Computing and Informatics, Vol. 38, 2019, 1272–1300, doi: 10.31577/cai_2019_6_1272

CELLULAR AUTOMATA BASED IMAGE AUTHENTICATION SCHEME USING EXTENDED VISUAL CRYPTOGRAPHY

Sonal Kukreja, Geeta Kasana, Singara Singh Kasana

Computer Science and Engineering Department
Thapar Institute of Engineering and Technology
Patiala, Punjab, India, 147004
e-mail: kukreja.sonal@gmail.com, {gkasana, singara}@thapar.edu

Abstract. Most of the Visual Cryptography based image authentication schemes hide the share and authentication data into cover images by using an additional data hiding process. This process increases the computational cost of the schemes. Pixel expansion, meaningless shares and use of codebook are other challenges in these schemes. To overcome these issues, an authentication scheme is proposed in which no embedding into the cover images is performed and meaningful authentication shares are created using the watermark and cover images. This makes the scheme completely imperceptible. The watermark can be retrieved just by superimposing these authentication shares, thus reducing the computational complexity at receiver's side. Cellular Automata is used to construct the master share that provides self-construction ability to the shares. The meaningful authentication shares help in enhancing the security of the scheme while size invariance saves transmission and storage cost. The scheme possesses the ability of tamper detection and its localization. Experimental results demonstrate the improved security and quality of the generated shares of the proposed scheme as compared to existing schemes.

Keywords: Image authentication, cellular automata, extended visual cryptography, watermarking, normalized Hamming similarity, PSNR, SSIM

1 INTRODUCTION

There have been tremendous advancements in data transmission technology in the past decade. The transmitted data can be easily recreated or tampered on the net-

work. Images are popular media used in data transmission. Hence protection and authentication of the images have gained a lot of attention in recent times. Protecting the integrity of image from modification by unauthorized users is called image authentication. Many image authentication schemes [11, 28] have been proposed in the literature that can be classified into two categories:

Digital signature based authentication: In this type of schemes [3, 4, 5, 8, 13, 20, 27, 36, 39, 40], a signature is generated from the image using a hash function. This signature is then embedded into the image. To verify authentication of the image, the signature is again calculated from the image using the same hash function and compared with the extracted signature. If both the signatures are same, the image is ensured to be authenticated else detected as tampered.

Watermarking based authentication: In watermarking based schemes [6, 25, 34, 37, 41], a watermark is embedded into the image. The resultant image is known as the marked image. On the receiver side, the watermark is extracted from the marked image. If the extracted watermark is different from the embedded one, the image is detected to be tampered. The original watermark is required for the comparison.

Apart from watermarking, cryptography also plays a crucial role to protect the data being transmitted. Naor and Shamir [19] proposed a modification of cryptography scheme to share a secret among a number of participants in such a way that every participant gets a part of the secret. This scheme is termed as Visual Cryptography (VC). A (k, n) VC is a scheme in which n random shares are constructed from the secret image and later, it can be reconstructed by superimposing authorized k or more shares where, $k \leq n$. No information can be retrieved from any subset of unauthorized shares or shares less than k. The shares created in this scheme were meaningless in appearance which may create a suspicion of some secret information being shared. Hence, this scheme was modified by Ateniese et al. [12] by creating meaningful shares and termed as Extended Visual Cryptography Scheme (EVCS). Here, when the meaningful shares are superimposed at the time of retrieval, the meaningful information disappears from them and the secret hidden inside the shares is recovered. Both of these schemes suffered from pixel expansion and low contrast in the generated shares.

Kafri and Keren [22] further enhanced the existing VC scheme by handling pixel expansion. Here, the binary secret image S is encoded into two random grids having the same size as that of S. This scheme removed pixel expansion but created random looking meaningless shares. Guo et al. [32] further improved the above scheme to create meaningful random grids. This scheme shows the benefits of random grid based VC to create meaningful shares with no pixel expansion. A probabilistic parameter β is used to make a trade-off of visual quality deterioration between share images and the decoded secret image. The larger value for β results in more visual-pleasing share images and less visual-pleasing decoded image, while smaller value for β results in less visual-pleasing share images and more visual-pleasing

decoded image. These schemes have been further enhanced in [43, 42] to improve the visual quality of generated shares.

The existing watermarking based authentication schemes [6, 25, 34, 37, 41] modify the original host image by embedding watermark into it, thereby resulting in the image quality degradation. Hence, in the past decade VC based authentication schemes [3, 5, 8, 13, 30, 36, 39] have gained a lot of attention as these schemes do not embed watermark into the host original image. The shares are constructed from the host image, and then these shares along with the authentication data or watermark are embedded into some other cover images which are transferred through the communication channels. This authentication data is extracted at the receiver's side and used to detect tamper in images. In all these schemes, an additional data hiding scheme is required to hide the constructed shares in some cover images, which increases complexity of these schemes.

The paper has been organized into the following Sections. Section 2 discusses the related works, Section 3 briefly reviews the concepts used in the proposed scheme like Cellular Automata (CA) and Wavelet Packet Decomposition (WPD). Section 4 presents the proposed authentication scheme. Experimental results and discussion are presented in Section 5, followed by conclusions in Section 6.

2 RELATED WORKS

In past few years, many VC based authentication schemes have been proposed that are briefly discussed in this section. In 2004, Lin et al. [5] proposed a VC based authentication scheme in which the shares are generated from the secret image using a polynomial. The image is divided into blocks and parity bits are calculated for every block. These parity bits are used as authentication data. This data together with shares are embedded into cover images. The drawback of this scheme is that the size of the cover image increases to four times the size of the secret image. Yang et al. [8] modified Lin et al. [5] to enhance authentication ability and quality of reconstructed image. This scheme also used polynomial based VC to generate n shares, but unlike the Lin's scheme [5] which set the value of the variable p to 251, this scheme set value of p to the Galois Field (GF), i.e. $p = g(x) = x^8 + x^4 + x^3 + x^1 + x^0$, which reduces the distortion in the received secret image. The extracted secret image has minimum distortion, but the cover image still remains four times the size of secret image. In some cases, this scheme provided fake authentication. Chang et al. [3] proposed another VC based authentication scheme using Chinese Remainder Theorem (CRT) that improved the authentication ability but the issue of pixel expansion still existed. The size of the cover image was relatively decreased as compared to the previous two schemes but it was still twice the size of the secret image. As this scheme uses CRT to evaluate the authentication bits, the computational complexity got increased. Another scheme was proposed by Lou et al. [9] in which the secret image is embedded inside two meaningful cover images, with no pixel expansion. This scheme provides larger em-

bedding capacity at the same transmission cost and better contrast of the generated shares.

The Two in One Secret Sharing Scheme [44] was proposed to provide good quality decoded images while performing decoding without use of any computations. But this scheme had security limitations as it created noisy shares. This scheme was improved by Srividhya et al. [30] by creating meaningful shares and enhancing its security by sharing an authentication image along with the secret image. The visual quality of the recovered image was improved due to usage of adaptive halftoning.

Eslami et al. [39] proposed an embedding scheme where the size of the block depends on the data to be hidden, hence the cover images are used efficiently for hiding the data. This scheme also included an authentication-chaining method which used 2 authentication bits and was able to achieve 15/16 tamper detection ability. But its disadvantage was that after encountering a tampered block, the rest of the image could not be tested. The authentication abilities for the increased block sizes were improved and the individual blocks of the stego image could also be authenticated in Ulutas et al. [13]. The visual quality of the stego images was also better as compared to the exisiting ones and could authenticate the rest of the stego image after encountering an altered block in the stego image.

Another VC scheme with authentication abilities, which could create meaningful shares, using the concepts of cellular automata, DWT and hash functions, was proposed by Wu et al. [36]. This scheme used an additional data hiding process to embed the shares inside cover images. This scheme had low visual quality for stego images and low tampered detection rate.

2.1 Motivation for the Proposed Work

From the study conducted on the existing watermarking based authentication schemes [7, 10, 15, 16, 18, 21, 24, 33, 35, 38], it is observed that the host image is modified to embed the watermark which degrades its visual quality. Also, to retrieve the watermark from the marked image, watermark extraction algorithm is followed, that increases the computation cost of the scheme. Pixel expansion, meaningless shares and use of codebook for share generation remain to be continuing challenges in the existing VC based authentication schemes [3, 4, 5, 8, 30, 36, 39]. These schemes generally require an additional data hiding process to conceal share and authentication bits into images, which increases the computation cost.

2.2 Contribution

The novelty of the proposed scheme is that the original host image is not modified for watermark embedding, instead authentication shares are constructed from host image using VC to store watermark information. This makes the scheme completely imperceptible. As no data hiding process is required to conceal these shares and authentication data into cover images, instead the meaningful authentication shares are constructed that resemble the cover images. This reduces complexity of the scheme

as, at the receiver's side, the watermark can be retrieved just by superimposing the shares.

Cellular Automata is used to create the master share, which eliminates pixel expansion and use of codebook, that saves transmission and storage cost. Also, to create meaningful authentication shares, a probabilistic parameter p is taken that decides the tradeoff between visual qualities of authentication shares and extracted watermark. This parameter makes the proposed scheme flexible for real-time applications. Meaningful shares enhance the security of the scheme, as random looking shares create suspicion that some secret information is hidden inside them. Use of VC further enhances security of the scheme, as watermark hidden in the shares cannot be detected or removed easily by any unauthorized entity but is retrieved only when k out of n shares are superimposed with each other.

