A Novel Approach of Image Steganography with Encoding and Location Selection

Debalina Ghosh, Arup Kumar Chattopadhyay and Amitava Nag

Abstract Steganography is a well-known technique of data hiding. The confidential pieces of information are concealed within cover media like image, audio, video such that it does not arouse any attention of eavesdroppers to scrutinize the object and that is the main advantage of steganography over conventional cryptography methods. Steganography techniques are increasingly used for audios and images. Least significant bit modification (LSB) is the most popular method for steganography. In this paper, we propose a novel secure LSB modification scheme, that can be used to hide a secret image with a few cover images. First, we encode the secret image using simple bitwise XOR operations to break strong correlation between adjacent pixels. Then the location selection algorithm has been carried out to find a particular position from least significant four bits to hide a secret bit (from secret image). We have experimented with the proposed method using MATLAB and tested on a grayscale secret image and two grayscale cover images.

Keywords Steganography · LSB · XOR · Cryptography · Grayscale image Secret image

1 Introduction

Securing the confidentiality of digital data has a great importance in our daily life. As the usage of Internet is increasing, the need to secure secret information is also increasing. Along with this requirement, the number of data hiding techniques [1] is

D. Ghosh (✉) · A. K. Chattopadhyay
Institute of Engineering and Management, Salt Lake, Kolkata, West Bengal, India
e-mail: debalinag1986@gmail.com

A. K. Chattopadhyay
e-mail: ardent.arup@gmail.com

A. Nag
Central Institute of Technology, Kokrajhar, India

M. Chakraborty et al. (eds.), *Proceedings of International Ethical Hacking Conference 2018*, Advances in Intelligent Systems and Computing 811,
https://doi.org/10.1007/978-981-13-1544-2_10

also increasing. Watermarking, cryptography, and steganography are some of them. Each of these techniques has their own advantages and disadvantages.

Watermarking [2] is a very efficient data hiding technique. In this technique, noise tolerant signals are used. These noise tolerant signals are embedded in digital media for security purpose. The disadvantage comes with the introduction of these noise tolerant signals because sometimes it is impossible to extract the digital media at the receiver end.

In cryptography [3, 4], the secret data is encrypted by a key but any unauthorized access of the key can hamper the security of the secret data. If an intruder gets the key, then easily original data could be recognized by deciphering the ciphertext.

Steganography is a technique of hiding information within some digital cover media like text, image, audio, video. Steganography [5] consists of two Greek words—"*stego*" means "*cover*" and "*grafia*" means "*writing*"; defining as "*covered writing*." Steganography hides the existence of the secret data as the secret data is hidden in a carrier file. So the existence of secret data will remain unknown to the observer [6]. There are various image steganography techniques. Some are based on spatial domain, and in some cases, we need to consider pixel values in binary format. In spatial domain, the steganographer modifies the secret data and the cover medium which involves encoding at the level of the LSBs. LSB is the least significant bit in a series of numbers in binary [7]. For example in the binary number: 101100010, the least significant bit is the far right 0. In the LSB-based steganography to embed the secret data, the least significant bits of the pixel values in the cover images are used. Cover images are needed to hide secret data. Generally, cover images are of 8-bit gray level or color image [8]. Other popular techniques for image steganography are (a) **Discrete cosine transform** (DCT) [9] is a mathematical transformation that takes a signal or image and transforms it from spatial domain to frequency domain. So it can separate an image into high-, middle- and low-frequency components. For JPEG compression, DCT coefficients are used. And (b) **Discrete wavelet transform** (DWT) [10] in which the wavelet coefficients of the cover image are modified to embed the secret message. We have considered LSB-based steganographic technique in this paper. LSB-based methods manipulate the least significant bit (LSB) planes by directly replacing the LSBs of the cover image with the secret message bits. LSB methods typically achieve high capacity. Different LSB-based steganography methods are proposed in [11–15]. In the proposed scheme, the hiding of a secret image in one or more cover images has been explained where the original data has been encoded first. Then encoded data of the secret image has been embedded in such a way that undistorted recovery of the image is possible. Here for steganography a modified LSB technique has been used. Since the data has been encoded first and then hidden, such that the security has also increased. So, to achieve higher security two levels have been introduced in the approach. In the first level, all the bits of the secret image have been encoded, and in the second level, steganography has been carried out.

