Secret Sharing and Authentication Using Visual Cryptography with RSA Algorithm

Simeranjot Kaur¹, Amandeep Kaur², Pooja Kumari³
¹Associate Professor, ²,³M.Tech Student
Department of Computer Science and Technology, School of Engineering and Technology, Central University of Punjab, Bathinda, India

Received: 10 May Revised: 18 May Accepted: 26 May

Abstract
In this world of digitalization, almost every communication is done over the internet. Therefore, any type of data like military maps is transmitted over the network and it creates a lot of issues like security, authenticity, and integrity of transmitted data. To provide the secrecy of transmitted data, there are lots of methods. The foremost and important method is visual cryptography scheme in which message like images, etc. can be broken down into transparencies or shares while transmitting over the network. To get the original message, transparencies need to be superimposed. But if these transparencies are traveling over the same network then attacker use these weak communications to steal these transparencies and the message will be leaked or may alter the pixels to change the original message. So, these shares must be encrypted by using some cryptographic algorithm in order to provide security while transmitting. And for the authenticity of the message, the asymmetric key algorithm should be used.

Keywords:- Visual cryptography, visual cryptography schemes, secret image sharing, encryption, RSA encryption decryption algorithm.

I. INTRODUCTION
In the latest years, the communication gets conveniently over the internet due to the technology and information technology field grows very rapidly. Over the Internet, various trustworthy information like military maps have communicated. Therefore, while sharing secret images; security concern is the major issue because hackers can steal the desired information by using the weak links of the communication network. For securing the data over communication a technique named cryptography has introduced and developed a lot of different methods to encrypt and decrypt the data. There is a development of many image secret sharing schemes. Naor and Shamir introduced the first technique as a Visual cryptography [1]. The concept of visual cryptography defines as the visualization characteristic of human uses to decipher the ciphered image. Shares have been generated by splitting the secret picture into the components. The shares are superimposed to decrypt the encrypted information and revealed the hidden image [2]. Anyone can change the components of the system, and decryption process can be performed visually just by looking at the components. It does not require any kind of knowledge about cryptography and there is no need to perform any computations related to cryptography. The original information that is required to be encrypted is called a secret. Once the encryption completes, shares referred to the generated ciphers. The part of secret in twisted form is known as share. The sharing of secret among a group of n participants is the fundamental idea behind visual cryptography. The secret divides into n number of pieces, referred to shares, to share the secret. Afterward, these shares are distributed among n participants. Each participant provides their transparencies to reveal the original secret information.
RSA (Ron Rivest, Adi Shamir, and Leonard Adleman), is first publicly defined algorithm in 1978. This algorithm is used to encrypt and decrypt secret messages by modern computers. It is an asymmetric cryptographic algorithm which means that it uses two different keys. It is also called public key cryptography as one of the keys is open that means known to everyone and the other key is private. The algorithm based on calculating the elements of a large composite number which is hard when the whole numbers are prime numbers, and this issue is defined as prime factorization. It is also called a key pair (public and private key) generator[3]. It involves public and private key. The known public key is used to encrypt messages. The encrypted message should be decrypted using the private key.

The paper organized in the five sections as: Section I contains the introduction of visual cryptography and RSA algorithm, Section II contain the related work of secret sharing schemes, Section III contain the existing and proposed methodology for secret sharing with flowchart, Section IV describes results and discussion, Section V concludes research work with future directions.

II. RELATED WORK

A secret sharing scheme is a technique to protect a secret K, by distributing partial information called shares. These shares give to the set of participants, \( P = \{ P_1, P_2, \ldots, P_n \} \), in a way such that only legal participants can recover the secret K, however any unauthorized subset of participants cannot recover K. Such schemes are used to protect critical secret data from lost or destroyed without accidental or malicious exposure, such as cryptographic keys[4]. Secret sharing schemes investigate since their proposal in 1979[5]. Naor and Shamir designed the first secret sharing method in which a secret information is converted into n components and distribute between them. However, k or more shares are required to recover the secret data, but no information gets revealed to an individual if he/she has less than k shares[1].