Also, if an attacker gets access to the image, he can also construct the key and create the master share. The watermark cannot be retrieved until it is superimposed with some authorized shares stored with participants. This ensures the security of the proposed scheme. The key used to create master share can be constructed at both sender and receiver sides. Hence, there is no need to transmit it as side information thereby saving transmission cost.

3 PRELIMINARIES

In this section, Cellular Automata and Wavelet Packet Decomposition are discussed, which are used in the proposed scheme.

3.1 Cellular Automata

Cellular Automata (CA) is an array of entities which are known as cells. Every cell has a finite state having value either 0 or 1. Every cell has a neighborhood, which is usually described by its adjacent cells. The cells of the cellular automata exhibit following properties:

Grid: All cells of cellular automata arrange themselves in the form of a grid, as shown in Figure 1 a).

State: Every cell has a state. The number of state possibilities is typically finite. Every cell usually has 2 states: (0 and 1) or (ON and OFF) or (ALIVE and DEAD), as shown in Figure 1 b).

Neighborhood: Neighborhood involves the cell and its adjacent cells, as shown in Figure 1 c).

The state of the cell at an instant of time t, depends on its state at time $t-1$ along with the state of its neighbors at time $t-1$. A certain set of rules is followed to determine this current state of the cell on the basis of the previous states of the cell and its neighbors. This can be written as:

$$S(t) = F(S(t-1))$$

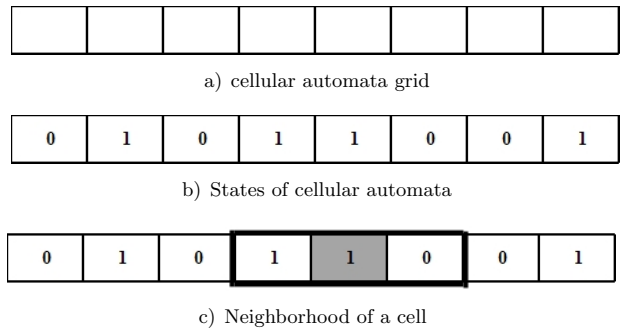


Figure 1. Representation of cellular automata

where $S(t)$ represents state of a cell at time t. Function F is determined by various rules described in [26]. This has been described in Figure 2.

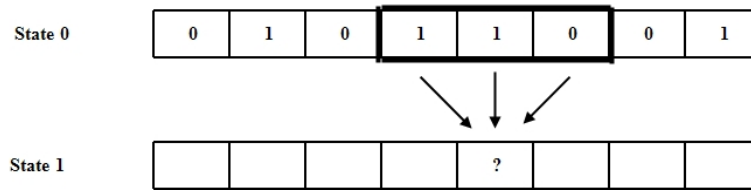


Figure 2. Transition of a cell from one state to the next state

The state configuration for every cell along with its right and left neighborhoods is represented by three bits, e.g. 100. Hence there are total eight possible neighborhood state configurations. Thus the rulesets are represented by eight bits, e.g. Rule 10001010, representing eight different state configurations. In the proposed scheme Rule 30 has been used. Generation of new state from the previous state using Rule 30 is shown in Figure 3.

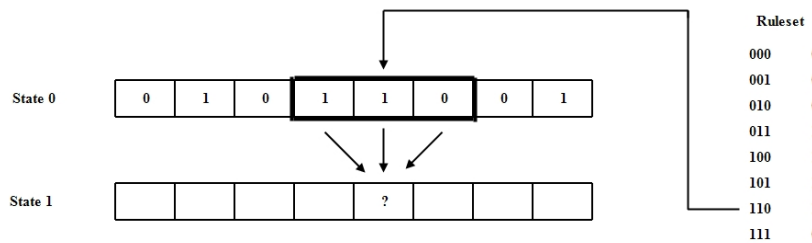


Figure 3. Use of Rule 30 to generate the next state

In terms of a Wolfram elementary CA, there are 256 possible rulesets. The ruleset used here is commonly referred to as Rule 30 because if the binary sequence

00011110 is converted to a decimal number, integer 30 is obtained. The generic CA is extended to two dimensions [26] which permits direct comparisons to real physical systems like crystal growth, chemical reaction-diffusion systems, simulation of turbulent flow patterns, etc. Two Dimensional CA supports variety of lattices and neighborhood structures like von-Neumann neighborhood where the center cell is surrounded by four neighbors, Moore neighborhood that has eight neighbors around the center cell, etc.

3.1.1 Rule 30

Rule 30 is an one dimensional binary CA rule introduced by Stephen Wolfram [31] in 1983. This rule has been used with VC in [26]. As stated in [2], Rule 30 is an exceptional legal rule that is highly periodic and random. Hence, this rule chosen in the proposed scheme helps in enhancing security. It is described in Figure 4. The figure shows all eight possible state configurations and their corresponding next state. The color of the next state is determined by the color of the cell and its neighbors in the previous state. As the binary representation of the outcome of the rule turns out to be 30, the rule is known as Rule 30. ($30 = 00011110_2$)

Figure 4. Representation of different state configurations and their next states using Rule 30

3.2 Wavelet Packet Decomposition

Wavelet Packet Decomposition (WPD), also known as Wavelet Packets, is a wavelet transform where discrete-time sampled signal is passed through more filters as compared to the Discrete Wavelet Transform (DWT) [17, 23]. In DWT, every level is calculated by passing previous wavelet approximation coefficients (low pass results) while in WPD, both detail (high pass results) and approximation coefficients are used to create the full binary tree.

The wavelet decomposition procedure splits the approximation coefficients into two parts. After splitting, we obtain a vector of approximation coefficients and a vector of detail coefficients, both at a coarser scale. The information lost between two successive approximations is captured in the detail coefficients. Then the new approximation coefficient vector is split again. In the wavelet packet approach, each detail coefficient vector is also decomposed into two parts as in approximation vector splitting. A pictorial representation of WPD over three levels is shown in Figure 5.

For n levels of decomposition the WPD produces 2^n different sets of coefficients (or nodes) as opposed to $n + 1$ sets for the DWT. However, due to the down sam-

pling process, the overall number of coefficients is still the same and there is no redundancy.

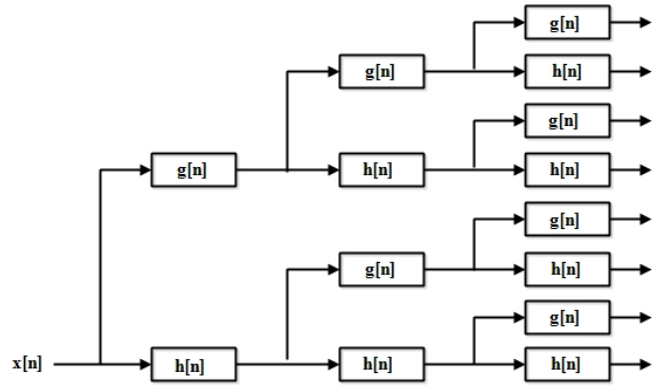


Figure 5. WPD over 3 levels. $g[n]$ is the low-pass approximation coefficients, $h[n]$ is the high-pass detail coefficients [17].

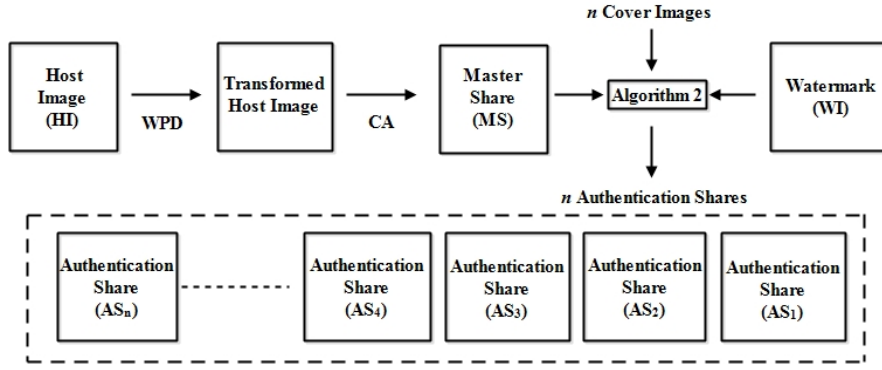
Wavelet Packets have a larger library of functions than wavelets, which help in representing different types of images efficiently. Especially the images that have smaller scale wavelet coefficients and carry very little energy, can be effectively represented by WPD. Thus, in the proposed scheme we have utilized WPD to create a master share that contains maximum features of the image, else it might lead to increase in false positives and false negatives in the tamper detection cases.

4 PROPOSED SCHEME

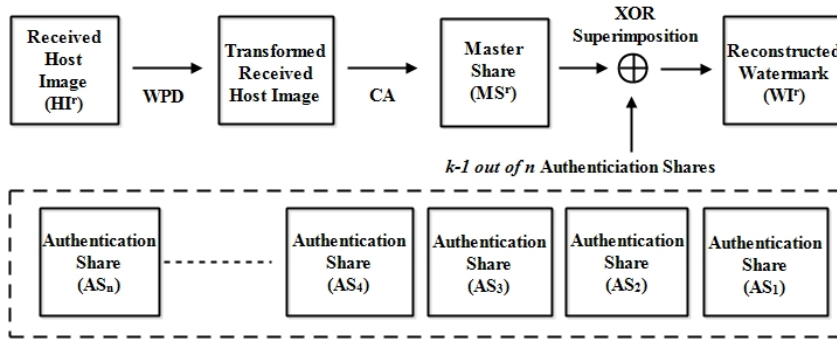
The proposed scheme consists of two phases: Share Generation Phase and Authentication Phase. It has been represented with the help of a block diagram shown in Figure 6.

