\ EI2' \\ EI3' \\ EI4' \end{bmatrix} \mod 2^8 \tag{8}$$

4. Take the first pixel of each *I1′*, *I2′*, *I3′*, and *I4′* and the *k1* into equation (9) to obtain the original pixels *p1*, *p2*, *p3*, and *p4*.

$$\begin{bmatrix} p1 \\ p2 \\ p3 \\ p4 \end{bmatrix} = \begin{bmatrix} k1_{11} & k1_{12} & k1_{13} & k1_{14} \\ k1_{21} & k1_{22} & k1_{23} & k1_{24} \\ k1_{31} & k1_{32} & k1_{33} & k1_{34} \\ k1_{41} & k1_{42} & k1_{43} & k1_{44} \end{bmatrix}^{-1} \begin{bmatrix} I1' \\ I2' \\ I3' \\ I4' \end{bmatrix} \bmod 2^8 \quad (9)$$

5. Take the recovered block $P = p1, p2, p3, p4)$ by scan order to reconstruct the recovered image.
6. Successively repeat the steps 3 and 5 until all pixels of *EI1′*, *EI2′*, *EI3′*, and *EI4′* scanned and recover the original secret image without any distortion.

5. Experimental results

As it has been mentioned above, the current VSS method is proposed with the use of the new TKHC algorithm for gray-level and RGB images. Four experiments are conducted to implement the proposed scheme. The first and second experiment are applied on the gray-level Lena and Pepper images with the size of 512×512 and 256×256 as shown in Figs. 2(a) & 3(a), separately and respectively.

Here, since the number of generated shares is four, the block size should be also four in order to be processed in turn and the size of the key matrices is 4×4 according to linear nature of Hill Cipher algorithm. To generate the two key matrices *k1* and *k2*, the two chosen numbers *a* and *b* belonging to [0,255] are assigned with 6 and 8 values, respectively. Based on the values of *a* and *b*, the first key matrix *k1* with the size of 4×4 and values belonging to [6,8] is generated randomly as an invertible matrix. The second key matrix *k2* can mathematically be generated by computing the cofactor matrix of the first generated key *k1* using equation (3). *K2* is an invertible matrix due to the mathematical proof.

The keys of the first experiment are shown as follows:

$$k1 = \begin{bmatrix} 7 & 8 & 7 & 8 \\ 7 & 8 & 8 & 8 \\ 8 & 8 & 7 & 7 \\ 6 & 7 & 7 & 7 \end{bmatrix}, k2 = \begin{bmatrix} 0 & 0 & 1 & -1 \\ -7 & 14 & -1 & -7 \\ 0 & -1 & 0 & 1 \\ 8 & -15 & 0 & 8 \end{bmatrix}$$

The keys of the second experiment are shown as follows:

$$k1 = \begin{bmatrix} 8 & 8 & 7 & 7 \\ 8 & 8 & 8 & 7 \\ 7 & 7 & 6 & 6 \\ 8 & 7 & 6 & 8 \end{bmatrix}, k2 = \begin{bmatrix} -16 & 10 & -1 & 8 \\ 2 & -2 & 1 & -1 \\ 15 & -8 & 0 & -8 \\ 1 & -1 & 0 & 0 \end{bmatrix}$$

In the shares' generation procedure, four encoded grids *E1, E2, E3*, and *E4* are generated using the two key matrices *k1* and *k2* generated in the first procedure. Firstly, the original secret image is spilt by raster scan order into sub-blocks where each block consists of four pixels *p1, p2, p3*, and *p4*. Secondly, the four pixels of every block is successively passed into equation (4) to be encrypted using *k1*. Then, every encoded block is successively taken into equation (5) and encoded again using *k2*. After that, four sub-images *EI1, EI2, EI3*, and *EI4* with the size of 512×128 and 256×64 are obtained as shown in Fig. 2(b, c, d, and e) and Fig. 3(b, c, d, and e) for the first and second experiment, respectively.

In the fifth step of this procedure, master random grid *M* with values belonging to [0,255] is randomly generated with the size of 512×128 and 256×64 as shown in Figs. 2(f) & 3(f). Next, the master random grid *M* and the four sub-images *EI1*, *EI2*, *EI3*, and *EI4* are successively taken into equation (6) to perform *XOR* operation, respectively.

Finally, four encoded grids *E1*, *E2*, *E3*, and *E4* with the size of 512×128 and 256×64 are obtained as illustrated in Fig. 2(g, h, i, and j) & 3(g, h, i, and j). Therefore, the encoded grids can be sent via a network even through one channel with only the first key matrix *k1*. The final procedure is to recover the original secret image by using right keys k1 and k2 without any distortion as can be shown in Figs. 2(o) & 3(o). Once using wrong keys, as shown in Figs. 2(p) & 3(p), the original image cannot be obtained.

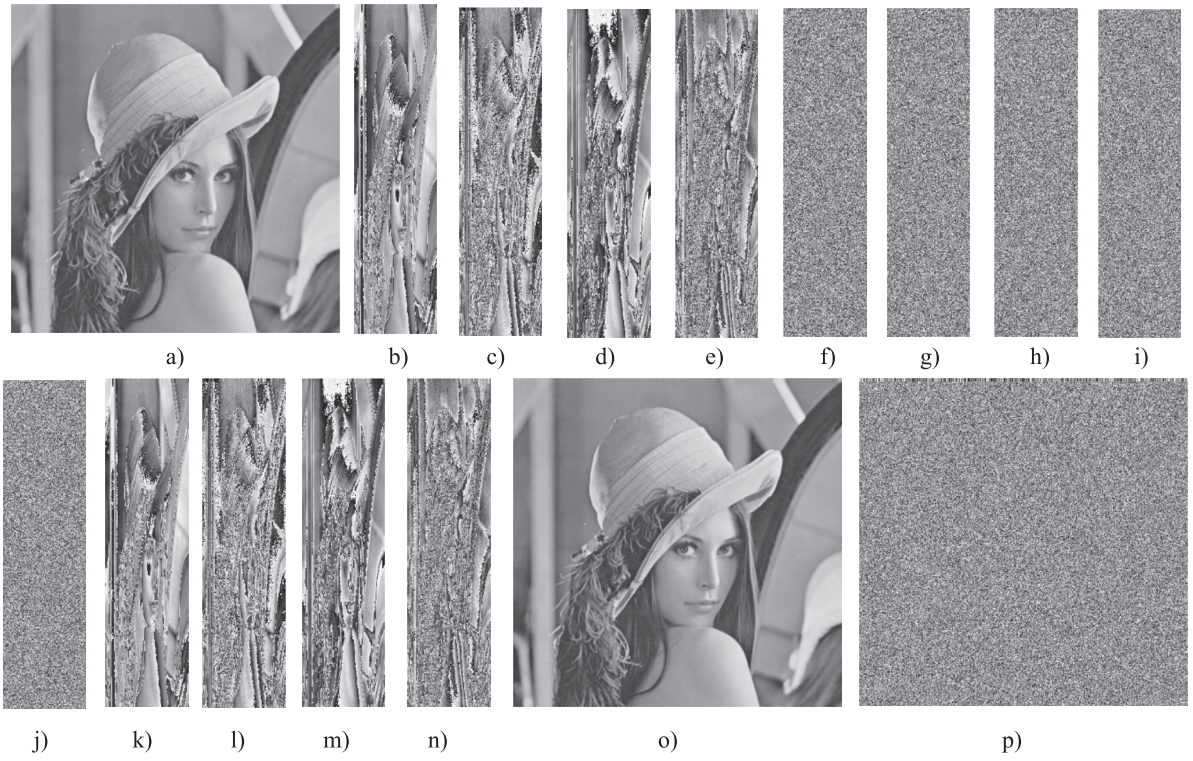


Fig. 2. Simulation results of the first experiment, (a) The secret image Lena with size 512×512, (b)-(e) the sub-images EI1, EI2, EI3, and EI4 with the size of 512×128, (f) master random grid M with size of 512×128, (g)-(j) The four encoded grids E1, E2, E3, and E4 with the size of 512×128, (k)-(n) The four retrieved sub-images with the size of 512×128, (o) The recovered original image, and (p) the recovered image of using wrong keys.

The third and fourth experiment of the proposed method is applied on RGB Lena and Pepper images with the size of $256 \times 256 \times 3$ as presented in Figs. 4(a) & 5(a), respectively. Here, the same steps done in the first experiment are applied to red (R), green (G), and blue (B) channels of the RGB Lena and Pepper images. Regarding the key generation, the two chosen numbers *a & b* are assigned with 1 and 2 values, respectively.

The two generated key matrices *k1 & k2* of the third experiment are shown as follows:

$$k1 = \begin{bmatrix} 1 & 1 & 2 & 2 \\ 1 & 2 & 2 & 2 \\ 2 & 2 & 2 & 1 \\ 1 & 2 & 1 & 1 \end{bmatrix}, k2 = \begin{bmatrix} 2 & -3 & 0 & 2 \\ -1 & 1 & 0 & 0 \\ -2 & 3 & 1 & -3 \\ 2 & -2 & -1 & 2 \end{bmatrix}$$

and the two generated key matrices k1 & k2 of the fourth experiment are shown as follows:

$$k1 = \begin{bmatrix} 2 & 2 & 2 & 1 \\ 2 & 1 & 2 & 2 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}, k2 = \begin{bmatrix} -1 & 0 & 0 & 1 \\ -1 & 1 & 0 & 0 \\ 1 & 0 & -1 & 0 \\ 2 & -2 & 1 & -2 \end{bmatrix}$$

6. Discussion and performance analysis

6.1. Pixel expansion

The problem of pixel expansion is eliminated in the proposed scheme not through generating shared images with the same size of the original image, but through reducing the size of the generated shared images to 1/4 as shown in Fig. 2(k, l, m, and n), 3 (k, l, m, and n), 4(k, l, m, and n), and 5(k, l, m, and n).

