Identity verification system: a visual cryptography-based approach to prevent fraudulent in admission process

Dhiraj Pandey*

Department of CSE,
JSS Academy of Technical Education,
C-20/1, Sector-62, Noida (UP), India
Email: dhip2@yahoo.co.in
*Corresponding author

Uma Shankar Rawat

School of Computing and IT,
Manipal University Jaipur,
Jaipur-Ajmer Express Highway,
Dehni Kalan, Jaipur (RJ), India
Email: umashankar.rawat@jaipur.manipal.edu

Abstract: In today’s competitive world, examinations are a means of assessing a person’s potential. It is therefore important that such process be unbiased, but several cases have been encountered where candidates use proxies to write exams and score well. To deal with the same, generally we use multiple identity proofs to authenticate the candidate, which increases the privacy concern and expended on maintaining the extra data and keeping it secure. This paper introduces a novel authentication technique using bit plane-based encryption for fraud candidate detection during any stage of the selection process. Multiple visual cryptography-based method has been explored for its suitability. The effect of noise and differently chosen encryption scheme has also been observed. With the currently available infrastructure, it is quite easy to implement the proposed system for authentication of students and provide a level platform for competition.

Keywords: visual cryptography; image encryption; identification; bit-level processing; authentication.


Biographical notes: Dhiraj Pandey received his MTech from University School of Information Technology, GGSIPU, New Delhi. He is pursuing his PhD in the area of visual cryptography-based security schemes from Manipal University Jaipur. He has 12 years of teaching experience. Currently, he is working as an Assistant Professor in the Department of CSE at JSS Academy of Technical Education Noida. His current research interests include information systems security allied areas.
1 Introduction

The current structure to authenticate students for entrance examinations is to use multiple identity proofs which include thumb impression, photograph, signature and government issued identity proof. Using multiple means for a single candidate authentication, achieves the ultimate goal, but proves to be a tedious task and gives a space for fraudulent activity at different stages of selection. Conventional security techniques take more computational time and space, compare to visual cryptography-based approach of securing digitally collected data. A large number of visual cryptography techniques have appeared in the literature. The traditional approach has been widely studied by many researchers and suggested variants of strategy for protecting the content and its applicability. Although researchers have suggested several means of checking the candidature, but an effective experimental implementation of verifying identity with minimal resources and cost remains an open question in the literature. The main objective of this paper is to create a system that can verify the identity of the examinee, maintain the privacy of the candidate by safeguarding the data provided for verification while simultaneously reducing the hassle involved with multiple identity proofs. A computational framework for visual cryptography-based verification is presented here, with an objective of solving the real life social problem.

This paper is organised as follows: Next section describes a brief review of visual cryptography-based schemes and its utility. A detailed system design and proposed scheme has been presented in the system outline section. Performance and security of the implemented scheme using bit level strategy are presented in section of Performance analysis and experimental results. Many types of visual cryptographic techniques including random grid technique have been examined for their suitability in the comparison section of the article. Some concluding remarks are given in the last section.

2 Review of TVC schemes

Research into the making digital content secure has been steadily growing. Conventional security techniques take more computational time and space, compare to visual cryptography-based approach of securing data. A large number of visual cryptography techniques have appeared in the literature. These techniques can be divided into two main classes: traditional visual cryptography (TVC) and the progressive visual cryptography (PVC). The traditional approach has been widely studied by many researchers and suggested variants of strategy for protecting the content. Cheating detection and prevention has been suggested by many researchers for traditional schemes (Chen and
A common drawback of using the TVC-based technique is the loss of contrast and pixel expansion problem. One may overcome issues of TVC, using PVC-based approaches. The concept emerged as ‘PVC’ has been explored by many researchers. This topic has gained a wide and equal attention from academician, researchers, and software developers.

In this section, a detailed review has been presented in related research of visual cryptography and their schemes for digital content security.