4.1 Share Generation Phase

In the Share Generation Phase, a share is generated from the host image using WPD and CA. This share is referred as Master Share *(MS)*. This phase is described in Algorithm 1. The Host Image is divided into equal sized blocks. A basis set is produced for every block by applying WPD. The binary code for the average value of this set is considered as the key for the respective block. The obtained key is used to generate the corresponding *MS* block using CA with Rule 30. Generation of *MS* has been explained with the help of an example in Figures 7 and 8. In Figure 7, a best basis set is constructed after applying WPD on an image block. The average of this set is calculated as 17. The binary conversion of 17 is considered as the key for CA, which is used to construct *MS* in Figure 8. The first row of the block is



a) Share generation phase



b) Authentication phase

Figure 6. Block diagram of proposed scheme

initialized with the key and the remaining rows are constructed from this first row using Rule 30.

The benefits of using CA are that no codebook is required to create shares, no pixel expansion as every host image bit is represented by one bit in *MS* and no need to store the share as it can construct itself from its initial state. Existing VC scheme based on CA [26] uses a key to generate the share. This key has to be transmitted from the sender to receiver as side information which results in additional transmission cost and can be accessed by third-party attackers too. While in the proposed scheme as a binary representation of mean for every block is considered as the key, there is no need to transmit the key as side information. It can be constructed by the sender and receiver individually from their host and received image respectively. This reduces transmission cost and enhances security too.

After constructing *MS*, n meaningful and non-expanded authentication shares are generated using *MS* and watermark. Generation of authentication shares is illustrated in Figure 9. For every pixel, a random bit x is generated with probability p.

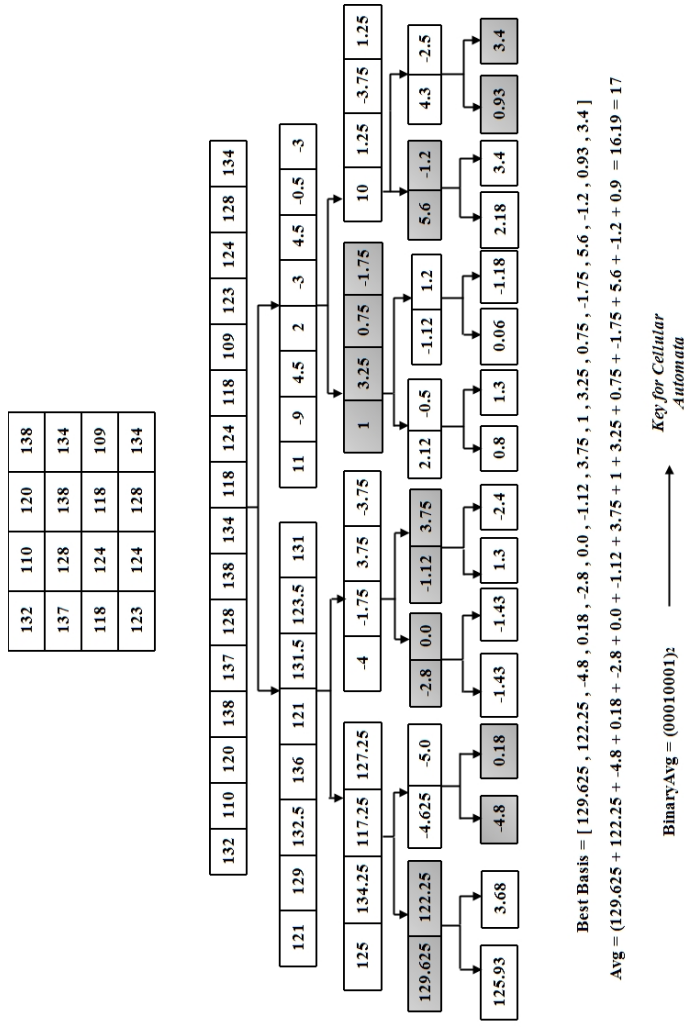
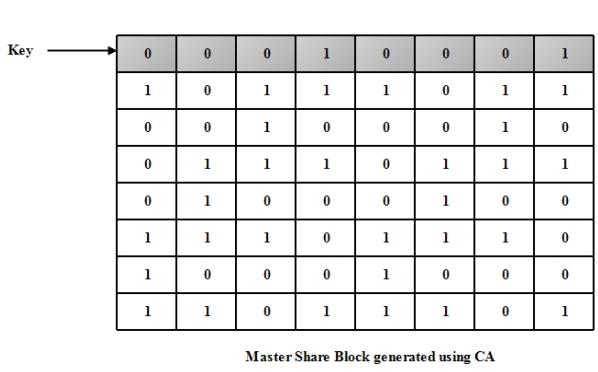


Figure 7. Example of WPD on SI Block of size 4×4

If x turns out to be 0, pixel from watermark is included in the authentication share and if it turns out to be 1, pixel from cover image is included in the authentication share.

In proposed scheme, parameter p is set as a trade-off between visual quality of share images and retrieved Watermark Image (WI), i.e., the smaller value for p results into more visual-pleasing share images and lower image quality of retrieved watermark image, while the larger value for p results in less visual-pleasing share images and higher image quality of retrieved watermark image. The generated



Rule 30

Previous State of cell and its neighbours	Next State of Cell
0 0 0	0
0 0 1	1
0 1 0	1
0 1 1	1
1 0 0	1
1 0 1	0
1 1 0	0
1 1 1	0

Figure 8. Generation of KS

Algorithm 1 Master Share Construction

Input: Host Image (HI) of size $r \times c$
Output: Master Share (MS)

Divide HI into equal size blocks HI^b of size $m \times m$, where $1 \leq b \leq a$, $a = \frac{r \times c}{m \times m}$
for every block (HI^b) **do**:
Apply WPD on HI^b and produce a best basis set.
Calculate average value Avg_b for the basis set
Convert Avg_b into 8 bit binary code $BinaryAvg_b$
Create corresponding Master Share by applying Rule 30 on $BinaryAvg_b$
Return MS

authentication shares $[AS_1, AS_2, \ldots, AS_n]$ are distributed among n participants and watermark is stored with a Trusting Authority (TA).

4.2 Authentication Phase

In this phase, the images are verified at the receiver's side, whether they have been maliciously tampered. For the received host image HI^r, master share MS^r is constructed using Algorithm 1 and authentication shares are retrieved from $k-1$ participants. These $k-1$ shares are superimposed with MS^r to retrieve the watermark WI^r using $k-1$ operations. The superimposed result WI^r should be similar to the WI stored with the TA. This similarity is compared using NHS, which is defined as:

$$\text{NHS} = \frac{\text{HD}(\text{WI}, \text{WI}^r)}{r \times c} \tag{1}$$

where HD is the Hamming distance between two binary images, WI is original watermark image, WI^r is extracted watermark image and $r \times c$ is the watermark

Algorithm 2 Authentication Shares Generation

Input: Master Share (MS), Watermark Image (WI), n Cover Images $[CI_1, CI_2, \ldots, CI_n]$ of size $r \times c$

Output: n Authentication Shares $[AS_1, AS_2, \ldots, AS_n]$

for $i = 1$ to r **do**
  for $j = 1$ to c **do**
    Generate a bit x, such that $x = 1$ with probability p and $x = 0$ with probability
$1 - p$.
    if $x == 1$ **then**
$[AS_1(i,j), AS_2(i,j), \ldots, AS_n(i,j)] =$
generateSecretBits$(WI(i,j), MS(i,j))$
    else
$[AS_1(i,j), AS_2(i,j), \ldots, AS_n(i,j)] =$
generateCoverBits$(CI_1(i,j), CI_2(i,j), \ldots, CI_n(i,j))$

function GENERATESECRETBITS(w, k, n)
  if $w == 0$ **then**
$m_1 = k$
  else
$m_1 =$ Complement(k)
  for z in range$(2, n)$ **do**
    if $w == 0$ **then**
$m_z = m_{z-1}$
    else
$m_z =$ Complement(m_{z-1})
  Return $[m_1, m_2, \ldots, m_n]$

function GENERATECOVERBITS(c_1, c_2, ..., c_n, n)
  for do$z$ in range$(1, n)$
    if $c_z == 0$ **then**
$m_z = 0$ or 1
    else
$m_z = 1$
  Return $[m_1, m_2, \ldots, m_n]$

image size. If the value of NHS tends towards unity, then original and extracted watermarks are identical and host image is authentic otherwise it is tampered. This phase is shown in Figure 10.

An additional refinement process is applied to WI^r to enhance the results of tamper detection. Logical NOR operation is applied between WI and WI^r for the areas which have been detected as tampered while the rest of the pixels remain unmodified. This helps in enhancing the accuracy of tamper detection scheme.