6.2. Contrast and statistical analysis

As shown in Figs. 2(o), 3(o), 4(o), and 5(o), the recovered images can be obtained without any distortion. Here, different statistical metrics of image restoration are used so as to evaluate the image quality and prove that the recovered images have been recovered with the same quality of original one. These metrics are defined as follows:

6.2.1. Mean Square Error (MSE) and Peak-Signal-to-Noise Ratio (PSNR)

The *PSNR* is an engineering formulation calculated via *MSE* (Chen et al., 2016) and mathematically computed as in (10 & 11).

$$\mathrm{MSE} = \frac{1}{\mathrm{M} \times \mathrm{N}} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(h_{ij} - h'_{ij}\right)^2 \tag{10}$$

where h_{ij} and h'_{ij} are the pixel values of the original image and the reconstructed image, respectively.

$$\mathrm{PSNR} = 10 \times \log \frac{R^2}{\mathrm{MSE}} \tag{11}$$

Statistically, when the *PSNR* value is equal to ∞, it indicates that the scheme provides a maximum visual quality (Shankar and Eswaran, 2015; Rose and Thampi, 2015).

6.2.2. Universal Index Quality (UIQ)

UIQ (Wang and Bovik, 2002) is different from the old-style error summation metrics and the way of its design was done by modeling any image distortion as a combination of three factors: loss of correlation, luminance distortion, and contrast distortion. However, can mathematically be computed as in (12).

$$\mathrm{UIQ} = \frac{4\sigma_{xy} \quad \bar{x}\bar{y}}{\left(\sigma_x^2 + \sigma_y^2\right) \quad \left[\left(\bar{x}\right)^2 + \left(\bar{y}\right)^2\right]} \tag{12}$$

The *UIQ* between two images varies from -1 to +1, i.e. $-1 \leq UIQ \geq +1$. Two images *X* and *Y* have strong positive linear correlation if *UIQ* is close to +1. The -1 value of *UIQ* indicates a negative relationship between the two images and the zero value indicates that there is no relationship between the two images (Wang and Bovik, 2002).

6.2.3. Maximum Difference (MD)

The *MD* metric is used to measure the maximum error between the original and the recovered image. It is direct proportional to contrast giving an image dynamic range (Rajkumar and Malathi, 2016) which expressed as (13).

$$MD = max\left|x_{ij} - y_{ij}\right| \tag{13}$$

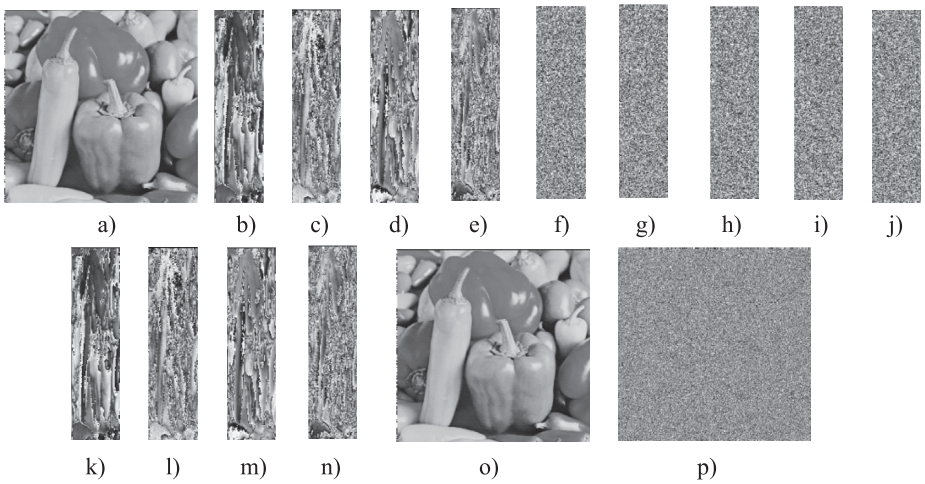


Fig. 3. Simulation results of the second experiment, (a) The secret image Pepper with size 256×256, (b)-(e) the sub-images EI1, EI2, EI3, and EI4 with the size 256×64, (f) master random grid M with size of 256×64, (g)-(j) The four encoded grids E1, E2, E3, and E4 with the size of 256×64, (k)-(n) The four retrieved sub-images with the size of 256×64, (o) The recovered original image, and (p) the recovered image of using wrong keys.

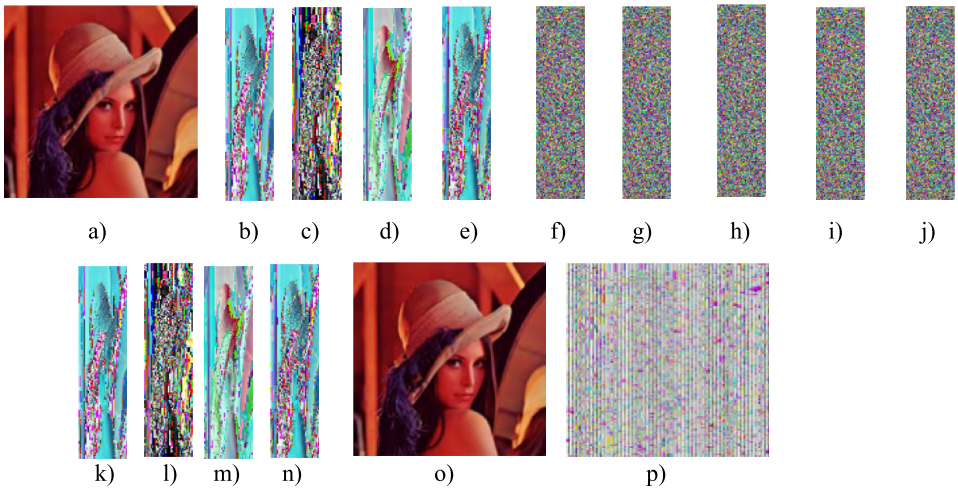


Fig. 4. Simulation results of the third experiment , (a) The secret image Lena with size 256 × 256 × 3, (b)-(e) the sub-images EI1, EI2, EI3, and EI4 with the size of 256 × 64 × 3, (f) master random grid M with size of 256 × 64 × 3, (g)-(j) The four encoded grids E1, E2, E3, and E4 with the size of 256 × 64 × 3, (k)-(n) The four retrieved sub-images with the size of 256 × 64 × 3, (o) The recovered original image, and (p) the recovered image of using wrong keys.

6.2.4. Average Difference (AD)

The average error between the input image and the recovered image is measured by *AD* metric (Ece and Mullana, 2011) and expressed as (14).

$$AD = \frac{1}{M \times N} \sum_{i=1}^{M} \sum\nolimits_{j=1}^{N} (x_{ij} - y_{ij}) \tag{14}$$

where, x and y denote input image and recovered image, respectively.

The values of *MSE*, *PSNR*, *UIQ, MD,* and *AD* in the four experiments of the proposed method, i.e. for gray-level and color images are given in Table 1a. Here, the zero value of (*MSE, MD, AD*), infinite *PSNR* value, and '1′ *UIQ* value confirm that the original images have been recovered completely without any loss of sensitive information.

6.2.5. Entropy

It is a measure to evaluate the quantity of image information or the amount of randomness (Wang and Shen, 2011). Mathematically expressed as (15).

$$Entropy = \sum_{i=0}^{255} P(x_i) log_2 P(x_i)) \tag{15}$$

where, $P(x_i)$ signifies the probability of image level x_i.

6.2.6. Standard Deviation (SD)

It is imitating the deviation of image contrast to the mean (Kumar and Gupta, 2012). In other words, it is a measure that is used to quantify the amount of variation or dispersion of a set of data values. Its formula expressed as (16)

$$\sigma^2 = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (X(i,j) - \mu)^2 \tag{16}$$

where, M and N the dimensions of the image that referred by X and μ denotes the mean value of X.

6.2.7. Mean-to-Standard-Deviation Ratio (MSDR)

It is called coefficient of variation (CV), which is a normalized measure of data distribution defined as SD divided by the Mean.

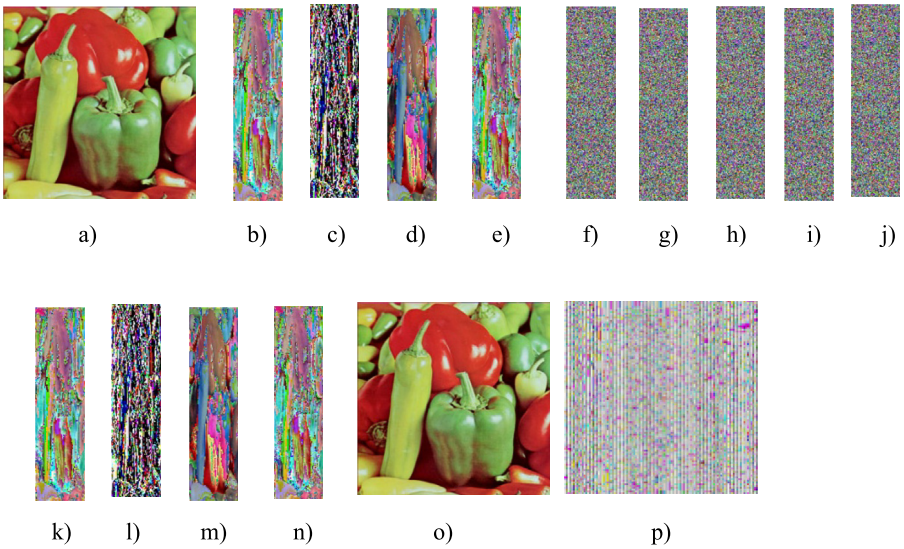


Fig. 5. Simulation results of the fourth experiment , (a) The secret image Pepper with size 256 × 256 × 3, (b)-(e) the sub-images EI1, EI2, EI3, and EI4 with the size of 256 × 64 × 3, (f) master random grid M with size of 256 × 64 × 3, (g)-(j) The four encoded grids E1, E2, E3, and E4 with the size of 256 × 64 × 3, (k)-(n) The four retrieved sub-images with the size of 256 × 64 × 3, (o) The recovered original image, and (p) the recovered image of using wrong keys.