A new approach has developed for Visual Cryptography by using the concept of Data Hiding by Conjugate Error Diffusion watermarking method. The generated shares embed into the cover image with the help of watermarking. Secret and cover images have revealed after overlapping transparencies. An extra storage space consumes by the cover image[6]. In[7], by using (2, 2) Visual Cryptography (VC) scheme, shares are generated. The shadow images were embedded with the help of watermarking technique into the cover images. These two cover images require an extra memory space. Later, an Improved Pixel Sieve Method has proposed for Visual Cryptography. In this scheme, Secret is hidden properly but the efficiency of this scheme cannot evaluate as decryption algorithm[8]. Further, an algorithm based on Visual Cryptography and Steganography is implemented[9]. The combination of steganography and visual cryptographic algorithm[10] is used to improve the double security of the system. The application creates an image of Stego in which personal data is embedded and protected by a highly secure password. Here the personal data is first encrypted using one of the cryptographic algorithms from (Rivest Cipher) RC2, DES or AES and then embedded, providing more security. But the algorithms cryptanalysis is possible, and passwords might get hacked.

The proposed system[11] takes the secret binary image to share which is first encrypted using the Advanced Encryption Standard. But there is a limitation of not working for color images and algorithm used is symmetric thus not providing any authentication and cryptanalysis is possible. To share the image secretly that required to be also authenticated, used the RSA algorithm to encrypt before sharing and decrypt after receiving. But
some noise is added in the resultant image that degrades some quality as the proposed scheme uses RGB pixels to extract from the separate color band. Then, the image divides into blocks, and each block is encrypted and decrypted using the RSA algorithm[12].

III. METHODOLOGY

After reviewing the literature in detail, it is observed that various visual cryptographic techniques are available for secret sharing. There are some pros and cons of these techniques. There is a requirement to authenticate the secret visual information and enhance the security using the asymmetric cryptographic algorithm. The existing and proposed methods are explained in detail.

A. Existing Methodology

The general (k, n) visual cryptography scheme is implemented in Matlab framework and detailed explanation is also provided. Naor and Shamir analysed the case of (k, n)-threshold visual cryptography scheme (k, n)-VCS, where 2 ≤ k ≤ n, for black and white images. In a (k, n)-VCS any set of k or more participants can recover the image by stacking their shares, whereas any set of less than k participants have no information on the secret image[13]. K is the minimum number of shares that have been required to get the original image and n is the maximum number of shares that have been required to get the original image. The existing methodology is described in figure 1.

![Figure 1: (K, N) Visual Cryptography Scheme](image-url)
B. Proposed Methodology

The general k out of n visual cryptography has extended with asymmetric key algorithm. As the shares generated with (k, n) VCS has encrypted with the RSA algorithm before sharing over the web. The encrypted shares must decrypt before stacking the transparencies to get the original message. For encrypting the shares, the public key used, and for decoding, the private key uses. As the public key shares with everyone to distribute the secret while the private key is kept private and shared to only that individual to whom you want to send the secret, thus providing the authenticity to the users. If the attacker gets the shares from the weak network, then shares must be decrypted to reveal the secret image. For that he/she must know the private key and its cryptanalysis is difficult as the algorithm used is based on the factorization of large prime numbers. If the hacker modifies the sequence of bits or bit values to change the message, then the decrypted values of the shares get altered. And the distortion in the image gets to know that there is some modification in the bits by some adversaries. The proposed technique of flowchart is shown in figure 2.