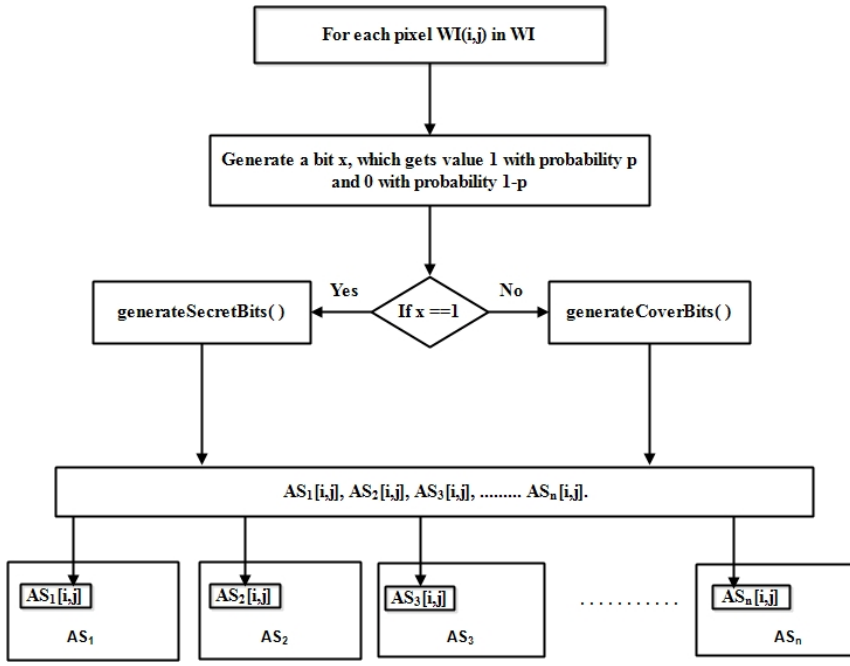


Figure 9. Generation of authentication shares

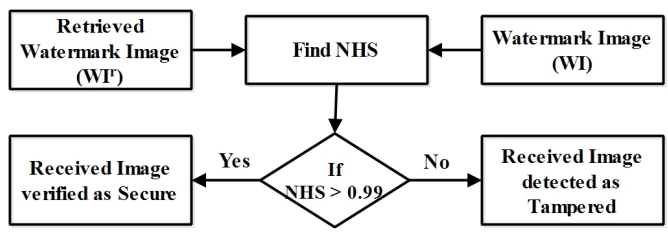
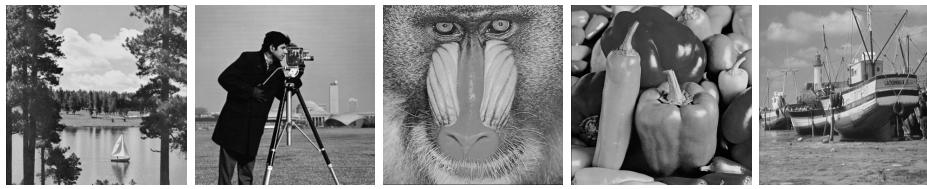


Figure 10. Tamper detection phase

5 EXPERIMENTAL RESULTS AND DISCUSSION

The performance of the proposed scheme is implemented using MATLAB (R2018a), 64-bit (win64) software. The experiment is conducted on 8-bit host images and binary watermark image of size 512×512. The size of the watermark can be lesser than size of Host Image, but that would lead to pixel expansion while generating shares. Five test images *viz.* Lake, Cameraman, Baboon, Peppers, and Boat are used for experimentation purpose and presented in Figure 11.

To evaluate the effectiveness of the proposed authentication scheme, some standard measures viz. Peak Signal to Noise Ratio (PSNR), Structural Similarity Index



a) b) c) d) e)

Figure 11. Different input test images used in the proposed method, a) Lake, b) Cameraman, c) Baboon, d) Peppers, e) Boat (Image source: `http://sipi.usc.edu/database/database.php?volume=misc`)

Module (SSIM) and Tamper Detection Rate (TDR) are used. Statistical analysis of the scheme is also performed using parameters like True Positive Rate (TPR), False Positive Rate (FPR) and accuracy. The efficiency of the proposed scheme is also tested against different tampering attacks. These measures and results are described in the following subsections.

5.1 Quality Analysis

The parameters used to analyze the visual quality of generated authentication shares are PSNR and SSIM while NHS is used to analyze similarity between original WI and retrieved WI^r.

5.1.1 Peak Signal to Noise Ratio

The visual quality of the authentication shares is evaluated using PSNR. It can be defined as:

$$\mathrm{PSNR} = 10 \log \frac{(2^{bd} - 1)^2}{\mathrm{MSE}} \tag{2}$$

where *bd* is bit depth of the image, MSE represents Mean Square Error between original cover image and authentication share. High value for PSNR shows better quality of the authentication share and least distorted. PSNR of authentication shares in the proposed scheme has been maintained above 50 dB, which is quite better with respect to the existing authentication schemes based on VC. This comparison has been shown in Table 3. PSNR of marked image with respect to original image tends toward infinity as watermark is not embedded into it.

5.1.2 Structural Similarity

This parameter is used to measure the similarity between two images by calculating similarity for various windows of the image. The similarity measure between two

windows of same size is given by:

$$\mathrm{SSIM}(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{3}$$

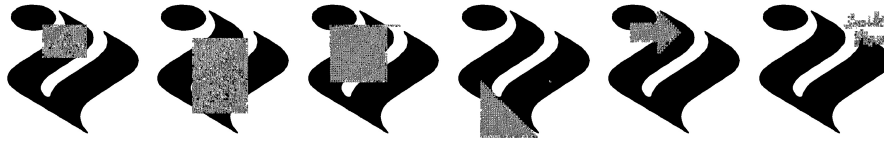
where x and y are the two different windows, μ_x and μ_y are the average values of x and y, σ_x^2 and σ_y^2 are the variance of x and y, σ_{xy} is the covariance of x and y, c_1 and c_2 are two variables to stabilize the division where $c_1 = (k_1 \times L)^2$, $c_2 = (k_2 \times L)^2$, L is the dynamic range of the pixels, $k_1 \leq 1$ is a small constant value.

Results for $(k = 2, n = 3)$-case of the scheme at successive values of $p = 0$, 0.2, 0.4, 0.6, 0.8, 1.0 have been shown in Table 1 (v)–(xviii). $(2, 3)$ represents that 3 shares are generated from the host image and at least 2 shares are required to retrieve the watermark. The table shows KS and MS at different values of p.

It can be observed from Table 1 that as the value of p increases, the visual quality of authentication share images enhances while superimposed result image deteriorates. Thus, depending upon the application and the requirements, the value of p can be chosen, i.e., when the security of the shares being stored is the main concern, a larger value of p would be preferred while if the quality of the watermark retrieved is the main concern to verify the image authentication, smaller value of p can be chosen.

The performance of the proposed scheme is tested against different tampering attacks on all test images. The tampered images and their detection results are shown in Figures 12, 13, 14, 15.

a) Attack 1 b) Attack 2 c) Attack 3 d) Attack 4 e) Attack 5 f) Attack 6



g) Tamper detection for attack 1 h) Tamper detection for attack 2 i) Tamper detection for attack 3 j) Tamper detection for attack 4 k) Tamper detection for attack 5 l) Tamper detection for attack 6

Figure 12. Different tampering attacks and their tamper detection results for Cameraman

It can be observed that the tampered areas in the original cameraman image shown in Figures 12 a)–12 f), are visible as gray patches on the retrieved watermarks