Table 1a
Statistical analysis (*MSE*, *PSNR*, *UIQ*, *MD*, and *AD*) for the four experiments of the proposed method.

Experiment	Statistical Metrics				
	MSE	PSNR	UIQ	MD	AD
1st experiment	0	∞	1	0	0
2nd experiment	0	∞	1	0	0
3rd experiment	0	∞	1	0	0
4th experiment	0	∞	1	0	0

It describes the variability of an image relative to its mean (Babu and Sudha, 2016) which expressed as (17).

$$MSDR = \frac{\sigma}{\mu} \tag{17}$$

The obtained results of entropy, SD, and MSDR presented in Table 1b are identically similar to the original and recovered images. These results, in turn, confirm and reinforce the obtained results shown in Table 1a.

Overall, the statistical analysis of the four experiments proves that the current scheme is an efficient scheme due to its ability to recover the secret images without any loss of information.

6.3. Histogram analysis

The image histogram analysis indicates graphical representation of the pixel intensity values and demonstrates the tonal distribution in an image (Somaraj and Hussain, 2015; Kanso and Ghebleh, 2018). In brief, it offers the statistical characteristics of image intensity from which image may be visible (Kandar et al., 2019). The main goal of the histogram analysis is to demonstrate the confusion and diffusion properties in the ciphered data. In the proposed scheme, the histogram shows that the pixel values of the final encrypted shares are uniformly distributed and also the pixels have random-like distributions. Thus, the final encrypted shares give no useful information about the secret image. It is evident from Figs. 6, 7, 8, and 9 that the encrypted shares content is random-like and have perfectly uniform histograms.

6.4. Pixels correlation

Pixel correlation determines the relationship between two adjacent pixels. Generally, the goodness of image encryption scheme is represented in its ability to hide all the attributes of a secret image and the encrypted image is totally random and highly uncorrelated (Ahmad et al., 2018). The image pixels is highly correlated, if the correlation between two adjacent pixels is nearly 1. On the contrary, if the correlation between two adjacent pixels is nearly 0, the image pixels is highly uncorrelated. The correlation coefficient of any two adjacent pixels in the same image can be expressed with relation (18):

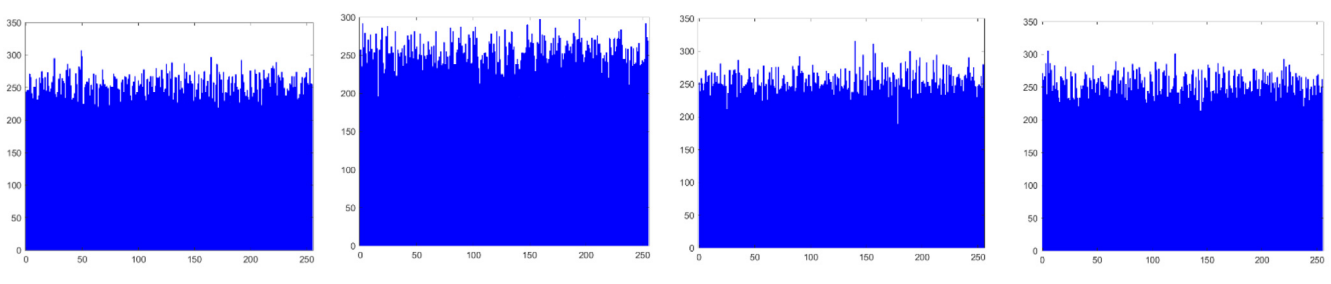
$$CorrCoeff = \frac{Cov(x,y)}{\sqrt{Var(x)} \times \sqrt{Var(y)}} \tag{18}$$

$$Var(x) = \frac{1}{N}\sum_{i=1}^{N}\left[(x_i - E(x))^2\right] and Cov = \frac{1}{N}[(x_i - E(x)) \times (y_i - E(y))]$$

where, *CorrCoeff* is the correlation coefficient and $Cov(x,y)$ is covariance at pixel $\times$ and y. $Var(x)$ is the variance at the pixel value $\times$ in the image, $E(x)$ is expected value operator and N is total number of pixels in the matrix.

Table 1b
Statistical analysis (*Entropy*, *SD*, and *MSDR*) for the four experiments of the proposed method.

Experiment		Statistical Metrics		
		Entropy	SD	MSDR
1st experiment	Original Image	7.4455	47.8537	0.3858
	Recovered Image	7.4455	47.8537	0.3858
2nd experiment	Original Image	7.5327	53.1529	0.4318
	Recovered Image	7.5405	53.2254	0.4289
3rd experiment	Original Image	7.7516	58.7835	0.4584
	Recovered Image	7.7516	58.7835	0.4584
4th experiment	Original Image	7.7339	65.6380	0.5924
	Recovered Image	7.7339	65.6380	0.5924



a) b) c) d)

Fig. 6. (a)-(d) Histogram of the final encrypted shares (shown in Fig. 2(g)-(j)).

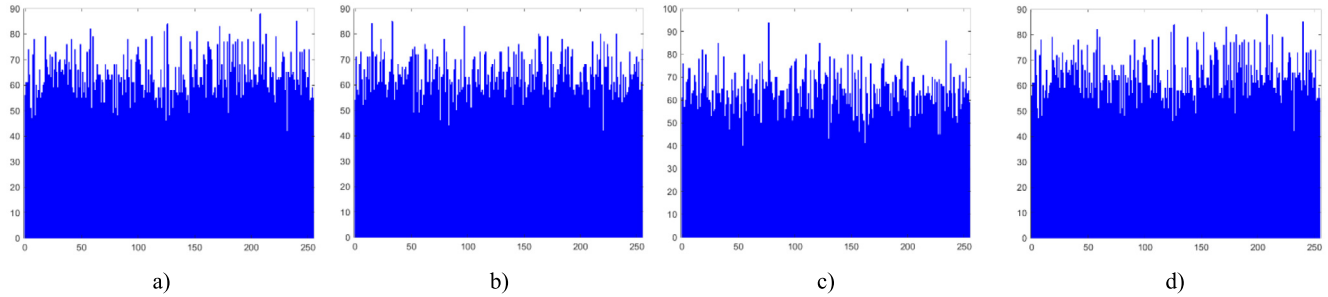


Fig. 7. (a)-(d) Histogram of the final encrypted shares (shown in Fig. 3(g)-(j)).

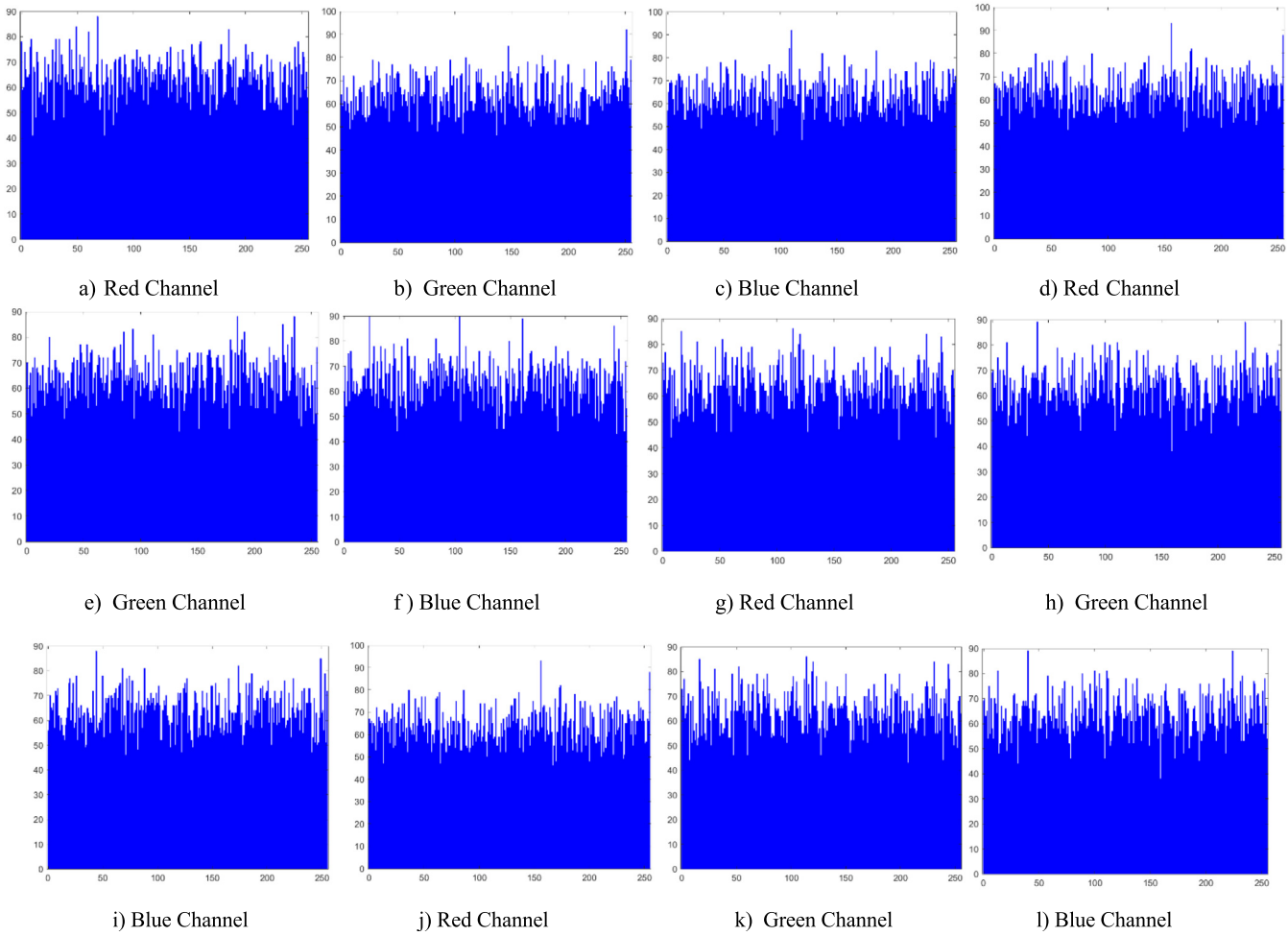


Fig. 8. (a)-(c) Histogram of the first encrypted share (shown in Fig. 4(g)), (d)-(f) Histogram of the second encrypted share (shown in Fig. 4(h)), (g)-(i) Histogram of the third encrypted share (shown in Fig. 4(i)), (j)-(l) Histogram of the first encrypted share (shown in Fig. 4(j)).