2.1 Traditional VCS scheme

A new cryptographic paradigm was designed based on the pixel level operation (Naor and Shamir, 1995). They termed this visual cryptography and introduced it as a method for encrypting images. In the (2, 2) VC scheme secret image is divided into two shares such that no information can be reconstructed from any single share. Each share is printed on transparencies. Stacking the two shares does decryption and the secret image can be seen by the naked eyes without any complex cryptographic computations. As suggested in the scheme, if a pixel in the original image was black, the sub pixel in the superimposition of the two shares will be fully black. Similarly, if a pixel in the original image was white, the sub-pixel in the superimposition of the two shares will be black and white. However, because the pixels are small and situated very close together, the human eye averages the relative contributions of the black and white pixels, resulting in a grey pixel. Neither of the shares generated, reveals any information about the original image, but when both are stacked, a representation of the original image can be seen. Visual cryptography scheme using random number has been suggested to apply the visual cryptography scheme for colour images (Kandar et al., 2011). Watermarking algorithm to improve the security of secret has also been suggested (Rawat and Raman, 2012; Ross and Othman, 2011).

2.2 VCS scheme using random grids

A visual cryptography scheme through the use of random grids (RG) is quite similar to basic scheme. RG scheme (Kafri and Keren, 1987) takes an input image and transforms it into multiple cipher-grids that provide no information on the original image. Kafri and Keren (1987) proposed three similar two out of two algorithms employing random grids, out of which third algorithm is discussed here. The algorithm takes an input image. It then initialises two ciphers-grid images R1 and R2 with the same dimensions as the input image. The algorithm then randomises the contents of R1, producing an image of random black and white pixels. R2 is next generated based on the input image and R1. This process occurs by scanning each pixel of the input image. If a pixel at location (x, y) in the input image is found to be black, then the pixel R2 (x, y) is set to a value of either 0 or 1 randomly. If, instead, the pixel at (x, y) in the input image is white, then the pixel R2 (x, y) is set to be the complement of R1 (x, y). The decryption is same as in traditional VC, that is, performing OR operation of both multiple ciphers-grids. This scheme has the additional benefit that it does not require pixel expansion. Many researches have been carried out to show the relationship between random grids and TVC methods (Prisco and Santis, 2014; Hou and Lin, 2014; Guo et al., 2014).
2.3 Bit-level-based VCS scheme

A new scheme has been proposed (Lukac and Plataniotis, 2005) in which traditional VC scheme developed by Naor and Shamir can be implemented on bit planes of the original secret image. Naor and Shamir (1995) scheme and Kafri and Keren’s (1987) scheme had some shortcomings. Darker decrypted image or image of low contrast is generated in both schemes, but the size of the reconstructed image becomes double the size of the original input image in first scheme. So, the authors have provided an alternative solution to overcome the above mentioned shortcomings. In this scheme, assuming that the number of bits per pixel in the input image is B, B-bit planes or binary images of the input image are decomposed. Bit level decomposition is the pre-processing step of share-based encrypting. Each binary image goes through the conventional way of encryption as developed by Naor and Shamir to generate n binary shares. To achieve the final n shares of the original input image, bit level stacking of individually encrypted bit planes is done. To achieve perfect reconstruction of input image, the authors have proposed to make the decryption process reciprocal of the encryption process. This method preserves all features of traditional \((k, n)\) sharing schemes, allow for perfect reconstruction of the input B-bit image, encrypts binary, greyscale and colour images, and can be effectively implemented either in software or hardware.