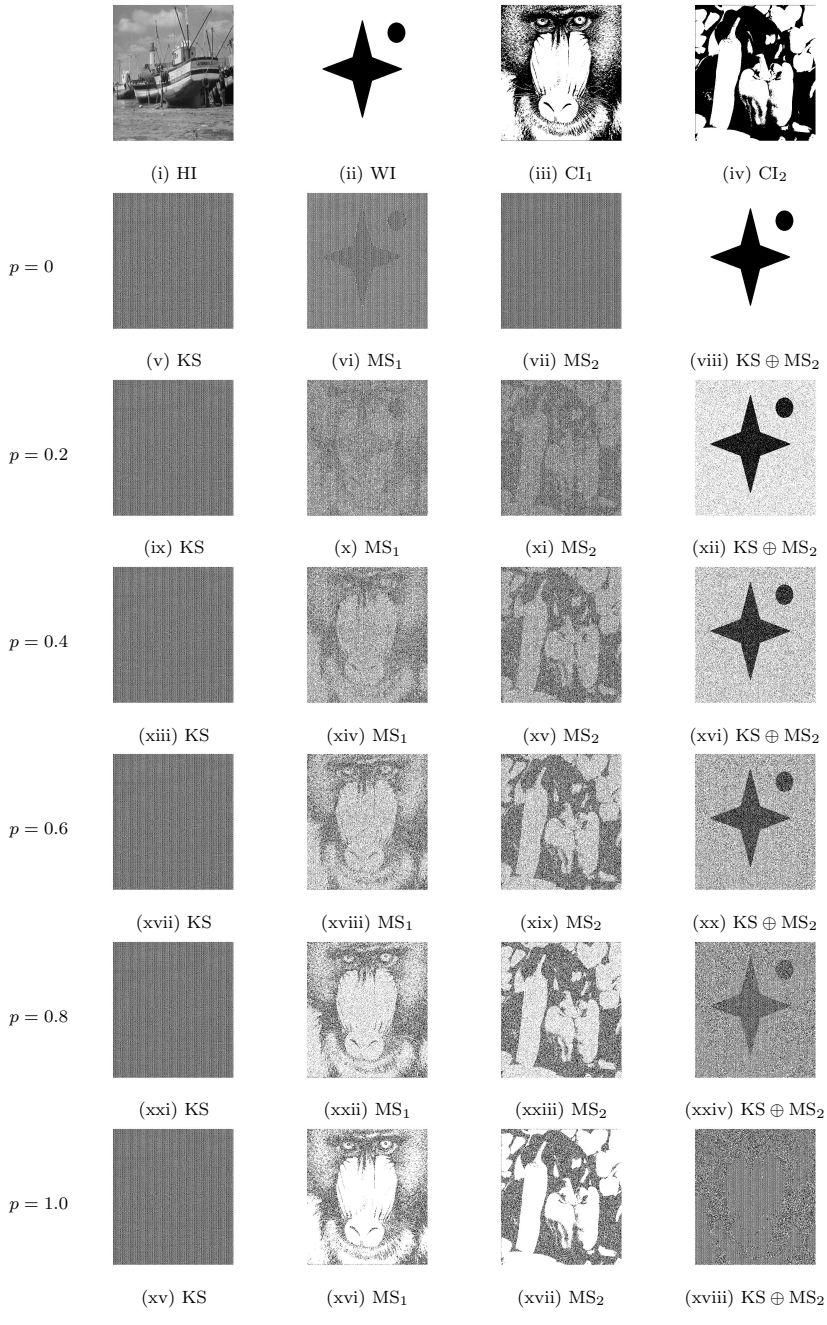
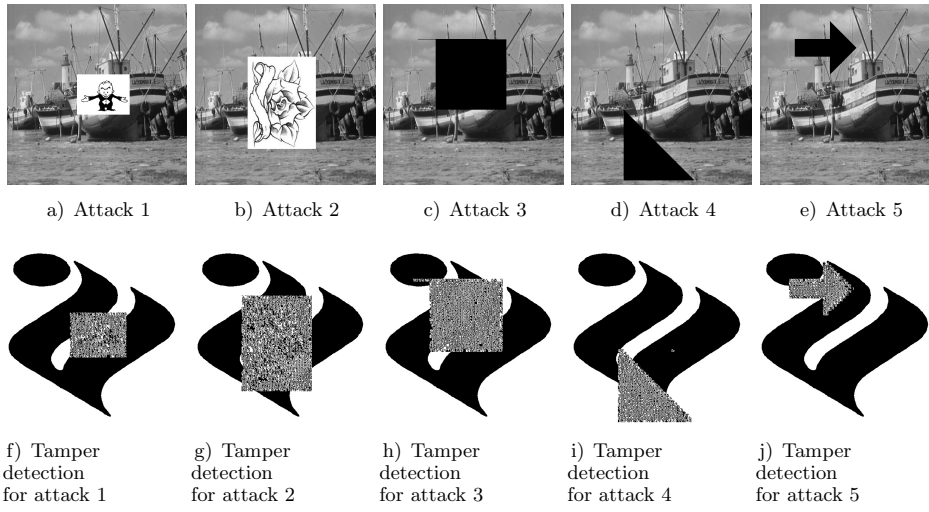


Table 1. Simulation results by proposed scheme for $(k = 2, n = 3)$

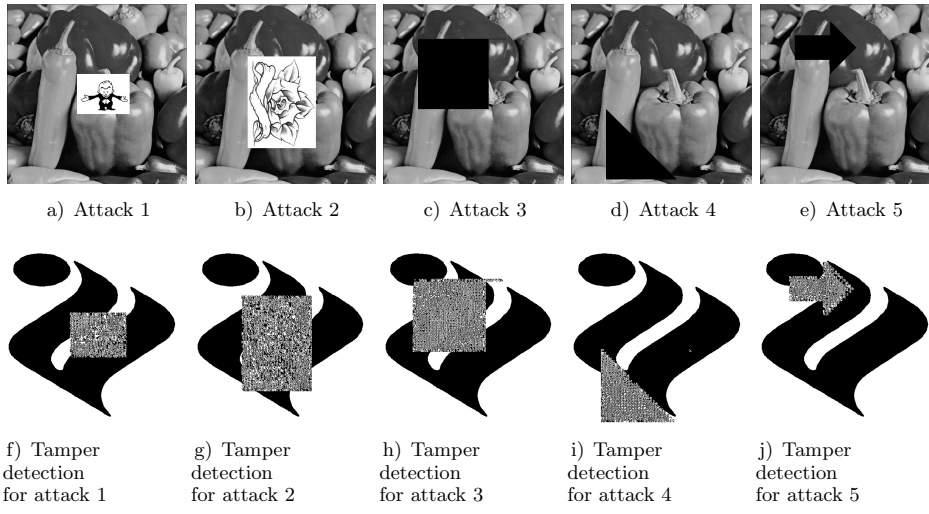
in Figures 12 g)–12 l). Similarly, the tamper detection results for Boat, Peppers and Baboon against different tampered attacks are shown in Figures 13, 14, 15.



a) Attack 1 b) Attack 2 c) Attack 3 d) Attack 4 e) Attack 5

f) Tamper detection for attack 1 g) Tamper detection for attack 2 h) Tamper detection for attack 3 i) Tamper detection for attack 4 j) Tamper detection for attack 5

Figure 13. Different tampering attacks and their tamper detection results for Boat

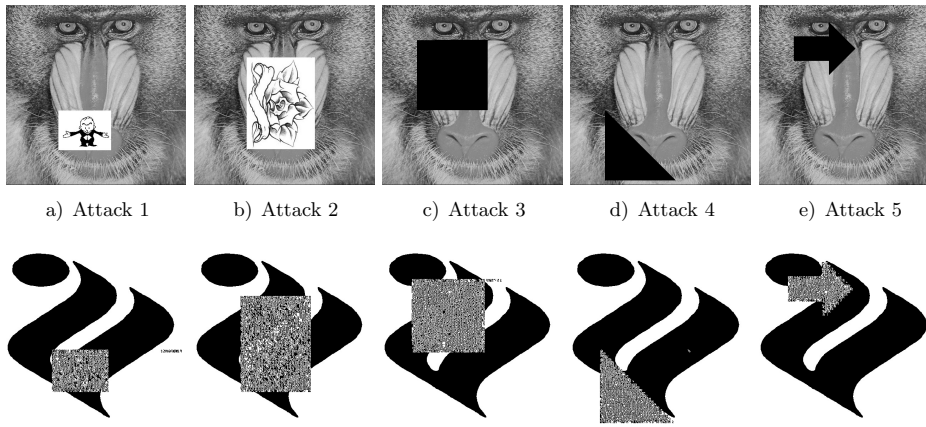


a) Attack 1 b) Attack 2 c) Attack 3 d) Attack 4 e) Attack 5

f) Tamper detection for attack 1 g) Tamper detection for attack 2 h) Tamper detection for attack 3 i) Tamper detection for attack 4 j) Tamper detection for attack 5

Figure 14. Different tampering attacks and their tamper detection results for Peppers

Thus, Figures 12, 13, 14, 15 verify the effectiveness of the proposed scheme in terms of tamper detection. The areas tampered in the attacked images can be visually observed in the retrieved watermark as a gray colored patch.



a) Attack 1 b) Attack 2 c) Attack 3 d) Attack 4 e) Attack 5

f) Tamper detection for attack 1 g) Tamper detection for attack 2 h) Tamper detection for attack 3 i) Tamper detection for attack 4 j) Tamper detection for attack 5

Figure 15. Different tampering attacks and their tamper detection results for Baboon

Table 2 shows the PSNR and SSIM values for the authentication shares generated at different values of p. The results have been shown for AS_1 and AS_2 which are two authentication shares created using the cover images Baboon and Peppers, as shown in Figure 1.

Probability (p)	PSNR		SSIM	
	MS_2	MS_3	MS_2	MS_3
0	54.92	54.29	0.9836	0.9806
0.25	53.04	53.26	0.9801	0.9772
0.5	52.12	52.42	0.9754	0.9741
0.75	51.53	51.74	0.97	0.97
1	51.14	51.16	0.965	0.964

Table 2. PSNR and SSIM of the authentication shares generated for different values of probability (p)

It can be observed from the results that the PSNR of the generated authentication shares have been maintained above 50 dB and SSIM between the share images and the cover images have been maintained close to 1. The values of PSNR and SSIM decrease, as the values of p increase. Table 3 shows the comparison of the PSNR values of the authentication shares of the proposed scheme with the stego images of the existing schemes, that have been created to authenticate the host image. The results for the proposed scheme are shown for an average p value, i.e. $p = 0.5$.

It can be observed from Table 3 that the *PSNR* of these images in the proposed scheme is maintained to be better as compared to the existing schemes. In the

Schemes → Images ↓	Lin et al. [5]	Chang et al. [3]	Chang et al. [4]	Eslami et al. [39]	Yang et al. [8]	Wu et al. [36]	Ulutas et al. [13]	Peng et al. [38]	Proposed Scheme
Baboon	39.18	40.93	45.10	48.10	36.20	47.17	–	40.71	52.12
Lena	39.18	40.97	45.12	48.13	36.17	47.19	48.45	40.73	52.25
Pepper	39.16	40.96	45.1	48.12	36.18	47.18	–	40.72	52.42

Table 3. Comparison with the existing schemes for the PSNR of the authentication shares generated

existing schemes, the stego images are created and stored with hash data and shares embedded into them. While, in the proposed scheme, instead of embedding any data, authentication shares are created using the master share, watermark and cover images.

5.2 Statistical Analysis

Some additional parameters are used to test the effectiveness of the proposed scheme for its tamper detection ability. These parameters are described in Table 4. Two cases have been considered for this evaluation:

Case A: In this case, tamper detection efficiency is analyzed in terms of number of pixels in the image.

Case B: In this case, tamper detection efficiency is analyzed in terms of number of blocks in the image.