To analyze the horizontal, vertical and diagonal correlation coefficients of the original and the final encrypted shared images, we have randomly selected same 2500 pairs of adjacent pixels for each image in horizontal, vertical and diagonal directions. The experimental values for pixel correlation in different directions, i.e., vertical, horizontal, and diagonal, for the different four conducted experiments are listed in Tables 2 & 3, and the graphical representations of the pixel correlations are shown in Figs. 10, 11, 12. As shown in the tables and figures, the low pixel correlation values of the final encrypted shares show that the proposed scheme is perfect in decorrelating the adjacent pixels of the final decrypted shares. Thus, it satisfies the goodness criteria of the image encryption scheme.

6.5. Security analysis

6.5.1. Key's space

For any Cryptosystem, the set of all possible keys used to generate a key for encoding process refers to the key space. The key space is considered as one of the most important attributes that supports the immenseness and robustness of a cryptosystem. Large key space of the cryptosystem effectively resists attackers and pro-

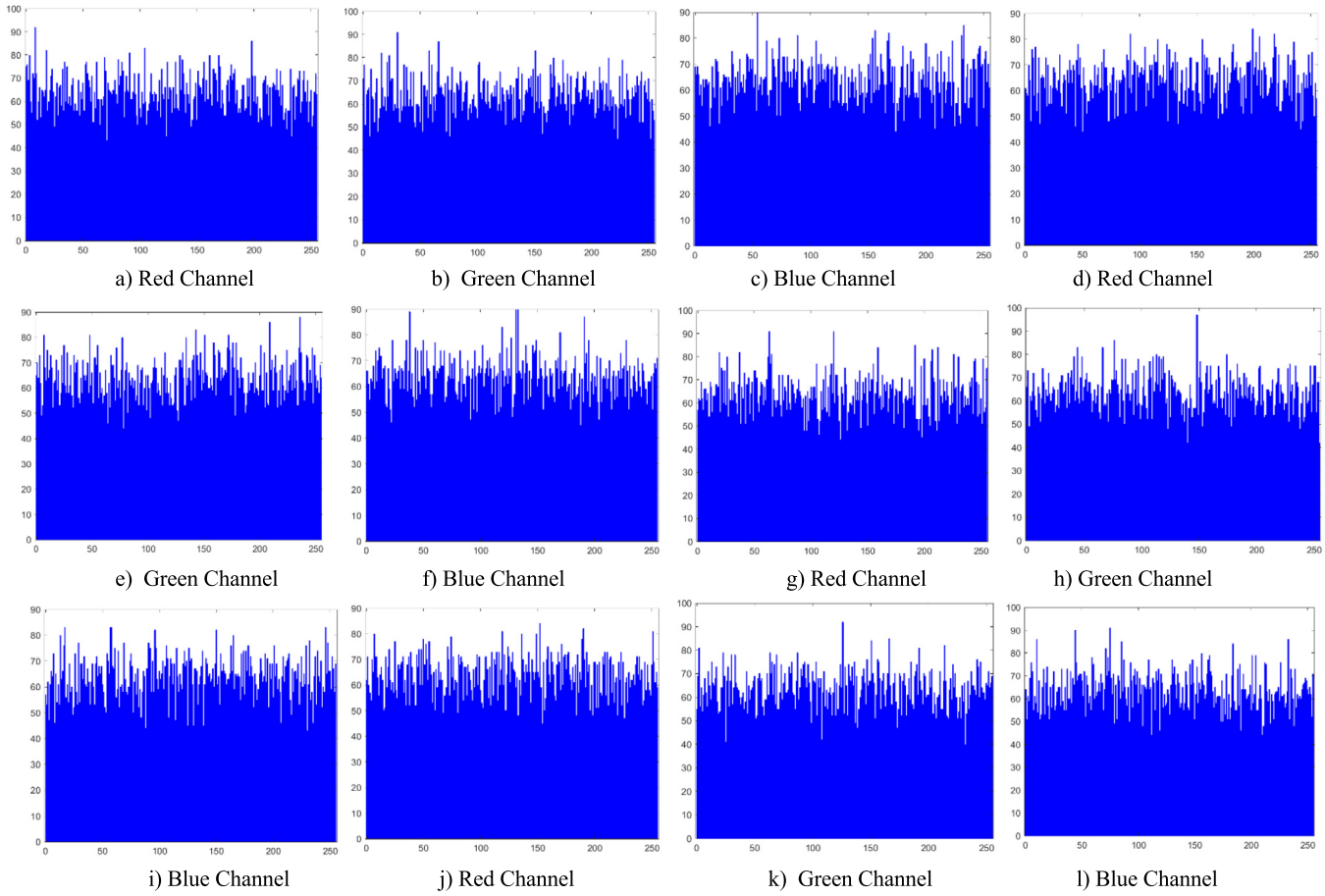


Fig. 9. (a)-(c) Histogram of the first encrypted share (shown in Fig. 5 (g)), (d)-(f) Histogram of the second encrypted share (shown in Fig. 5(h)), (g)-(i) Histogram of the third encrypted share (shown in Fig. 5(i)), (j)-(l) Histogram of the first encrypted share (shown in Fig. 5(j)).

Table 2
Pixels Correlations Results for gray Lena, Pepper and final encrypted shared images.

Image	Direction		
	Vertical	Horizontal	Diagonal
Plain gray Lena image (Fig. 2(a))	0.9739	0.9862	0.9618
Cipher image of share 1 (Fig. 2(g))	−0.0036	0.0072	0.0232
Cipher image of share 2 (Fig. 2(h))	0.0438	−0.0356	−0.0294
Cipher image of share 3 (Fig. 2(i))	0.0034	−0.0040	−0.0249
Cipher image of share 4 (Fig. 2(j))	−0.0212	0.0526	−0.0049
Plain gray Pepper image (Fig. 3(a))	0.9624	0.9456	0.9149
Cipher image of share 1 (Fig. 3(g))	0.0159	−0.0178	0.0221
Cipher image of share 2 (Fig. 3(h))	−0.0072	−0.0152	−0.0111
Cipher image of share 3 (Fig. 3(i))	−0.0068	−0.0228	−0.0168
Cipher image of share 4 (Fig. 3(j))	−0.0326	0.0012	0.0245

vides robustness against a known-plaintext, chosen-ciphertext, and brute-force attacks (Mishra et al., 2015; Shafique and Shahid, 2018; Zhang, 2018). In the proposed scheme, two key matrices are used, and both of them are multiplicative. The key space of the first key is generated based on choosing a two integer numbers *a* & *b*, belonging to [0,255]. Then, the size of the randomly generated key matrix should be 4×4, and accordingly, the elements of the generated key matrix should belong to [*a, b*]. The second phase is to generate the second key matrix based on the first generated key matrix. Here, the least possible key space can be obtained by *n (n-r)*, where *n* equals to 256 and *r* is the first chosen number. Here, each possibility of the least possible key space is likely to have many actual generated keys. This is to say that the key space of the proposed method is enormous. Thus, the exhaustive keys research is not possible for the hackers. Furthermore, the proposed method is free from any known-plaintext attack, unlike the classical Hill Cipher algorithm.

6.5.2. Key sensitivity analysis

To prevent breaking the cryptosystem by any hacker, high sensitivity is required since the robustness of any cryptosystem is totally based on the sensitivity of keys (Fu et al., 2018). With the use of RG, the proposed method can broadly be a secured method in a sense that the profile of the secret image cannot be recovered as shown in Fig. 2(k, l, m, and n) and Fig. 3(k, l, m, and n).With respect to the keys of new Two-Key Hill Cipher algorithm, only the first key can be sent to the participants or to the combiner while the second key can be generated at the decryption side. Moreover, the chosen parameters *a & b* as well as the two generated key matrices are sensitive. Therefore, the sensitivity analysis of the proposed method confirms that the keys are highly sensitive. Table 4 shows the results of the current scheme in comparison with some recently published methods proposed for protecting the security of the secret image.

6.6. Cryptanalysis

The VC with additional security gained by Hill Cipher, there are only 256 possible plaintext numbers. In a Hill Cipher with 2×2 key matrix, there are 256^2 =65,536 possible plaintext row matrices, and with256^3 = 16777216 possible plaintext row matrices. Since the key matrix *K* for a Hill Cipher can be of any size (provided

Table 3
Pixels Correlations Results for color Lena, Pepper and final encrypted shared images.