2.4 Size invariant visual cryptography

Image size invariant VC has been proposed to overcome the problem of the traditional scheme (Ito et al., 1999). TVC schemes employ pixel expansive. Many researchers have worked on how to improve problem of pixel expansion (Tzeng and Hu, 2002). The scheme (Ito et al., 1999) uses the traditional \((k, n)\) scheme where \(m\) is equal to one. The recovered secret can be viewed as the difference of probabilities with which a black pixel in the reconstructed image is generated from a white and a black pixel in the secret image. The most important part of any VC scheme is the contrast. The lower the contrast of the recovered secret, the harder it is to visually recover the secret. The contrast for this scheme is defined as follows: \(\beta = |p_0 - p_1|\), where \(p_0\) and \(p_1\) are the probabilities with which a black pixel on the reconstructed image is generated from a white and black pixel on the secret image. Another method (Yang, 2004) to deal with size invariant shares was proposed in which the frequency of white pixels is used to show the contrast of the recovered images. If quality and contrast matter, then the size of the shares will increase, for a user’s particular application. So these size invariant schemes always incur a cost in terms of losing contrast. Image size invariant visual cryptography for general access structures has also been suggested to improve the visual quality (Lee and Chiu, 2013; Liu and Qian, 2012; Shi et al., 2014).

2.5 Friendly, progressive visual secret sharing scheme

For progressively share a halftone secret image, a scheme has been suggested (Fang, 2008). Each secret pixel in the halftone secret image is expanded into a four-pixel block. In the decoding process, the halftone secret image can be recovered progressively by stacking the shares of different quantities. Unfortunately, this scheme suffers from the pixel-expansion problem, i.e., the sizes of the generated shares and the recovered halftone
Identity verification system

secret image increase fourfold, in other words, their size is four times as large as the original secret image.

Fang’s (2008) tried to solve the problem of the presence of all or nothing by progressive recovery, but still it suffers from the same problem of pixel expansion which is an innate drawback of TVC.

2.6 PVC with unexpanded shares

A new scheme of progressive VC has been proposed to produce pixel unexpanded shares (Hou and Quan, 2011). By stacking few pieces of shares scheme gives a little sketch about the original secret, but more details can be revealed if more shares are stacked and contrast will also get better. In the method suggested by the author, encoding process will not leak out any secret information on any share. The design guarantees that the black pixels of secret image are fully restored and the contrast increases gradually as more shares are stacked and thus providing better contrast. As the block is not divided into any sub pixels in the share therefore each block contains single pixel. Thus the size of the share and secret image remains the same.

2.7 Application of visual cryptography schemes for security

Visual cryptography is a fascinating technique. To preserve the privacy of digital data (raw images), visual cryptography has gained a lot of attention from both researchers as well as industry people. It can be said that visual cryptography applications range from banking industry, satellite imaging to commercial application for preserving collected biometric data. Visual cryptography has a very wide range of applications. Practical uses for visual cryptography come in the form of watermarking (Memon and Wong, 1998; Lou et al., 2007). Robust recovery of the watermark is also possible after the image has been defaced. Without the key, no watermark recovery is possible. One of the most robust ways to hide a secret within natural images is by typically employing visual cryptography based on half tone techniques. VC potentially makes it applicable to a wider range of security applications, such as within the banking industry. Hence it can be said that by using the different variety of available visual cryptography, encryption scheme, one can transmit the secret message with more security as compared to the existing others security means. Besides the robust security, the presented novel scheme here also possesses, the better recovered thumbprint image as compared to traditional other approaches. So an extended idea of detection of the fraud candidate by a practical, feasible approach has been discussed in the next section of this article.

3 Proposed scheme

The overall design of the system, the user interface and how the student will interact with the system has been discussed in this section. A conventional method for authenticating students in entrance exams is to use biometrics. Biometric identification techniques like face authentication, iris recognition and handwritten signature recognition, suffer from the problems of low uniqueness, easy intrusion and low permanence respectively. Compared to these, thumbprint has a higher value of permanence and uniqueness. The
friction ridges on our fingers to form patterns that are entirely unique to us. Thus, thumbprint is the perfect biometric for the purpose of authentication. Because of its advantages, bit-level slicing has been used as a technique for creating shares during the encryption process.