5.3 Tamper Detection Rate

Tamper detection rate (TDR) for the scheme for both the cases is shown in Table 10. It can be observed that, for Case A, the detection rate is satisfactory while for Case B it is quite high. This can be defined as: $\text{TDR} = \frac{\text{TP}}{X_{pixels}}$ for Case A, while for Case B, it is defined as: $\text{TDR} = \frac{\text{TP}}{X_{blocks}}$. Value for TP would depend on the Case being followed.

The results of the proposed scheme for the statistical parameters are shown in Tables 3, 4, 5, 6, 7, 8, and 9. Values in these tables show results obtained for various test images at different attacks. Referring to these tables, results clearly demonstrate that the algorithm shows high accuracy in tamper detection. It can be observed that for the blocks, accuracy is around 100 % for most of the images at different attacks. For the pixels it is low, as compared to blocks, but still it is quite high.

Table 10 shows the tampered detection rate of both cases for different images and at different attacks. It can be observed that the proposed scheme shows very high tampered detection rate for Case B while it is satisfactory for Case A.

Table 11 shows the timing analysis of the scheme for different images. It can be observed from this table that the scheme is quite efficient in terms of the time complexity. The construction of authentication shares takes less than one second.

Parameter	Description
T_{pixels}	Total number of pixels in HI^r
X_{pixels}	Total number of tampered pixels in HI^r
T_{blocks}	Total number of blocks in HI^r
X_{blocks}	Total number of tampered blocks in HI^r
True Positive (TP)	A true positive is an outcome where the model correctly predicts the positive class, i.e. number of tampered pixels or blocks that are accurately identified as tampered.
True Negative (TN)	A true negative is an outcome where the model correctly predicts the negative class, i.e. number of untampered pixels or blocks that are accurately identified as untampered.
False Positive (FP)	A false positive is an outcome where the model incorrectly predicts the positive class, i.e. number of pixels or blocks that are tampered but falsely identified as untampered
False Negative (FN)	A false negative is an outcome where the model incorrectly predicts the negative class, i.e. number of pixels or blocks that are untampered but falsely identified as tampered
False Positive Rate (FPR)	$\frac{\text{FP}}{\text{FP} + \text{TN}}$
True Positive Rate (TPR)	$\frac{\text{TP}}{\text{TP} + \text{FN}}$
Accuracy (%)	$\frac{(\text{TP} + \text{TN})}{(\text{Total number of pixels or blocks})}$

Table 4. Parameters used for statistical analysis of tamper detection

Table 12 shows the comparison of the proposed scheme with existing image authentication schemes. In this table, the first column shows different authentication schemes. Subsequently, performance evaluation matrices such as *PSNR*, the similarity between extracted and embedded watermark and tamper detection ability are compared. It can be observed that, as the scheme uses VC, the watermark is not embedded inside the host image, but is hidden in the shares generated. Hence *PSNR* of the marked image with respect to original image tends toward infinity. Also, as XOR operation is used to superimpose *MS* and *AS*, which ensures maximum similarity between the original and extracted watermark, *NHS* tends towards 1. Methods suggested by other authors embed the watermark into the host image, hence the *PSNR* value decreases. Tamper detection ability of the proposed scheme is also high which has been shown in the results. The '–' in the table shows the corresponding data is not available in respective papers.

Table 13 shows the comparison of the proposed scheme with existing image authentication schemes based on VC. In the proposed scheme, CA is used to construct shares and watermark is hidden in these shares. Hence, unlike the existing schemes, there is no requirement of embedding watermark inside the host image and can be

Attack	T_{pixels}		X_{pixels}		TP		FP		TN		FN		TPR		FPR		Accuracy(%)	
Index	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks
1	262 144	4 096	17 097	300	10 595	299	6 502	1	245 047	3 796	989	0	0.9146	1	0.0258	0.00026	97.52	99.98
2	262 144	4 096	50 321	849	32 397	848	17 924	1	211 823	3 247	1 907	0	0.9444	1	0.0780	0.00037	93.16	99.98
3	262 144	4 096	40 000	682	26 763	680	13 237	2	222 144	3 414	1 738	0	0.9390	1	0.0562	0.00058	94.95	99.95
4	262 144	4 096	20 100	377	15 700	377	4 400	0	242 044	3 719	1 931	0	0.8905	1	0.0179	0	98.32	100
5	262 144	4 096	10 700	203	8 025	203	2 675	0	251 444	3 893	1 136	0	0.8760	1	0.0105	0	98.98	100

Table 5. Statistical analysis of tamper detection capacity in terms of pixels and blocks for Boat

Attack	T_{pixels}		X_{pixels}		TP		FP		TN		FN		TPR		FPR		Accuracy(%)	
Index	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks
1	262 144	4 096	17 012	308	10 010	308	7 002	0	245 132	3 788	1 308	0	0.8844	1	0.0278	0	97.33	100
2	262 144	4 096	50 332	850	32 898	850	17 434	0	211 812	3 246	2 016	0	0.9423	1	0.0760	0	93.35	100
3	262 144	4 096	40 000	682	26 546	682	13 454	0	222 144	3 414	1 732	0	0.9388	1	0.0571	0	94.87	100
4	262 144	4 096	20 100	352	17 319	352	2 781	0	242 044	3 414	1 185	0	0.9360	1	0.0114	0	98.94	100
5	262 144	4 096	12 700	227	9 579	227	3 121	0	249 444	3 869	790	0	0.9238	1	0.0124	0	98.81	100

Table 6. Statistical analysis of tamper detection capacity in terms of pixels and blocks for Baboon

Attack	T_{pixels}		X_{pixels}		TP		FP		TN		FN		TPR		FPR		Accuracy(%)	
Index	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks
1	262 144	4 096	17 088	300	10 515	295	6 573	5	245 056	3 796	991	0	0.9139	1	0.0269	0.0013	97.49	99.88
2	262 144	4 096	50 329	849	31 788	841	18 541	8	211 815	3 247	1 943	0	0.9424	1	0.0805	0.0025	92.93	99.80
3	262 144	4 096	39 970	682	26 549	680	13 421	2	222 174	3 414	1 543	0	0.9451	1	0.0570	0.0005	94.88	99.95
4	262 144	4 096	20 092	352	17 289	350	2 803	2	242 052	3 744	1 027	0	0.9439	1	0.0114	0.0005	98.93	99.95
5	262 144	4 096	12 697	227	9 748	223	2 949	4	249 447	3 869	712	0	0.9319	1	0.0117	0.0010	98.88	99.90

Table 7. Statistical analysis of tamper detection capacity in terms of pixels and blocks for Cameraman

Attack	T_{pixels}		X_{pixels}		TP		FP		TN		FN		TPR		FPR		Accuracy(%)	
Index	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks
1	262 144	4 096	17 099	319	11 556	319	5 543	1	245 045	3 777	1 575	0	0.8801	1	0.0221	0	97.89	100
2	262 144	4 096	50 313	849	32 226	848	18 087	1	211 831	3 247	1 921	0	0.9437	1	0.0787	0.0003	93.10	99.98
3	262 144	4 096	40 000	680	26 464	680	13 536	2	222 144	3 414	1 639	0	0.9417	1	0.0574	0.0005	94.84	99.95
4	262 144	4 096	20 100	352	17 300	350	2 800	2	242 044	3 744	1 238	0	0.9332	1	0.0114	0.0005	98.93	99.95
5	262 144	4 096	12 700	224	9 746	224	2 954	3	249 444	3 869	838	0	0.9208	1	0.0117	0.0007	98.87	99.93

Table 8. Statistical analysis of tamper detection capacity in terms of pixels and blocks for Peppers

Attack	T_{pixels}		X_{pixels}		TP		FP		TN		FN		TPR		FPR		Accuracy(%)	
Index	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks	Pixels	Blocks
1	262 144	4 096	17 097	300	9 992	299	7 105	1	245 047	3 796	1 028	0	0.9067	1	0.0282	0.0002	97.29	99.98
2	262 144	4 096	50 304	849	32 453	848	17 851	1	211 840	3 247	1 919	0	0.9442	1	0.0777	0.0003	93.19	99.98
3	262 144	4 096	40 000	682	26 517	682	13 483	0	222 144	3 414	1 657	0	0.9412	1	0.0572	0	94.86	100
4	262 144	4 096	20 100	352	17 270	352	2 830	0	242 044	3 744	1 115	0	0.9394	1	0.0116	0	98.92	100
5	262 144	4 096	12 700	227	9 571	227	3 129	0	249 444	3 869	877	0	0.9161	1	0.0124	0	98.81	100

Table 9. Statistical analysis of tamper detection capacity in terms of pixels and blocks for Lake

Images	Boat		Baboon		Lena		Lake		Peppers		Cameraman	
Attack Index	Case A	Case B	Case A	Case B	Case A	Case B	Case A	Case B	Case A	Case B	Case A	Case B
1	66.91	99.67	58.84	100	67.48	100	58.44	99.67	67.58	100	61.53	98.33
2	64.38	99.88	65.36	100	64.57	99.41	64.51	99.88	64.05	99.88	63.16	93.06
3	66.91	99.71	66.36	100	61.25	100	66.29	100	66.16	99.71	66.42	99.71
4	78.10	100	86.16	100	85.93	100	85.92	100	86.07	99.43	86.05	99.43
5	75.00	100	75.43	100	75.55	100	75.36	100	76.74	98.68	76.77	98.24

Table 10. Detection rate for different images at different attacks

extracted just by overlapping the shares without any use of complex extraction algorithm. This reduces the complexity of the scheme. As mean of every block is used as a key, there is no need of transmitting any side information, as mean can be calculated by the sender and receiver individually. This saves the transmission cost. In the existing schemes, all the shares constructed have to be stored with the recipients which are later superimposed together to retrieve the watermark, while in the proposed scheme only one share needs to be stored as the other share is auto-generated using CA. All algorithms can locate tamper detection, but accuracy is either low or not calculated. Most of the reported techniques did not suggest any method to classify attacks quantitatively. While in the proposed scheme, a complete statistical analysis of the scheme has been performed and shown for different images and at different attacks, showing high accuracy.