Image	Direction	Channels		
		Red	Green	Blue
Plain color Lena image (Fig. 4(a))	Vertical	0.9483	0.9459	0.9203
	Horizontal	0.9728	0.9757	0.9529
	Diagonal	0.9208	0.9183	0.8898
Cipher image of share 1 (Fig. 4(g))	Vertical	0.0483	0.0168	0.0151
	Horizontal	0.0150	0.0319	−0.0020
	Diagonal	0.0275	0.0081	−0.0150
Cipher image of share 2 (Fig. 4(h))	Vertical	0.0089	0.0204	−0.0084
	Horizontal	0.0093	−0.0250	−0.0356
	Diagonal	−0.0109	−0.0204	−0.0376
Cipher image of share 3 (Fig. 4(i))	Vertical	−0.0098	−0.0159	0.0514
	Horizontal	−0.0183	−0.0351	0.0012
	Diagonal	0.0134	0.0119	−0.0297
Cipher image of share 4 (Fig. 4(j))	Vertical	0.0111	0.0382	−0.0020
	Horizontal	0.0036	−0.0122	−0.0045
	Diagonal	−0.0295	−0.0269	0.0079
Plain color Pepper image (Fig. 5(a))	Vertical	0.9625	0.9774	0.9509
	Horizontal	0.9607	0.9772	0.9585
	Diagonal	0.9203	0.9596	0.9164
Cipher image of share 1 (Fig. 5(g))	Vertical	0.0167	0.0036	−0.0111
	Horizontal	0.0166	−0.0105	−0.0016
	Diagonal	−0.0332	−0.0106	−0.0015
Cipher image of share 2 (Fig. 5(h))	Vertical	0.0315	−0.0268	0.0126
	Horizontal	0.0094	0.0083	0.0247
	Diagonal	−0.0231	0.0190	0.0012
Cipher image of share 3 (Fig. 5(i))	Vertical	0.0182	−0.0307	−0.0015
	Horizontal	0.0089	−0.0077	0.0352
	Diagonal	0.0317	0.0017	0.0178
Cipher image of share 4 (Fig. 5(j))	Vertical	−0.0283	−0.0259	−0.0131
	Horizontal	−0.0231	0.0084	−0.0072
	Diagonal	−0.0433	−0.0234	0.0203

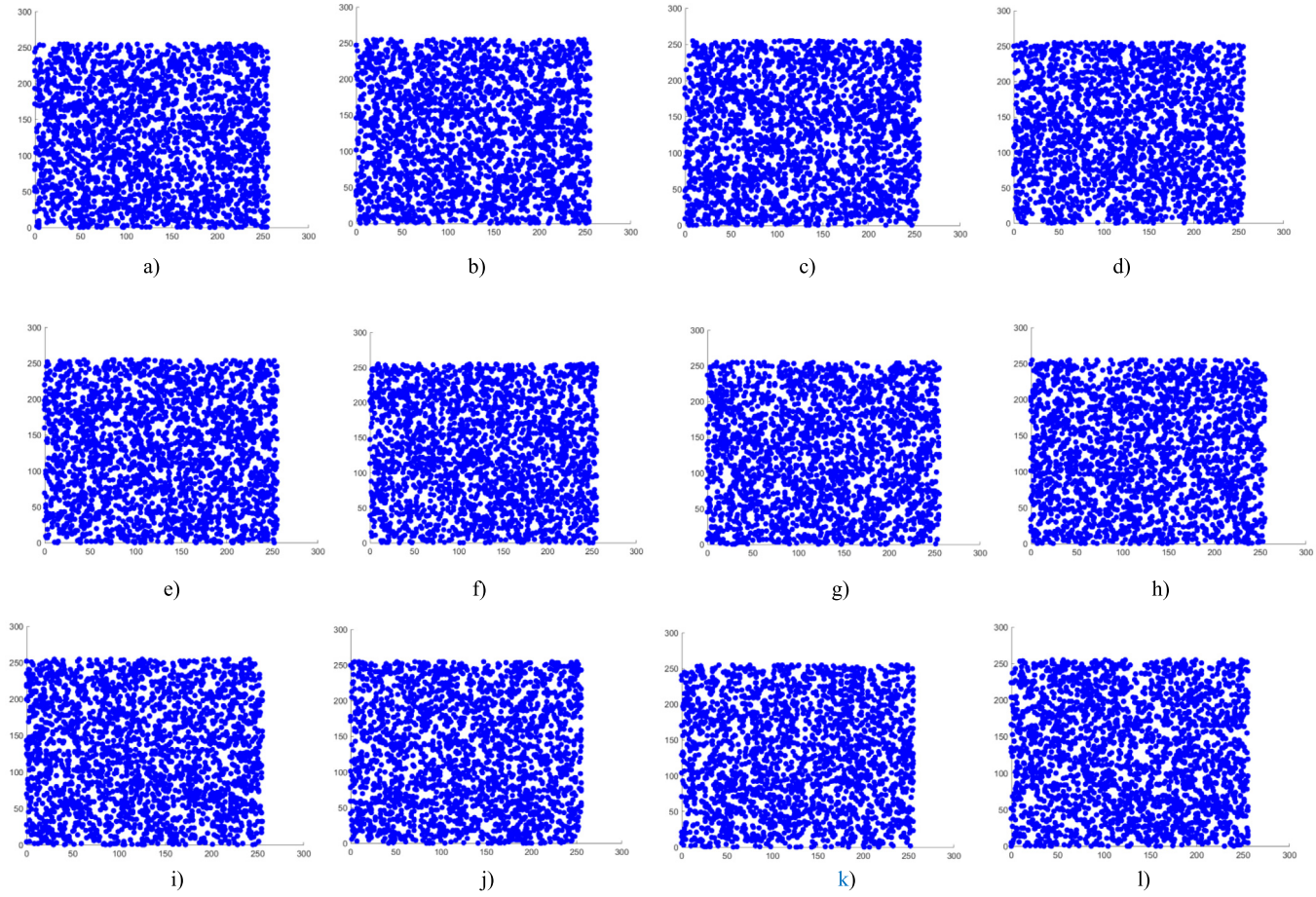


Fig. 10. Pixel correlation ((a) Vertical, (b) Horizontal, &(c) Diagonal) of share1 (Fig. 2(g)), Pixel correlation ((d) Vertical, (e) Horizontal, &(f) Diagonal) of share3 (Fig. 2(i)), Pixel correlation ((g) Vertical, (h) Horizontal, &(i) Diagonal) of share2 (Fig. 3(h)), Pixel correlation ((j) Vertical, (k) Horizontal, &(l) Diagonal) of share4 (Fig. 3(j)).

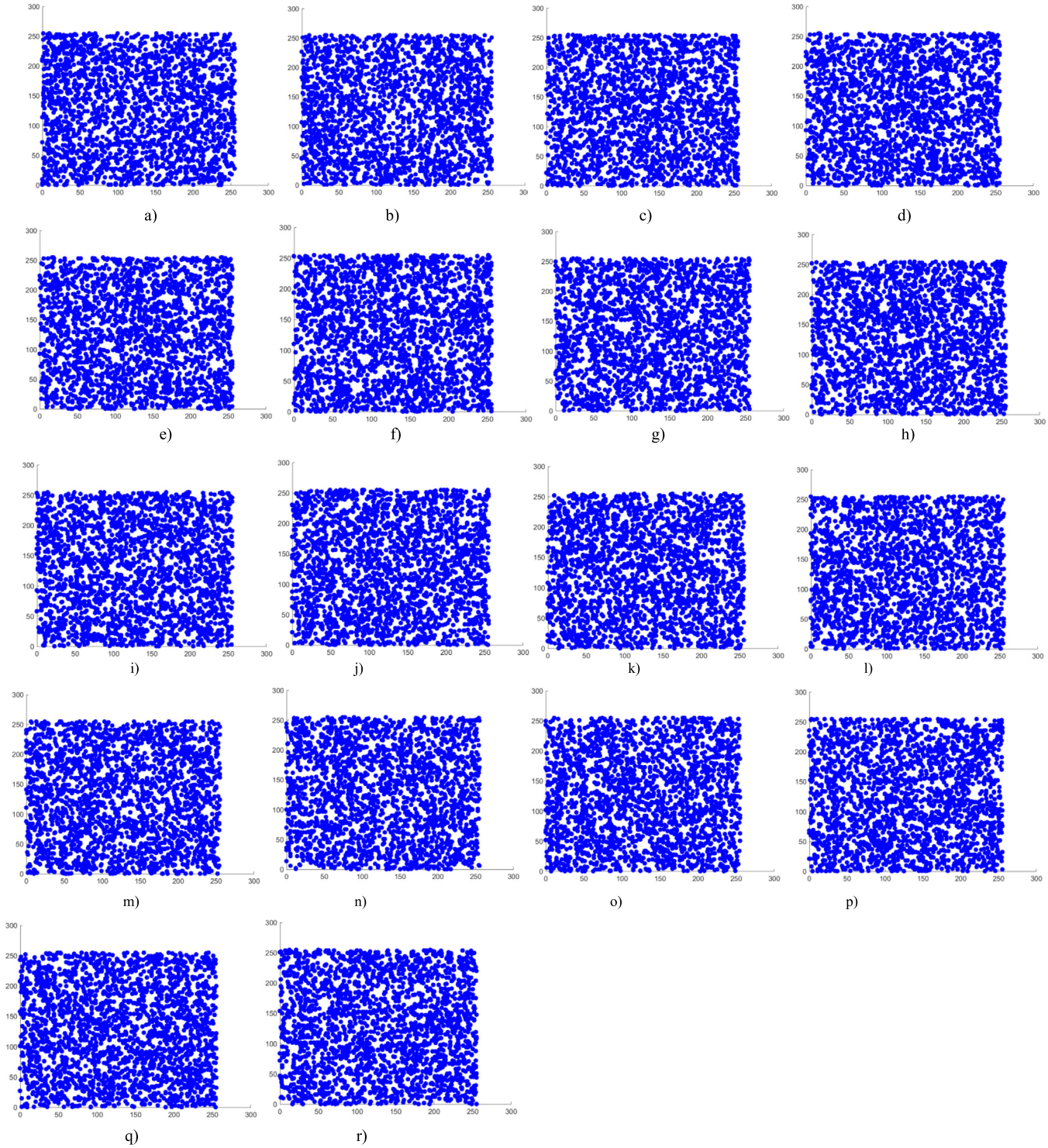


Fig. 11. Pixel correlation ((a) Vertical, (b) Horizontal, &(c) Diagonal) of Red Channel of share1 (Fig. 4(g)), Pixel correlation ((d) Vertical, (e) Horizontal, &(f) Diagonal) of Green Channel of share1 (Fig. 4(g)), Pixel correlation ((g) Vertical, (h) Horizontal, &(i) Diagonal) of Blue Channel of share1 (Fig. 4(g)), Pixel correlation ((j) Vertical, (k) Horizontal, &(l) Diagonal) of Red Channel of share2 (Fig. 4(h)), Pixel correlation ((m) Vertical, (n) Horizontal, &(o) Diagonal) of Green Channel of share2 (Fig. 4(h)), Pixel correlation ((p) Vertical, (q) Horizontal, &(r) Diagonal) of Red Channel of share2 (Fig. 4(h)).