![Flowchart of Proposed Methodology](image)

**Figure 2: Proposed Method Flowchart**

**RSA Algorithm**

RSA (Ron Rivest, Adi Shamir, and Leonard Adleman), algorithm is used to encrypt and decrypt secret messages by modern computers. It is an asymmetric cryptographic algorithm which means that it uses two different keys. It is also called public key cryptography as one of the keys is open that means known to everyone and the other key is private. The algorithm based on calculating the elements of a large composite number which is hard when the whole numbers are prime numbers, and this issue is defined as prime factorization. RSA involves
both a public key and a private key. The RSA algorithm generates keys by using the algorithm, and the algorithm is as follows:

- Choose two discrete prime numbers, say p and q. It should be selected randomly and of identical length of bits for security purpose. Primality test is used for the calculation of prime integers.
- Compute \( n = p \times q \)
  
  Where, n is used as modulus for both the public and private keys. The length of key is defined in bits.
- Compute \( \varphi(n) = \varphi(p) \times \varphi(q) \)
  
  \( = (p - 1) \times (q - 1) \)
  
  \( = n - (p + q - 1) \)
  
  where, \( \varphi(n) \) is Euler's totient function.
- Choose an integer ‘e’ such that, \( 1 < e < \varphi(n) \) and \( \text{gcd}(e, \varphi(n)) = 1 \) that is e, and \( \varphi(n) \) are co-prime.
- Determine d as \( d = e^{-1} \mod \varphi(n) \).

The public key is \((e, n)\) and private key is \((d, n)\). The pixels of image are extracted from the RGB channel and encrypt it using the public key. The formula for encryption is \( \text{pixel}^e \mod n \). The decryption process uses the private key to decrypt the pixels and formula used for calculation is \( \text{encpixel}^d \mod n \).

IV. RESULTS AND DISCUSSION

A. Experimental Results:

In the proposed technique, the RSA algorithm is integrated with \((k, n)\) Visual Cryptography Scheme to overcome the limitation of existing work. After applying the k out of n VCS over the secret image, the transparencies are encrypted with the RSA algorithm using the public key. Instead of sharing the shadow images, encrypted shadow images shared over the channel. Here, the sender generates the public key by using two large prime numbers ‘p’ and ‘q’. The values of ‘p’ and ‘q’ are 223 and 233 respectively. The public key is generated using the key generation algorithm of the RSA algorithm, and its value is \((5, 51959)\). The encrypted shadow images show in figure 3. At the receiver side, shares must be decrypted with the RSA algorithm using the receiver’s private key. The private key is generated using the key generation algorithm of the RSA algorithm, and its value is \((10301, 51959)\). Decrypted shares must be stacked to obtain the original message.
B. Analysis of Proposed Method

The analysis has been done based on the cryptographic security of encryption schemes for images.

1) Encryption Quality Analysis:

The metrics used for testing the quality of the encrypted components are Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR). MSE provides a numerical value of distortion in the recovered component. PSNR gives the ratio between the maximum possible power of the signal and the power of the corrupted noise[14]. Table 1 provides the numerical values of both metrics for existing and proposed work.

<table>
<thead>
<tr>
<th>Technique</th>
<th>MSE</th>
<th>PSNR (in db)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing Technique</td>
<td>11983.38</td>
<td>55.54</td>
</tr>
<tr>
<td>Proposed Technique</td>
<td>4461.66</td>
<td>59.83</td>
</tr>
</tbody>
</table>

From the table 1, the value of the MSE decreases as the distortion between the proposed work and existing work of original and shared component (share/encrypted share). It provides security to encrypted shares.
While the value of PSNR also increases which represents better encryption quality with high protection of the secret image. The quality of the recovered image after overlaying the components needs to be checked as while securing it, the quality of the picture does not compromise. The value of MSE between the original image and the output image is zero and PSNR is infinite that means there is no distortion and the quality of the recovered image does not get affected.

2) **Structural Similarity Analysis:**

Structural Similarity Index (SSIM) requires improving the similarity measure based on human visual perception of traditional parameters such as PSNR and MSE. It differs from other methods as it considers image quality degradation as observed variance in structural information[15]. The numerical results of SSIM use for similarity calculation. The higher value indicates more similarity between the images and in the case of identical photos; the amount is taken as 1. Table 2 and figure 5 shows the numerical values of SSIM evaluating that there is very less similarity between the secret image and the component that is required to share over the web in proposed technique (encrypted) as compared to an existing method. While calculating between the original and recovered, value seems to be 1; indicating that the output image is identical.