3.1 System architecture

Candidate fills in the necessary details and then uploads his/her scanned thumbprint image. The uploaded image is used to create two shares using chosen bit-level-based visual cryptography. One of the shares is stored on the server to be used at the time of authentication while the other share is printed on the admit card of the student. The coordinator scans the admit card of the candidate at the test centre and uploads it to the server for overlapping with the share stored on the server. The thumb print of the candidate will be gathered via thumbprint scanner on the spot again by the coordinator at the centre. The overlapped image is returned from the server, which is then matched with the thumbprint given by the candidate on the spot. A match of the two images guarantees that the candidate taking an exam is the one whose details were filled in the form. The same fingerprint-based authentication needs to be repeated at the time of admission so that the situation does not arise where the candidate taking the exam is different from the one taking admission.

3.2 Proposed scheme

In the proposed scheme, during registration, the thumbprint image is first sliced into its corresponding bit planes. Each of the bit planes is then encrypted using 2, 2 visual cryptography, resulting in 16 binary shares. Every first share from the original bit planes is stacked using bit-plane stacking to give us first final share, the admit card share and the remaining eight shares, after bit-plane stacking, result in the second final share which is the server share. Figure 1 shows the encryption process of the scheme.

3.2.1 Procedure for thumbprint encryption and share generation

Step 1 Read thumbprint image taken from a scanner.
Step 2 Divide thumbprint into bit-plane using function bitplane_slice(img).
Step 3 For each bit b of every pixel and for each row and column of image bitget(img(row, col), b) used by function bitplane_slice(img) returns 8-bit planes. Save all the created 8-bit plane images.
Step 4 For each bit plane, use V_Encrypt(img) function.
Step 5 Encryption matrices used by V_Encrypt(img) is of following nature for binary image.
Identity verification system

\begin{align*}
  s_{10} &= [1 \; 0; \; 1 \; 0; \; 1 \; 0; \; 10] ; \; s_{00} = [0 \; 0; \; 1 \; 1; \; 1 \; 0 \; 0] \\
  s_{11} &= [0 \; 1; \; 0 \; 1; \; 0 \; 1] ; \; s_{01} = [1 \; 1; \; 0 \; 0; \; 0 \; 1 \; 1] \\
  s_{12} &= [1 \; 1; \; 0 \; 0; \; 1 \; 1; \; 00] ; \; s_{02} = [0 \; 1; \; 0 \; 1 \; 0 \; 10] \\
  s_{13} &= [0 \; 0; \; 1 \; 1; \; 0 \; 0; \; 11] ; \; s_{03} = [1 \; 0; \; 1 \; 0; \; 0 \; 1 \; 1] \\
  s_{14} &= [1 \; 0; \; 0 \; 1; \; 1 \; 0; \; 01] ; \; s_{04} = [1 \; 0; \; 0 \; 1; \; 0 \; 1 \; 10] \\
  s_{15} &= [0 \; 1; \; 1 \; 0; \; 0 \; 1; \; 10] ; \; s_{05} = [0 \; 1; \; 1 \; 0; \; 0 \; 1 \; 1] \\
\end{align*}

Step 6  Save the output of V_Encrypt(img) into corresponding locations.

Step 7  Use bitplane_stack(s11, ……, s81) to generate share for printing into admit card.

Step 8  Use bitplane_stack(s12, …….., s82) to generate share for storing into coordinating university.

To authenticate an individual, the images of the candidate admit card is scanned. This image is divided into its corresponding bit planes. The same is done for the corresponding image on the server. This results in 2 * B binary bit planes for a B-bit plane image. These 2 * B binary planes are decrypted by using the reverse process of 2, 2 visual cryptography by Naor and Shamir. Each plane from the admit card image is decrypted with each corresponding plane of the server image. This results in B binary images. These B binary images are then stacked using bit-plane stacking to give the final decrypted image of the thumbprint. Figure 2 shows the decryption process of the scheme.

Figure 1  Encryption phase of proposed scheme
3.2.2 Procedure for thumbprint decryption and authentication

Step 1  Read both share from admit card and coordinating university.

Step 2  Use bitplane_slice(img) for both shares to divide it into bit plane.

Step 3  Use V_decrypt (img1, img2) for decryption from these planes.