K^{-1} mod 256 exists). It is to say that; a larger key matrix allows for more possible plaintext row matrices. Therefore, the security of Hill Cipher grows as the size of the key matrix increases.

In the proposed method with a 4×4 key matrix K, there are$256^4 = 4294967296$ possible plaintext row matrices. Since the key matrix K for the proposed method, K^{-1} mod 256 exists and *cof(K)* exists. Whereas the *Chen's* method (Chen, 2013) with 2×2 key matrix, there are only $256^2 = 65536$ possible plaintext row matrices. More precisely, by using a Hill Cipher with the $n \times n$ key matrix, the number of possible plaintext row matrices is256^n, a number that grows, and grows very quickly, as n increases. Accordingly, $n = 4$ in the proposed method whereas

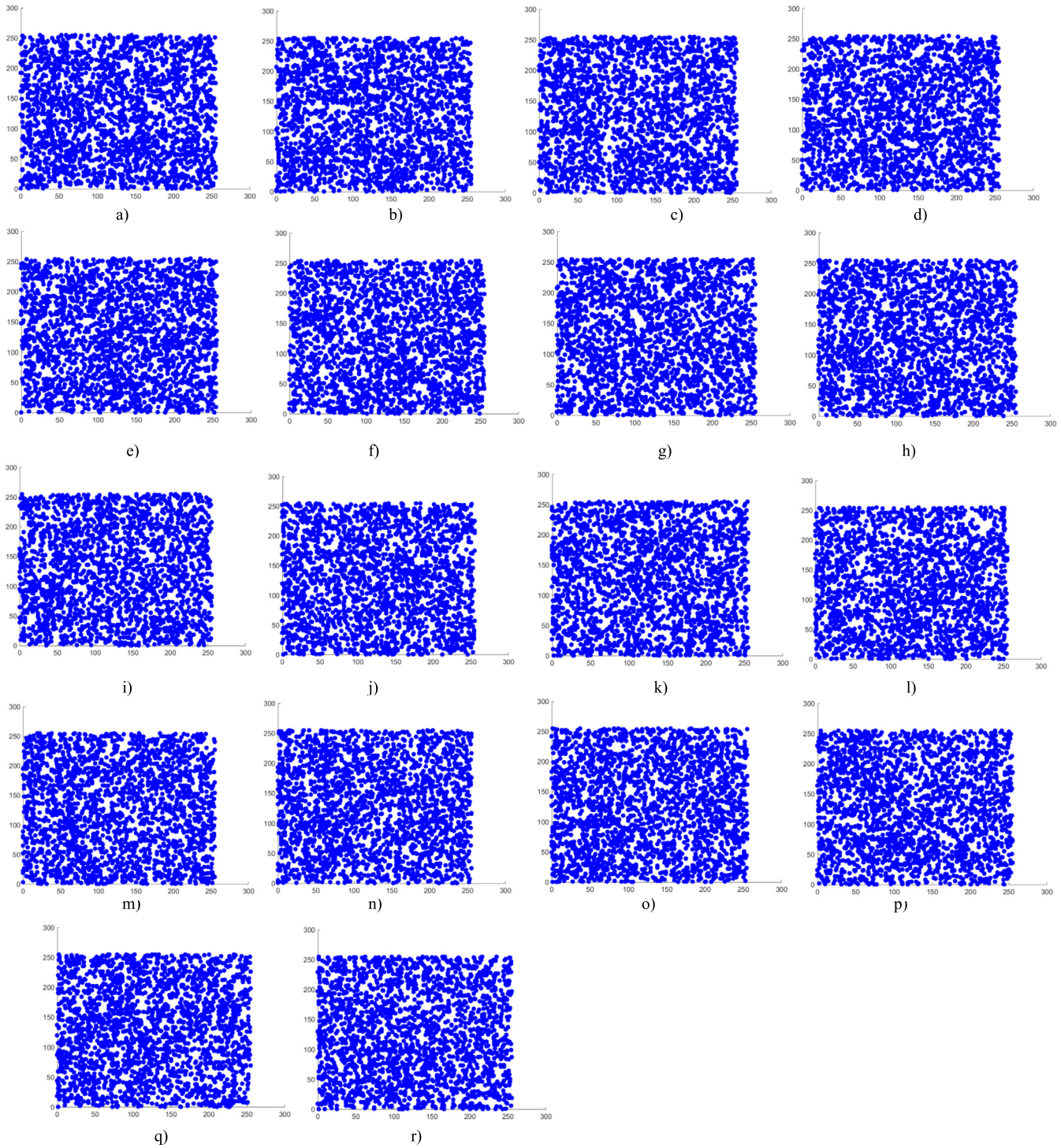


Fig. 12. Pixel correlation ((a)Vertical, (b) Horizontal, &(c) Diagonal) of Red Channel of share3 (Fig. 5(i)), Pixel correlation ((d) Vertical, (e) Horizontal, &(f) Diagonal) of Green Channel of share1 (Fig. 5(i)), Pixel correlation ((g) Vertical, (h) Horizontal, &(i) Diagonal) of Blue Channel of share1 (Fig. 5(i)), Pixel correlation ((j) Vertical, (k) Horizontal, &(l) Diagonal) of Red Channel of share4 (Fig. 5(j)), Pixel correlation ((m) Vertical, (n) Horizontal, &(o) Diagonal) of Green Channel of share2 (Fig. 5(j)), Pixel correlation ((p) Vertical, (q) Horizontal, &(r) Diagonal) of Red Channel of share2 (Fig. 5(j)).

Table 4
The results in comparison with some recent published methods.

Scheme	Secret image	Shared images	Recovered image	Sensitivity	Robustness
Chen's Scheme (Chen, 2013)	Gray-level	(m × n/2)	Lossless	Insensitive	Infirm
Yadav & Ojha's Scheme (Yadav and Ojha, 2013)	Gray-level	(m × n)	Lossless	Insensitive	Infirm
Shankar & Eswaran's Scheme (Shankar and Eswaran, 2015)	Color	(m × n)	Lossless	Sensitive	Robust
Shankar & Eswaran's Scheme (Shankar and Eswaran, 2017)	Color	(m × n)	Lossy	Insensitive	Robust
The Proposed Scheme	Gray-level, color	(m × n/4)	Lossless	Highly sensitive	Robust

equal to 2 in the *Chen's* method (Chen, 2013). Thus, the proposed method is more secure than the *Chen's* method (Chen, 2013). The emphasis here is on comparing our method with Chen's method because they were designed on the basis of linear equations.

6.6.1. Brute-Force attack

With respect to brute force attack on a Hill Cipher with the $n \times n$ key matrix, would require trying to decrypt the ciphertext assuming a much larger number of possible keys. However, the number of possible n × n matrices with entries in Z_{256} is256^n. In *Chen's* method (Chen, 2013), the number of possible 2×2 matrices is $256^4 = 4294967296$, and while many of these matrices would not have an inverse modulo 256 and thus is not a valid key matrix for a Hill Cipher. A brute force attack on the proposed method with 4×4 key matrix would require some level of testing with up to a maximum of near$256^{16} = 3.403E + 38$ matrices multiplying by$256^{16} = 3.403E + 38$ of k2. So, the proposed method is much more resistant to brute force attack than the *Chen's* method (Chen, 2013). In fact, the accentuation here is on comparing our method with Chen's method since they were designed on the basis of linear equations. For other compared schemes, which are designed utilizing AES & ECC, it can be noticed that the proposed scheme enjoys the same resistant to brute force attack of AES & ECC. However, Table 5 and Fig. 13 demonstrate the superiority of the proposed method.

6.7. Time complexity

In spite of the proposed method including two phases for encryption with different keys, the implementation of the current method and the recent methods compared in Table 2 has a runtime of at least $O(n^2)$ for the same length of n. Expectedly, the proposed method implementation is significantly faster than the implementation of the compared methods. As shown in Fig. 14, it is evident that the proposed method is very fast.

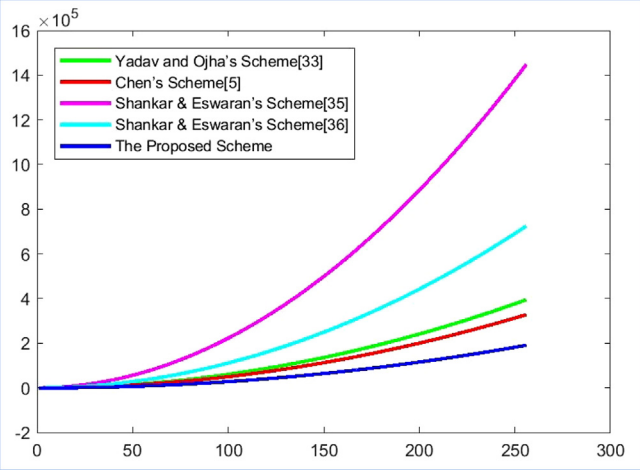


Fig. 14. Comparison of time complexity.

6.8. Theoretical analysis

The formal definition of the proposed scheme is given in Definition 1 as follows:

Definition 1. *Let S be the secret image is encoded by the* (*n*,*n*) *TKHC-based VC with RG into n shares denoted by E1 , ..., En which XORed with a master grid M. the scheme is a valid construction of* (*n*, *n*) *TKHC-based VC with RG, the following conditions must be met*:

- By XORing all *n* shares with *M* and decrypting it with the right keys, the secret image is visually recovered.
- The secret cannot be disclosed by insufficient number of shares.
- The XORed up result by any *n* shares gives no clue about the secret.