<table>
<thead>
<tr>
<th>Technique</th>
<th>SSIM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing Technique</td>
<td>0.128557</td>
</tr>
<tr>
<td>Proposed Technique</td>
<td>0.001331</td>
</tr>
</tbody>
</table>

3) **Resistance to Differential Attack:**

The differential analysis based on the study of change in output pixels in response to a change in input pixels. Avalanche effect is used to measure the diffusion characteristic of an image cryptosystem. It is an important parameter that must be checked to verify the randomness and complexity of the system. To measure the avalanche effect, NPCR (number of pixels change rate) and UACI (unified average changing intensity) are two essential metrics that measures the performance of resisting differential attack[16].

For both the techniques, experiments are evaluated using secret image and recovered image tabulated in table 3 that shown the high NPCR values means encoded image pixels are thoroughly scrambled when comparing with secret image. From these results, NPCR and UACI values are getting near to ideal amount and thus, the proposed algorithm is resisted actively against the differential attack.
Table 3: Numerical Values of NPCR and UACI

<table>
<thead>
<tr>
<th>Technique</th>
<th>NPCR</th>
<th>UACI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing Technique</td>
<td>95.22%</td>
<td>33.13%</td>
</tr>
<tr>
<td>Proposed Technique</td>
<td>98.79%</td>
<td>22.53%</td>
</tr>
</tbody>
</table>

4) **Information Entropy Analysis:**

Information entropy is a mathematical constraint of data and coding theory that reflects the randomness and uncertainty of a source. It is an essential concept for analysing any cryptosystem as it measures its uncertainty and randomness. The ideal information source is never actually random, so its entropy value is smaller than the ideal one [17]. However, in a practical cryptosystem, the entropy must be as closer to the absolute amount as possible. Otherwise, the security of the cryptosystem will threaten.

Table 4: Numerical Value of Entropy of Image and its Shared Component

<table>
<thead>
<tr>
<th>Technique</th>
<th>Secret Image</th>
<th>Share/Encrypted Share</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing Technique</td>
<td>7.8869</td>
<td>4.9808</td>
</tr>
<tr>
<td>Proposed Technique</td>
<td>7.8869</td>
<td>6.9706</td>
</tr>
</tbody>
</table>

Table 4 indicates the entropy values of the original images and their components for both the techniques. The entropy values of the shares are closer to the theoretical value of \(8sh\), which means that the highly resist against entropy attacks.

5) **Resistance to Statistical Attack:**

Histogram Analysis: Histogram of an image depicts the frequency of each pixel. A right encrypted image has a uniform frequency distribution of the pixel values. The statistical analysis of the original image and the image, Figure 4 shows the color histograms of the original image, generated share and its encrypted share. Figures show that the histogram results of the proposed scheme generated component are different from that the existing system that shows the goodness of the generated share of the proposed method. Because its encrypted component has more uniformly distributed pixel values.
6) **Correlation Coefficient Analysis:**

Correlation is a measure of the relationship involving a couple of variables. If the two variables are the image and its transparency, then they are usually in high correlation and the correlation coefficient equates to one when they are remarkably reliant (identical). They are highly uncorrelated if the value is zero and -1 is for negative image (reverse). If the pictures are similar, then the encryption process was unsuccessful in concealing the essential points in the original image [18].
Visual Cryptography is used to provide secure communication in which secret visual information such as images, videos cannot be revealed. The proposed technique uses the RSA algorithm along with visual cryptography, to improve security. The generated transparencies encrypt before transmitting over the network which makes it difficult to extract any information until decryption performed on them. For encryption and decryption process, public and the private key are used respectively which provides authentication to the components. The overall results show that the proposed technique gives a good quality secret image with better security and reliability than the existing method. In comparison with the existing technique, the proposed method yields better results in terms of quality (PSNR and SSIM). The proposed method is also
analysed using security parameters such as Entropy, Correlation coefficient. On analysis, the proposed technique is resistant to attacks such as differential and statistical. The recovered image of the proposed scheme obtains with SSIM value 1, which means information is not lost. The work can be extended for multiple sharing of color image in a single communication. Further the size of secret images can be increased.

REFERENCES