Step 4  Use bitplane_stack (img) to recover the thumbprint.

Step 5  Find correlation between recovered thumbprint and read new thumbprint from the candidate on the spot. If $\text{abs (correlation)} \leq 0.3$, the two images do not match, else the two images match.

This retrieved image is then compared with the image captured by the thumbprint scanner at the place of examination. If the two images match, then the identity of the candidate can be successfully established else the candidate is a proxy and can be easily eliminated. The process flow for the authentication is as shown in Figure 3.
4 Performance analysis and experimental results

A concrete evaluation of the quality of a modified image can be made using similarity measures. Existing measures of similarity include the mean squared error (MSE), the peak signal to noise ratio (PSNR), and the structural similarity (SSIM) index. The MSE is the average value of the square of the difference between the two images. MSE is not necessarily a good indicator of quality to hide message in an encoded share. The PSNR is in essence the logarithm of the reciprocal of the MSE. Although recently SSIM seems to be a better measure of the quality of encoded shares, PSNR is more commonly reported. For experiment, dataset of 200+ user’s details along with their photographs; signature and thumbprints has been collected. Different types of file format of thumbprint data have been used to save the collected data. As unique differences in our fingerprints are extremely small and subtle, it is important that fingerprint readers should have the ability to image our fingers in great detail. A fingerprint reader with a low DPI will not offer incredible security because a blurry image of our finger notes fewer data points than a high-resolution image. Verifi P5100 fingerprint scanner has been used for collecting thumbprint of all the sample users. The proposed scheme has been implemented in MATLAB 7.11.0.584 (R 2010 b) on 64-bit Windows 7 system. Figure 4 shows a screenshot of the registration page for the entrance examination.
Candidate fills in details like name, college, address and also uploads his photograph, signature and thumbprint. Figure 5 shown below is a screenshot of the registration page once the candidate has clicked the ‘Register’ button. Text details, i.e., name, college and address are saved in a CSV file while the photograph and signature get saved into separate folders. Thumbprint undergoes processing using bit-level-based visual cryptography, which includes a bit-level slicing, encryption using (2, 2) VSS scheme and finally bit-plane stacking. Two shares are generated: Server share, which is automatically saved into a folder and Admit share, which is available for the candidate to download.

Each integer pixel value in digital image can be expressed equivalently in a binary form using B bit representation.

\[ I_{(i,j)} = i_{(i,j)}^1 2^{B-1} + i_{(i,j)}^2 2^{B-2} + \ldots + i_{(i,j)}^{B-1} 2 + i_{(i,j)}^{B} \]

Figure 6 shows the terminal for authentication at the examination centre. Invigilator scans and uploads the image on the admit card of the candidate (no other information is printed on admit card) and selects the corresponding share on the server. The test for robustness of the proposed scheme has been done by checking all kinds of distortion in admit card.
image using different types of attack. Thumbprint image of the candidate is also taken on the spot at the centre.

**Figure 6** Terminal for authentication system (see online version for colours)

![Authentication System](image)

Figure 7 shows the result of the process. Decryption is performed using the scanned share from the admit card and the share on the server. It results in an image which is then compared to the image of the thumbprint taken using the thumbprint sensor. Based on the similarity of the two images, the result of the authentication process identity of the candidate is established. It is assumed that thumbprint reconstructed after decryption process and thumbprint taken using sensors stores the image in same format and size. Image rotation or resize is needed before comparing similarity between images. Correlation coefficient has been computed between the images to check the similarity.

**Figure 7** Result of matching (see online version for colours)

![Authentication System](image)
To faithfully decrypt the original $B$-bit image from its $B$-bit shares, the decryption function must satisfy the perfect reconstruction property, meaning that the output should be identical to the original input. This can be obtained only if the encryption and decryption operations are reciprocal.