Table 5
The results of cryptanalysis and brute force attack comparison.

Scheme	Size of Key Matrix	Cryptanalysis Possible Plaintext Row Matrices	Brute Force Attack Maximum Level of Required Test
Chen's Scheme (Chen, 2013)	2 × 2	256^2	256^4
Yadav & Ojha's Scheme (Yadav and Ojha, 2013)	1 × 1	256^1	256^1
Shankar & Eswaran's Scheme (Shankar and Eswaran, 2015)	4 × 4	256^4	256^{16}
Shankar & Eswaran's Scheme (Shankar and Eswaran, February 2017)	4 × 4	256^4	256^{16}
The Proposed Scheme	4 × 4	256^4	256^{16}

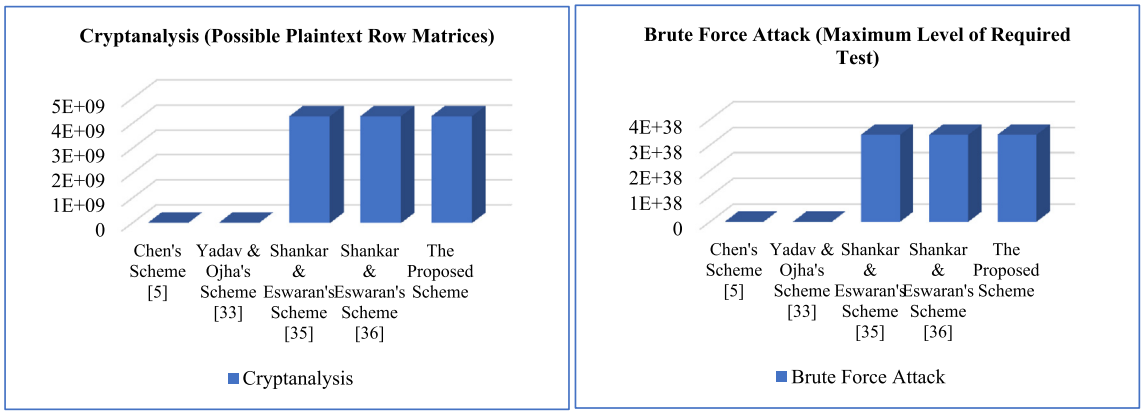


Fig. 13. Comparison of Cryptanalysis and resistance to brute force attack.

- The master grid M is a random grid. Therefore, XORing any share with M is also a random grid and gives no clue about the profile of secret.

We further prove that the proposed scheme is valid construction which satisfies the security conditions of definition 1.

Lemma 1. *The proposed method is a secure access structure. The deciphered grids* $D(\overbrace{E_1 \oplus \mathrm{M}}^{d_1}, \ldots\ldots, \overbrace{E_t \oplus \mathrm{M}}^{d_t})$, $1 \leqslant \mathrm{t} < n$ *by insufficient number of shares cannot disclose the secret.*

Proof. *In the proposed method, four shares are constructed by* (4, 4) *TKHC-based VC with RG. Obviously, the associated four pixels p*1, *p*2, *p*3, *and p*4 *are independent but encrypted together as shown in eq.* (4) *and eq.* (5) *then distributed to four shares as* $\mathrm{E}_1(\mathrm{i},\mathrm{j}) = \mathrm{C}_1$, $\mathrm{E}_2(\mathrm{i},\mathrm{j}) = \mathrm{C}_2$, $\mathrm{E}_3(\mathrm{i},\mathrm{j}) = \mathrm{C}_3$, $\mathrm{E}_4(\mathrm{i},\mathrm{j}) = \mathrm{C}_4$.

Clearly, the secret can completely be recovered if and only if $\mathrm{Encryption}(\frac{\mathrm{NP}}{\mathrm{NS}}) = \mathrm{Decryption}(\frac{\mathrm{NS}}{\mathrm{NP}}) = 1$, where *NP* denotes the required number of associated pixels for encryption and decryption processes and *NS* refers to the number of shares. Suppose, we have only three shares out of four to recover the secret. Therefore, $\mathrm{Encryption}(\frac{4}{4}) = 1$ and $\mathrm{Decryption}(\frac{3}{4}) \neq 1$. Thus, the insufficient number of shares leads to insufficient number of required associated pixels and the secret cannot completely be recovered.

Lemma 2. *The XORing up result of every share with M gives no clue about the secret*: *XOR* $((E_1 \oplus \mathrm{M}), \ldots, (E_t \oplus M))$, *t = n.*

Proof. *Let S is a secret image encrypted by two keys (k1,k2) then XORed with a random grid M as C = XOR((E(k2,E(K1,S)),M). indeed, the decryption process requires that the keys be applied in reverse order*: *S = XOR((D(k1,E(K2,C)),M). so XOR (C,M) without applying the required keys the secret cannot completely be recovered.*

With respect to RG in the proposed scheme, we refer to a gray pixel m as a random pixel if the choice for m in a master grid M is totally random; or equivalently, the probability for m to be 0,1, …, 255 is equal,

$$\mathrm{Prob}(m = 0) = \mathrm{Prob}(m = 1) = \ldots = \mathrm{Prob}(255) = \frac{1}{256} \tag{19}$$

where m = 0, …, 255 denotes the intensity of m pixel in a gray level image. Thus, the average light transmission of random pixel m is $\frac{1}{256}$ denoted as

$$t(m) = \frac{1}{256} \tag{20}$$

Definition 2. *M is a gray random grid if each pixel m in M is a gray random pixel.*

With respect to *M*, the number of light pixels is probabilistically the same as that of dark ones. Therefore, the average light transmission of *M* is also $\frac{1}{256}$,denoted as

$$\mathrm{T(M)} = \frac{1}{256} \tag{21}$$

By applying the threshold concept, the value of a light pixel is 1 and the value of a black pixel is 0 by threshold *Th =128*. Thus, the average light transmission of *M* is $\frac{1}{2}$,denoted as

$$\mathrm{T(M)} = \frac{1}{2} \tag{22}$$

In the proposed method, let $\oplus$ denote "XOR" operation which describes the relation of XORing two grids pixels. Obviously, $m \oplus m$ $(M \oplus M)$ is completely the same as *m(M)* for each pixel m in M which denoted as

$$\mathrm{t(m \oplus m) = T(M \oplus M)} = \frac{1}{256} \tag{23}$$

For a systematic grid, the number of light pixels is probabilistically not same as that of dark ones. So, is XORing a systematic grid with *M* is a random grid and gives no clue about the profile of secret?

Lemma 3. *If M and E are two independent random and systematic grid, respectively with* $T(M) = \lambda_1$ *and* $T(E) = \lambda_2$, *the* $M \oplus E$ *is also random grid if* $T(M \oplus E) = \lambda_1\lambda_2$, *where* $0 < \lambda_1 < 1$ *and* $0 < \lambda_2 < 1$.

Proof. *Let m = M[I,j]* $\in$ *M and e = E[I,j]* $\in$ *E, be the corresponding pixels if and only if i = i' and j = j' which leads to say that the order of M and E does not affect the XORed results as*

$$M \oplus E = E \oplus M \tag{24}$$

According to XOR truth table for two grids, there are only two outcomes among four possible combinations of $m \oplus e$ showing transparency. Since the four possible combinations occur with an equal probability, the probability of $m \oplus \mathrm{e}$ to be light is $\frac{1}{2}$. Therefore, the average light transmission of $M \oplus E$ is $\frac{1}{2}$. Here, the $t(m) = \mathrm{Prob}(m = 0) = \lambda_1$ and $t(e) = \mathrm{Prob}(e = 0) = \lambda_2$. Due to that *M* and *E* independent, $m \oplus \mathrm{e} = 0$ if and only if *m = 0(1)* and *e = 0 (1)*. Thus,

$$\begin{aligned}(m \oplus e) &= \mathrm{Prob}(m \oplus \mathrm{e} = 0) = \mathrm{Prob}(\mathrm{m} = 0(1) \mathrm{and}\, \mathrm{e} = 0(1)) \\ &= \mathrm{Prob}(\mathrm{m} = 0(1)) \times \mathrm{Prob}(\mathrm{e} = 0(1)) = \lambda_1\lambda_2.\end{aligned}$$

This is to say that XORing any systematic grid with random grid generates a random grid as shown in Figs. 2, 3, 4 & 5(g, h, i, and j). Further, the major merits of the proposed scheme can be represented as follows: (1) It can be applied to gray-level and RGB images. (2) With the use of the new TKHC algorithm, it is free from known-plaintext attack problem. (3) The generated shared images have a smaller size equals to ¼ of the size of the original secret image, which saves the space of the participants. (4) Applying TKHC algorithm and RG method dramatically increases the security of the secret image in a sense that it prevents any hacker to obtain the information of the secret image from any one of the shared images. (5) It is so resistant to the brute force attack due to using two keys. (6) The RG and the first key cannot recover the secret image but only its profile. (7) The proposed method is free from the problem of the noninvertible matrix of the classical Hill Cipher algorithm. (8) By using the right keys and RG, the original secret image can be recovered without any distortion. (9) And finally, it can be implemented easily and fast in regard to the time complexity.