Images → Algorithms ↓	Boat	Baboon	Lena	Lake	Peppers	Cameraman
Master Share Construction	29.82	36.77	31.84	34.50	30.61	31.80
Authentication Shares Construction	0.64	0.65	0.59	0.61	0.59	0.83
Authentication Phase	46.25	49.55	43.52	46.28	43.72	46.05

Table 11. Timing analysis for different images (in seconds)

5.4 Security Analysis

To prove the security of the proposed scheme, it has been analyzed using the following security aspects.

5.4.1 Construction of Shares

Unlike the existing authentication schemes [24, 15, 7, 21, 10, 18, 16] based on watermarking, the watermark is not embedded inside the host image, but it is used to construct shares. This makes it very difficult to detect or recover the watermark from marked image, thereby making the scheme more secure.

5.4.2 Meaningful Shares

The meaningless random looking shares generated in the traditional VC schemes usually create a suspicion that some secret data is being shared which proves to be a security threat. Thus in the proposed scheme meaningful authentication shares have been generated to ensure the security of the proposed scheme.

Technique	Scheme	PSNR (dB)	Similarity Factor	Tamper Detection/ Localizing	Embedding Required
Chuang et al. [16]	VQ Scheme	≈ 34	–	Possible	Yes
Shen et al. [14]	DWT based scheme	≈ 30	NC = 0.98	Not discussed	Yes
Preda et al. [24]	DWT based scheme	≈ 40	–	Possible	Yes
Al et al. [21]	DWT quantization	≈ 41	–	Possible, can detect 8×8 region	Yes
Li et al. [7]	Two Level DWT	≈ 36	NC = 0.8	Possible, localization accuracy medium	Yes
Li et al. [18]	VQ Scheme	≈ 31.3	SSIM = 0.88	Possible	Yes
Shojanazeri et al. [15]	DWT and Zernike moments	≈ 40.9	–	Possible	Yes
Singh et al. [10]	DCT based scheme	≈ 39.3	NC = 0.98	Possible	Yes
Tiwari et al. [1]	Two stage VQ technique	≈ 42	NHS = 1.0	Possible	Yes
Proposed Work	VC based scheme	*Infinite*	NHS ≈ 1.0, NC = 1.0, SSIM = 0.9	Possible, accuracy is very high	No

Table 12. Comparison of proposed scheme with recent image authentication schemes

5.4.3 k out of n scheme

The watermark image has been used to ensure the authentication of the shares generated, thereby enhancing the security. The watermark can be revealed only when k participants superimpose their shares including master share generated from host image. No less than k shares have the ability to extract the watermark. This ensures the security of the scheme.

6 CONCLUSION

In this paper, an authentication scheme based on WPD, VC and CA is proposed. The tampered areas are detected just by XOR-superimposition of shares, thus reducing computational complexity. Experimental results and discussions demonstrate the efficiency of the proposed scheme in terms of imperceptibility, extraction of the hidden watermark with minimum complexity, high accuracy in tamper detection, high security due to meaningful shares, low storage cost and low transmission cost. Also, as compared to some existing authentication schemes based on VC, the proposed scheme can directly generate meaningful authentication shares with wa-

Scheme	Scheme Used for Share Creation	Authentication Data	Embedding Required	Extraction Scheme	Pixel Expansion	Storage Cost for Shares	Transmission Cost for Side Information	Accuracy %
Lin et al. [5]	Polynomial based VC	Parity bits	Yes	Extraction and Overlapping	–	Yes	Yes	–
Chang et al. [3]	Polynomial based VC	Chinese Remainder Theorem	Yes	Extraction and Overlapping	–	Yes	Yes	–
Eslami et al. [39]	Polynomial based VC	Hash Function	Yes	Extraction and Overlapping	–	Yes	Yes	–
Wu et al. [36]	Cellular Automata	Hash Function	Yes	Extraction and Overlapping	–	Yes	Yes	–
Ulutas et al. [13]	Polynomial based VC	Hash Function	Yes	Extraction and Overlapping	–	Yes	Yes	–
Shrividhya et al. [30]	Traditional VC	Authentication Image	No	Extraction and Overlapping	–	Yes	Yes	–
Proposed Work	Cellular Automata and Traditional VC	Watermark	No	XOR-Overlapping	No	Partial	No	High

Table 13. Comparison of proposed scheme with existing image authentication schemes based on VC

termark, host and cover image information, without any extra data hiding process. Tamper detection rate and accuracy have been observed more than 99 % for different images against different tamper attacks. The proposed scheme can be extended to color images.

REFERENCES

[1] Tiwari, A.—Sharma, M.—Tamrakar, R. K.: Watermarking Based Image Authentication and Tamper Detection Algorithm Using Vector Quantization Approach. AEU – International Journal of Electronics and Communications, Vol. 78, 2017, pp. 114–123, doi: 10.1016/j.aeue.2017.05.027.

[2] Ilachinski, A.: Cellular Automata – A Discrete Universe. World Scientific, 2001, doi: 10.1142/4702.

[3] Chang, C.-C.—Hsieh, Y.-P.—Lin, C.-H.: Sharing Secrets in Stego Images with Authentication. Pattern Recognition, Vol. 41, 2008, No. 10, pp. 3130–3137, doi: 10.1016/j.patcog.2008.04.006.

[4] Chang, C.-C.—Chen, Y.-H.—Wang, H.-C.: Meaningful Secret Sharing Technique with Authentication and Remedy Abilities. Information Sciences, Vol. 181, 2011, No. 14, pp. 3073–3084, doi: 10.1016/j.ins.2011.03.002.

[5] Lin, C.-C.—Tsai, W.-H.: Secret Image Sharing with Steganography and Authentication. Journal of Systems and Software, Vol. 73, 2004, No. 3, pp. 405–414, doi: 10.1016/S0164-1212(03)00239-5.

[6] Lo, C.-C.—Hu, Y.-C.: A Novel Reversible Image Authentication Scheme for Digital Images. Signal Processing, Vol. 98, 2014, pp. 174–185, doi: 10.1016/j.sigpro.2013.11.028.

[7] Li, C.—Zhang, A.—Liu, Z.—Liao, L.—Huang, D.: Semi-Fragile Self-Recoverable Watermarking Algorithm Based on Wavelet Group Quantization and Double Authentication. Multimedia Tools and Applications, Vol. 74, 2015, No. 23, pp. 10581–10604, doi: 10.1007/s11042-014-2188-7.

[8] Yang, C. N.—Chen, T. S.—Yu, K. H.—Wang, C. C.: Improvements of Image Sharing with Steganography and Authentication. Journal of Systems and Software, Vol. 80, 2007, No. 7, pp. 1070–1076, doi: 10.1016/j.jss.2006.11.022.

[9] Lou, D. C.—Chen, H. H.—Wu, H. C.—Tsai, C. S.: A Novel Authenticatable Color Visual Secret Sharing Scheme Using Non-Expanded Meaningful Shares. Displays, Vol. 32, 2011, No. 3, pp. 118–134, doi: 10.1016/j.displa.2011.02.001.

[10] Singh, D.—Singh, S. K.: DCT Based Efficient Fragile Watermarking Scheme for Image Authentication and Restoration. Multimedia Tools and Applications, Vol. 76, 2017, No. 1, pp. 953–977, doi: 10.1007/s11042-015-3010-x.

[11] Frattolillo, F.: Watermarking Protocols: An Excursus to Motivate a New Approach. International Journal of Information Security, Vol. 17, 2018, No. 5, pp. 587–601, doi: 10.1007/s10207-017-0386-9.

[12] Ateniese, G.—Blundo, C.—De Santis, A.—Stinson, D. R.: Extended Schemes for Visual Cryptography. Theoretical Computer Science, Vol. 250, 2001, pp. 143–161, doi: 10.1016/S0304-3975(99)00127-9.

[13] Ulutas, G.—Ulutas, M.—Nabiyev, V. V.: Secret Image Sharing Scheme with Adaptive Authentication Strength. Pattern Recognition Letters, Vol. 34, 2013, No. 3, pp. 283–291, doi: 10.1016/j.patrec.2012.10.017.

[14] Shen, H.—Chen, B.: From Single Watermark to Dual Watermark: A New Approach for Image Watermarking. Computers and Electrical Engineering, Vol. 38, 2012, No. 5, pp. 1310–1324, doi: 10.1016/j.compeleceng.2011.11.012.

[15] Shojanazeri, H.—Adnan, W. A. W.—Ahmad, S. M. S.—Rahimipour, S.: Authentication of Images Using Zernike Moment Watermarking. Multimedia Tools and Applications, Vol. 76, 2017, No. 1, pp. 577–606, doi: 10.1007/s11042-015-3018-2.