The decryption function, generalised for any $\{k, n\}$ configuration is proposed here as follows:

$$\hat{i}_{(i,j)}^b = f_d \left( s_1^b, s_2^b, \ldots, s_k^b \right)$$

$$\begin{cases} 
1 & \text{for } \left[ s_1^b, s_2^b, \ldots, s_k^b \right]^T \in S_1, \\
0 & \text{for } \left[ s_1^b, s_2^b, \ldots, s_k^b \right]^T \in S_0 
\end{cases}$$

where $S_1$ and $S_0$ are basis matrices given in Section 3 and $s_q^b \in S_q^b$ for $q = 1, 2, \ldots, k$.

4.1 Effect on scheme due to characteristics of image

As the image size decreases, quality of reconstructed image also decreases and vice versa (Kumar and Chahal, 2014). Huffman coding may be applied to the higher capacity thumbprint for providing compression. Table 1 displays the results of size variation and size $150 \times 220$ pixels has been considered here for experimentation.

Table 1  MSE and PSNR values for thumbprint using the proposed scheme

<table>
<thead>
<tr>
<th>Image characteristic (different sizes or pixels)</th>
<th>MSE</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thumbprint ($100 \times 146$ pixels)</td>
<td>4,507.96</td>
<td>11.6249974</td>
</tr>
<tr>
<td>Thumbprint ($150 \times 220$ pixels)</td>
<td>3,720.07</td>
<td>12.4592906</td>
</tr>
<tr>
<td>Thumbprint ($200 \times 293$ pixels)</td>
<td>1,782.14</td>
<td>15.6553791</td>
</tr>
</tbody>
</table>

Table 2 displays the MSE, PSNR and correlation coefficient values for images of different formats using bit level-based visual cryptography. The proposed scheme can work well with different formats of image and its PSNR values are shown in Figure 8.

Table 2  MSE, PSNR and correlation coefficient values for thumbprint of different formats using the proposed scheme

<table>
<thead>
<tr>
<th>Image characteristic (different formats)</th>
<th>MSE</th>
<th>PSNR</th>
<th>Correlation coefficient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thumbprint (.jpg)</td>
<td>2,820.25</td>
<td>13.6619202</td>
<td>0.8669</td>
</tr>
<tr>
<td>Thumbprint (.png)</td>
<td>2,733.68</td>
<td>13.7973258</td>
<td>0.8629</td>
</tr>
<tr>
<td>Thumbprint (.tif)</td>
<td>2,752.32</td>
<td>13.7678083</td>
<td>0.8648</td>
</tr>
</tbody>
</table>

5 Comparison of bit-level with differently chosen VC schemes

The proposed scheme is compared with the TVC and visual cryptography, which employs random grids to show the differences in respective decrypted images after the algorithm has been performed. To make a comparison, we report PSNR, MSE and correlation coefficient values here.
Identity verification system

Figure 8  PSNR values for different image formats using proposed scheme (see online version for colours)

Figure 9 shows the implementation of the proposed scheme, that is, bit level-based visual cryptography on the thumbprint with the original image, and it is both shares and decrypted image.

Figure 9  Applying bit level-based VC on a thumbprint (see online version for colours)

Figure 10 shows the implementation of traditional or conventional visual cryptography on the thumbprint with the original image, it is both shares and decrypted image.
Figure 10  Applying (2, 2) traditional VC on a thumbprint (see online version for colours)

Figure 11 shows the implementation of visual cryptography using random grids on the thumbprint with the original image, it is both shares and decrypted image.

Figure 11  Applying (2, 2) VC using random grids on a thumbprint (see online version for colours)

From Table 3, it can be observed that bit level-based visual cryptography has less MSE value as compared to other two values, hence the quality of reconstructed image using the proposed scheme is much better than other two. This method increases security and
prevents unauthorised decryption through brute-force enumeration as the encryption is based on B bit encryption. Figures 12 to 14 show the comparison of MSE, PSNR and correlation coefficient values for different images using the mentioned visual cryptography schemes.