7. Conclusion

To conclude, a new image sharing method has been proposed for gray-level and RGB images security. It is based on TKHC algorithm proposed in this paper. The two key matrices belonging to [0,255] rang depends on two chosen integer numbers from the same rang, to provide an enormous key space for the proposed method. Besides, sending only one key for the encryption side and in this case if it is held by the attacker, the attacker will not be able to recover the original information with one key. Furthermore, the proposed scheme provides security of gray-level and RGB images without any impairment of information because of

the correct values of MSE, PSNR, UIQ, MD, and AD equaling to 'zero', 'infinity', '1′,'zero', and 'zero', respectively. In addition, for both the original and the recovered images, the equal values of entropy, SD, and MSDR have been obtained. The pixel correlation towards their ideal values and the encrypted shares content is random-like and perfectly have uniform histograms. In addition, the proposed scheme decreases the overall complexity to increase the overall possibility for practical applications of VC. The security and statistical analysis including the theory analysis and experimental demonstration effectively ensure the immenseness and robustness of the present method to withstand the brute-force attack. Briefly, the performance of the proposed scheme is better than the compared schemes. Therefore, it can be used to secure the transmission of visual information through less channel by using the leak of the internet. It can also be appropriate and effective in digital forensic, military, and medical applications. The future work can be extended to apply the characteristics of lightweight Cryptography to be merged with the VC and distribute the keys using the concept of secret sharing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Acharya, B., Panigrahy, S.K., Patra, S.K., Panda, G., 2009. Image encryption using advanced hill cipher algorithm. Int. J. Recent Trends Eng. 1 (1).

Ahmad, M., Doja, M.N., Beg, M.S., 2018. Security analysis and enhancements of an image cryptosystem based on hyperchaotic system. J. King Saud Univ.-Comput. Information Sci.

Babu, J.J.J., Sudha, G.F., 2016. Adaptive speckle reduction in ultrasound images using fuzzy logic on Coefficient of Variation. Biomed. Signal Process. Control 23, 93–103.

Bibhudendra, A. et al., 2008. A Novel Cryptosystem Using Matrix Transformation. SPIT-IEEE Colloquium and International Conference 4, 92–95.

Blakley, G.R., 1979, June. Safeguarding cryptographic keys. In Proceedings of the national computer conference (Vol. 48, No. 313).

Bora, S., Ojha, A., 2015, July. Analysis and combination of positive aspects of threshold RG based VSS schemes. In: Science and Information Conference (SAI), 2015 (pp. 1192-1200). IEEE.

Chen, W.K., 2013. Image sharing method for gray-level images. J. Syst. Softw. 86 (2), 581–585.

Chen, C.Y., Chen, C.H., Chen, C.H., Lin, K.P., 2016. An automatic filtering convergence method for iterative impulse noise filters based on PSNR checking and filtered pixels detection. Expert Syst. Appl. 63, 198–207.

Chen, T.H., Tsao, K.H., 2009. Visual secret sharing by random grids revisited. Pattern Recogn. 42 (9), 2203–2217.

Chen, J.X., Zhu, Z.L., Fu, C., Zhang, L.B., Zhang, Y., 2015. An image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach. Commun. Nonlinear Sci. Numer. Simul. 23 (1–3), 294–310.

Ching-Nung, Y.A.N.G., Tse-Shih, C.H.E.N., 2006. New size-reduced visual secret sharing schemes with half reduction of shadow size. IEICE Trans. Fundamentals Electronics, Commun. Comput. Sci. 89 (2), 620–625.

Ece, C., Mullana, M.M.U., 2011. Image quality assessment techniques in spatial domain. IJCST 2 (3).

Enayatifar, R., Abdullah, A.H., Isnin, I.F., 2014. Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. Opt. Lasers Eng. 56, 83–93.

Fang, W.P., 2008. Friendly progressive visual secret sharing. Pattern Recogn. 41 (4), 1410–1414.

Fu, C., Zhang, G.Y., Zhu, M., Chen, Z., Lei, W.M., 2018. A New Chaos-Based Color Image Encryption Scheme with an Efficient Substitution Keystream Generation Strategy. Security and Communication Networks, 2018.

Hodeish, M.E., Humbe, V.T., 2015, January. A (2, 2) secret sharing scheme for visual cryptography without Pixel Expansion. In: 2015 IEEE International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO).

Hodeish, M.E., Humbe, V.T., 2014. State-of-the-Art Visual Cryptography Schemes. Int. J. Electronics Commun. Comput. Eng. 5, 412–420.

Hodeish, M.E., Bukauskas, L., Humbe, V.T., 2016. An Optimal (k, n) Visual Secret Sharing Scheme for Information Security. Procedia Comput. Sci. 93, 760–767.

Hou, Y.C., 2003. Visual cryptography for color images. Pattern Recogn. 36 (7), 1619–1629.

Kafri, O., Keren, E., 1987. Encryption of pictures and shapes by random grids. Opt. Lett. 12 (6), 377–379.

Kandar, S., Chaudhuri, D., Bhattacharjee, A., Dhara, B.C., 2019. Image encryption using sequence generated by cyclic group. J. Information Security Appl. 44, 117–129.

Kanso, A., Ghebleh, M., 2018. An efficient lossless secret sharing scheme for medical images. J. Vis. Commun. Image Represent. 56, 245–255.

King, O.D., Gaborit, P., 2007. Binary templates for comma-free DNA codes. Discrete Appl. Math. 155 (6–7), 831–839.

Kumar, V., Gupta, P., 2012. Importance of statistical measures in digital image processing. Int. J. Emerging Technol. Adv. Eng. 2 (8), 56–62.

Liu, F., Wu, C.K., Lin, X.J., 2009. The alignment problem of visual cryptography schemes. Des. Codes Crypt. 50 (2), 215–227.

Lukac, R., Plataniotis, K.N., 2005. Bit-level based secret sharing for image encryption. Pattern Recogn. 38 (5), 767–772.

Marwan, M., Kartit, A., Ouahmane, H., 2018. A Cloud Based Solution for Collaborative and Secure Sharing of Medical Data. Int. J. Enterprise Information Syst. (IJEIS) 14 (3), 128–145.

Marwan, M., AlShahwan, F., Sifou, F., Kartit, A., Ouahmane, H., 2019. Improving the Security of Cloud-based Medical Image Storage. Eng. Lett. 27 (1).

Mishra, D.C., Sharma, R.K., Ranjan, R., Hanmandlu, M., 2015. Security of RGB image data by affine hill cipher over and domains with Arnold transform. Optik-Int. J. Light Electron Optics 126 (23), 3812–3822.

Muttoo, S.K., Aggarwal, D., Ahuja, B., 2011. A secure image encryption algorithm based on hill cipher system. Bull. Electrical Eng. Informatics 1 (1), 51–60.

Naor, M., Shamir, A., 1995. Visual cryptography. Lect. Notes Comput. Sci. 950 (1), 1–12.

Pal, J.K., Mandal, J.K., Dasgupta, K., 2010. a (2, n) visual cryptographic technique for banking applications. Int. J. Network Security Appl. (IJNSA) 2 (4), 118–127.

Rajkumar, S., Malathi, G., 2016. A comparative analysis on image quality assessment for real time satellite images. Indian J. Sci. Technol. 9, 1–11.

Rose, A.A., Thampi, S.M., 2015. A Secure Verifiable Scheme for Secret Image Sharing. Procedia Comput. Sci. 58, 140–150.

Ryo, I.T.O., Kuwakado, H., Tanaka, H., 1999. Image size invariant visual cryptography. IEICE Trans. Fundamentals Electronics Commun. Comput. Sci. 82 (10), 2172–2177.

Shafique, A., Shahid, J., 2018. Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps. Eur. Phys. J. Plus 133 (8), 331.

Shamir, A., 1979. How to share a secret. Commun. ACM 22 (11), 612–613.

Shankar, K., Eswaran, P., 2015. Sharing a Secret Image with Encapsulated Shares in Visual Cryptography. Procedia Comput. Sci. 70, 462–468.

Shankar, K., Eswaran, P., February 2017. RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography. China Commun. 14 (2), 118–130. https://doi.org/10.1109/CC.2017.7868160.

Shetty, S., Abraham, M.P., April 2015. A Secure Visual Cryptography Scheme for Sharing Secret Image using RSA. Int. J. Innovative Res. Comput. Commun. Eng. 3 (4), 3331–3336.

Shyu, S.J., 2007. Image encryption by random grids. Pattern Recogn. 40 (3), 1014–1031.

Shyu, S.J., 2009. Image encryption by multiple random grids. Pattern Recogn. 42 (7), 1582–1596.

Somaraj, S., Hussain, M.A., 2015. Performance and Security Analysis for image encryption using Key image. Indian J. Sci. Technol. 8 (35).

Tuncer, T., Avci, E., 2016. A reversible data hiding algorithm based on probabilistic DNA-XOR secret sharing scheme for color images. Displays 41, 1–8.

Tuyls, P., Hollmann, H.D., Lint, J.V., Tolhuizen, L.M.G.M., 2005. XOR-based visual cryptography schemes. Des. Codes Crypt. 37 (1), 169–186.

Tuyls, P., Hollmann, H.D., Van Lint, J.H., Tolhuizen, L.M.G.M., 2005. XOR-based visual cryptography schemes. Des. Codes Crypt. 37 (1), 169–186.

Umamageswari, A., Ukrit, M.F., Suresh, G.R., 2011. A survey on security in medical image communication. Int. J. Comput. Appl. 30 (3), 41–45.

Wang, Z., Bovik, A.C., 2002. A universal image quality index. IEEE Signal Process Lett. 9 (3), 81–84.

Wang, D.S., Dong, L., 2011. XOR-based visual cryptography. In Visual Cryptography and Secret Image Sharing, 155.

Wang, C., Shen, H.W., 2011. Information thedory in scientific visualization. Entropy 13 (1), 254–273.

Yadav, G.S., Ojha, A., 2013, December. A novel visual cryptography scheme based on substitution cipher. In: Image Information Processing (ICIIP), 2013 IEEE Second International Conference on (pp. 640-643). IEEE.

Yang, C.N., 2004. New visual secret sharing schemes using probabilistic method. Pattern Recogn. Lett. 25 (4), 481–494.

Yang, C.N., Chen, T.S., 2005. Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion. Pattern Recogn. Lett. 26 (2), 193–206.

Yang, C.N., Wang, D.S., 2014. Property analysis of XOR-based visual cryptography. IEEE Trans. Circuits Syst. Video Technol. 24 (2), 189–197.

Zhang, Y., 2018. The image encryption algorithm based on chaos and DNA computing. Multimedia Tools Appl., 1–27