[16] Chuang, J.-C.—Hu, Y.-C.: An Adaptive Image Authentication Scheme for Vector Quantization Compressed Image. Journal of Visual Communication and Image Representation, Vol. 22, 2011, No. 5, pp. 440–449, doi: 10.1016/j.jvcir.2011.03.011.

[17] Jensen, A.—la Cour-Harbo, A.: Ripples in Mathematics: The Discrete Wavelet Transform. Springer Verlag, 2001, doi: 10.1007/978-3-642-56702-5.

[18] Li, M.—Xiao, D.—Zhang, Y.: Attack and Improvement of the Fidelity Preserved Fragile Watermarking of Digital Images. Arabian Journal for Science and Engineering, Vol. 41, 2016, No. 3, pp. 941–950, doi: 10.1007/s13369-015-1941-1.

[19] Naor, M.—Shamir, A.: Visual Cryptography. In: De Santis, A. (Ed.): Advances in Cryptology – EuroCrypt '94. Springer, Berlin, Heidelberg, Lecture Notes in Computer Science, Vol. 950, 1995, pp. 1–12, doi: 10.1007/BFb0053419.

[20] Singh, M.—Kaur, H.—Kakkar, A.: Digital Signature Verification Scheme for Image Authentication. 2015 2nd International Conference on Recent Advances in

Engineering and Computational Sciences (RAECS), Chandigarh, India, 2015, doi: 10.1109/RAECS.2015.7453277.

[21] Al-Otum, H. M.: Semi-Fragile Watermarking for Grayscale Image Authentication and Tamper Detection Based on an Adjusted Expanded-Bit Multiscale Quantization-Based Technique. Journal of Visual Communication and Image Representation, Vol. 25, 2014, No. 5, pp. 1064–1081, doi: 10.1016/j.jvcir.2013.12.017.

[22] Kafri, O.—Keren, E.: Encryption of Pictures and Shapes by Random Grids. Optics Letters, Vol. 12, 1987, No. 6, pp. 377–379, doi: 10.1364/OL.12.000377.

[23] Percival, D. B.—Walden, A. T.: Wavelet Methods for Time Series Analysis. Cambridge University Press, 2000, doi: 10.1017/CBO9780511841040.

[24] Preda, R. O.: Semi-Fragile Watermarking for Image Authentication with Sensitive Tamper Localization in the Wavelet Domain. Measurement, Vol. 46, 2013, No. 1, pp. 367–373, doi: 10.1016/j.measurement.2012.07.010.

[25] Preda, R. O.—Vizireanu, D. N.: Watermarking-Based Image Authentication Robust to JPEG Compression. Electronics Letters, Vol. 51, 2015, No. 23, pp. 1873–1875, doi: 10.1049/el.2015.2522.

[26] Yampolskiy, R. V.—Rebolledo-Mendez, J. D.—Hindi, M. M.: Password Protected Visual Cryptography via Cellular Automaton Rule 30. In: Shi, Y. Q., Liu, F., Yan, W. (Eds.): Transactions on Data Hiding and Multimedia Security IX. Springer, Berlin, Heidelberg, Lecture Notes in Computer Science, Vol. 8363, 2014, pp. 57–67, doi: 10.1007/978-3-642-55046-1_4.

[27] Alam, S.—Jamil, A.—Saldhi, A.—Ahmad, M.: Digital Image Authentication and Encryption Using Digital Signature. International Conference on Advances in Computer Engineering and Applications, Ghaziabad, India, 2015, pp. 332–336, doi: 10.1109/ICACEA.2015.7164725.

[28] Han, S.-H.—Chu, C.-H.: Content-Based Image Authentication: Current Status, Issues, and Challenges. International Journal of Information Security, Vol. 9, 2010, No. 1, pp. 19–32, doi: 10.1007/s10207-009-0093-2.

[29] Shyu, S. J.: Image Encryption by Random Grids. Pattern Recognition, Vol. 40, 2007, No. 3, pp. 1014–1031, doi: 10.1016/j.patcog.2006.02.025.

[30] Srividhya, S.—Sathishjumar, R.—Sudha, G. F.: Implementation of TiOISSS with Meaningful Shadows and with an Additional Authentication Image. Journal of Visual Communication and Image Representation, Vol. 38, 2016, pp. 284–296, doi: 10.1016/j.jvcir.2016.03.012.

[31] Wolfram, S.: Statistical Mechanics of Cellular Automata. Reviews of Modern Physics, Vol. 55, 1983, No. 3, pp. 601–644, doi: 10.1103/RevModPhys.55.601.

[32] Guo, T.—Liu, F.—Wu, C.: K out of K Visual Cryptography Scheme by Random Grids. Signal Processing, Vol. 94, 2014, pp. 90–101, doi: 10.1016/j.sigpro.2013.06.003.

[33] Nguyen, T.-S.—Chang, C.-C.—Yang, X.-Q.: A Reversible Image Authentication Scheme Based on Fragile Watermarking in Discrete Wavelet Transform Domain. AEU – International Journal of Electronics and Communications, Vol. 70, 2016, No. 8, pp. 1055–1061, doi: 10.1016/j.aeue.2016.05.003.

[34] Korzhik, V.—Zhuvikin, A.—Morales-Luna, G.: Selective Image Authentication Tolerant to JPEG Compression. 2015 6th International Conference on Infor-

mation, Intelligence, Systems and Applications (IISA), Corfu, Greece, 2015, doi: 10.1109/IISA.2015.7388076.

[35] Hong, W.—Chen, M.—Chen, T. S.: An Efficient Reversible Image Authentication Method Using Improved PVO and LSB Substitution Techniques. Signal Processing: Image Communication, Vol. 58, 2017, pp. 111–122, doi: 10.1016/j.image.2017.07.001.

[36] Wu, X.—Sun, W.: Secret Image Sharing Scheme with Authentication and Remedy Abilities Based on Cellular Automata and Discrete Wavelet Transform. The Journal of Systems and Software, Vol. 86, 2013, No. 4, pp. 1068–1088, doi: 10.1016/j.jss.2012.11.021.

[37] He, Y.—Yang, G.—Zhu, N.: A Real-Time Dual Watermarking Algorithm of H.264/AVC Video Stream for Video-on-Demand Service. AEU – International Journal of Electronics and Communications, Vol. 66, 2012, No. 4, pp. 305–312, doi: 10.1016/j.aeue.2011.08.007.

[38] Peng, Y.—Niu, X.—Yin, Z.: Image Authentication Scheme Based on Reversible Fragile Watermarking with Two Images. Journal of Information Security and Applications, Vol. 40, 2018, pp. 236–246, doi: 10.1016/j.jisa.2018.04.007.

[39] Eslami, Z.—Ahmadabadi, J. Z.: Secret Image Sharing with Authentication-Chaining and Dynamic Embedding. Journal of Systems and Software, Vol. 84, 2011, No. 5, pp. 803–809, doi: 10.1016/j.jss.2011.01.002.

[40] Ziaullah, M.—Shetty, P.—Kamal, S.: Image Feature Based Authentication and Digital Signature for Wireless Data Transmission. 2016 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2016, doi: 10.1109/ICCCI.2016.7480009.

[41] Yin, Z.—Niu, X.—Zhou, Z.—Tang, J.—Luo, B.: Improved Reversible Image Authentication Scheme. Cognitive Computation, Vol. 8, 2016, No. 5, pp. 890–899, doi: 10.1007/s12559-016-9408-6.

[42] Qin, H. D.—Dai, Y.—Wang, Z.: A Secret Sharing Scheme Based on (t, n) Threshold and Adversary Structure. International Journal of Information Security, Vol. 8, 2009, No. 5, pp. 379–385.

[43] Hadavi, M. A.—Jalili, R.—Damiani, E.—Cimato, S.: Security and Searchability in Secret Sharing-Based Data Outsourcing. International Journal of Information Security, Vol. 14, 2015, No. 6, pp. 513–529, doi: 10.1007/s10207-015-0277-x.

[44] Lin, S.-J.—Lin, J.-C.: VCPSS: A Two-in-One Two-Decoding-Options Image Sharing Method Combining Visual Cryptography (VC) and Polynomial-Style Sharing (PSS) Approaches. Pattern Reognition, Vol. 40, 2007, pp. 3562–3666, doi: 10.1016/j.patcog.2007.04.001.

Sonal Kukreja graduated in 2012 from Rajasthan Technical University, Kota, India and received her M.Tech. degree in 2015 in the field of computer science and applications from the Thapar Institute of Engineering and Technology, Patiala, India. In 2016, she enrolled as doctoral student at the Thapar Institute of Engineering and Technology, Patiala, India. Her research interest has focused on information security, particularly on data hiding in images, visual cryptography and watermarking.

Geeta Kasana is working as Assistant Professor in Computer Science and Engineering Department, Thapar University, Patiala, India. She has twelve years of teaching and research experience. She received her Ph.D. degree in information security from the Thapar Institute of Engineering and Technology. Her research interests include image processing and information security. She has published many research papers in reputed international journals and conferences. She is currently guiding Ph.D. students on information security.

Singara Singh Kasana is working as Associate Professor in Computer Science and Engineering Department, Thapar Institute of Engineering and Technology, Patiala, Punjab, India. He has nineteen years of teaching and research experience. He received his Ph.D. degree in image compression from the Thapar Institute of Engineering and Technology. His research interests include image processing, wireless networks, and information security. He has published many research papers in reputed international journals and conferences. He is currently guiding Ph.D. students on information security, machine learning and remote sensing.