### Table 3  
MSE, PSNR and correlation coefficient values for thumbprint using different VCS

<table>
<thead>
<tr>
<th>Implementation characteristic for greyscale</th>
<th>MSE</th>
<th>PSNR</th>
<th>Correlation coefficient</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2, 2) TVC</td>
<td>33,504.46</td>
<td>2.9137731</td>
<td>-0.9307</td>
</tr>
<tr>
<td>(2, 2) Bit level-based VC</td>
<td>2,820.25</td>
<td>13.6619202</td>
<td>0.8779</td>
</tr>
<tr>
<td>(2, 2) VC using random grids</td>
<td>14,315.44</td>
<td>6.6067528</td>
<td>0.4254</td>
</tr>
</tbody>
</table>

**Figure 12**  
MSE values for images using different schemes (see online version for colours)

**Figure 13**  
PSNR values for images using different schemes (see online version for colours)
Figure 14  Correlation coefficient values for images using different schemes (see online version for colours)

5.1 Robustness of the proposed scheme

The test for robustness of the proposed scheme has been done by checking against salt and pepper noise attack, blurring attack and averaging attack.

Figure 15  Admit card share under salt and pepper attack and its impact on decrypted image (see online version for colours)

As is evident from Figure 15, the proposed scheme is robust against salt and pepper attack. The decrypted image can still be used as a means for authentication of a person.
Figure 16  Admit card share under blurring attack and its impact on decrypted image. (see online version for colours)

Figure 16 shows the admit card share under blurring attack. Even if deblurring of the admit card image is done before using it for decryption, the recovered image is not good enough for authentication of personnel. Less than 50% of the decrypted image match the original image. Hence, the proposed image is not robust under blurring attack.

Figure 17  Admit card share with Gaussian noise and the decrypted image (see online version for colours)

Figure 17 shows the admit card share under Gaussian noise of value 0 and variance 0.015. The proposed scheme is robust under Gaussian attack. The decrypted image can still be used to authenticate the person.
Table 4  Correlation factor between the original and extracted fingerprint after several attacks

<table>
<thead>
<tr>
<th>Attack method</th>
<th>Correlation factor between original and extracted thumbprint (in %)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No attack</td>
<td>0.8779</td>
</tr>
<tr>
<td>Gaussian noise</td>
<td>0.7181</td>
</tr>
<tr>
<td>Salt and pepper attack</td>
<td>0.8126</td>
</tr>
<tr>
<td>Blurring attack</td>
<td>0.4778</td>
</tr>
</tbody>
</table>

As shown in Table 4, correlation factors between original and extracted thumbprint for Gaussian noise and salt and pepper attack are above the threshold value, i.e., 70%, hence the scheme is robust against them. However, the scheme is not robust against blurring attack as the correlation factor is below the threshold value.

6  Conclusions

A verification technique for an original identification of candidate during the examination and admission is proposed in this paper. The noises like outputs of the bit level secret sharing is used to scatter between candidates admit card and examination conducting authority. Thumbprint of the candidate is used as secret for sharing registration unique information. In particular, it is shown that the proposed scheme has good imperceptibility. Finally, in comparison with some existing VC schemes, the proposed scheme is shown to have superior performance. It is well known that the confusion in the encryption process is ultimately related to the security, i.e., more confusion leads to more security. Hence it can be said that by using the proposed scheme using bit-level encryption, one can transmit the secret message with more security as compared to the existing others VC. Besides the robust security, the presented scheme also possesses, the better recovered thumbprint image as compared to traditional other approaches. In summary, extended idea of detection of the fraud candidate by a practical, feasible approach has been provided in this paper. The proposed scheme uses only the thumbprint of the candidate to establish the identity, saving one the handling of multiple files per candidate. This approach can be easily implemented for any kind of examination and gives a fair chance to all candidates for admission without having any fraudulent activities. This method also increases security and prevents unauthorised decryption through brute-force enumeration as the encryption is based on B bit encryption.

An improvement can be incorporated with respect to the processing time of share generation which can be further reduced by ignoring the LSBs as bits contain less significant information compared to the MSBs.

References


Identity verification system