Rest of the paper is divided into five major parts; in Sect. 2, we have the discussion of the previous work done in the domain of steganography. Section 3 comprises the

proposed algorithm. Section 4 contains the experimental results and analysis of the result. Section 5 concludes the paper.

2 Related Study

In the proposed scheme, we first encode the image to break the correlation between the adjacent pixels. Our encoding scheme utilizes only bitwise XOR operations between consecutive bits in all the pixels of the secret image. For steganography, we have used LSB technique very similar to [16] proposed by Pathak et al.

2.1 Brief Discussion on Audio Steganograpy Scheme Based on Location Selection [16]

It considers a secret text T_s to be hidden in a cover audio file A_c (16-bit .wav format). Traditional LSB scheme converts the secret text T_s in binary format. Then, each bit will be replacing the bit at LSB position of each sample of the cover audio sequentially. Unlike traditional LSB, this scheme selects a specific bit from least significant eight bits of a sample where the secret binary bit will be inserted. Hence, it enhances the security of the stego-audio. The steps are as follows:

Embedding of secret. Consider the encrypted secret text T_s which is in binary format with m number of bits. Store the audio samples from the cover audio file A_c into an array $SAMPLES[]$.
Step 1: for $i = 1$ to m.
Step 1.1: Consider $SAMPLES[i]$ as cover sample.
Step 1.2: Compute the decimal equivalent of first (MSB) three bits as j.
Step 1.3: Insert the secret bit $T_s[i]$ at j position from LSB of $SAMPLES[i]$.
Step 2: Store the modified $SAMPLES[i]$ for ($i = 1$, to, m) into stego-audio file A_{stego}. Keep the rest of the samples in A_{stego} same as original cover A_c.
Step 3: Transfer the stego-audio file A_{stego} on public channel.

Extraction of secret. The encrypted secret message can be extracted if the number of bits in the secret text m is known to the receiver. The receiver performs the following actions to reveal the secret inside the stego-image.
Step 1: Store the audio samples from the stego-audio file A_{stego} into an array $SAMPLES[]$.
Step 2: for $i = 1$ to m.
Step 2.1: Consider $SAMPLES[i]$ as stego-sample.
Step 2.2: Compute the decimal equivalent of first (MSB) three bits as j.
Step 2.3: Extract the secret bit b_i from jth position from LSB of $SAMPLES[i]$.
Step 3.0: Combine the m bits as binary sequence as $b_m b_{m-1} \ldots b_2 b_1$ and regenerate the secret encrypted text T_s.

3 Proposed Method

In the proposed scheme, the inputs are the grayscale secret image ($n \times n$) and m grayscale cover images ($s \times r$). In this scheme, the secret image will be first encoded and then LSB-based steganography has been used to hide the secret image in cover images. For steganography, a modified LSB with location selection has been used. The process for encoding and embedding is as shown in Fig. 1, whereas extraction and decoding are as shown in Fig. 2.

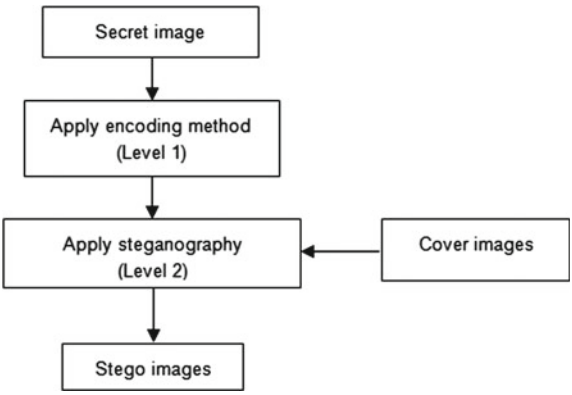


Fig. 1 Block diagram presenting embedding process

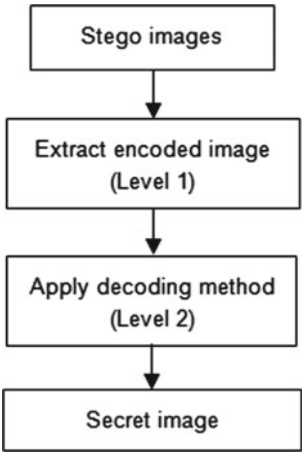


Fig. 2 Block diagram presenting extraction process

3.1 Embedding and Encoding Phase

1. Let I_s be the original secret image of $n \times n$ pixels. If the original image having $n \times k (k < n)$ pixels, then use sufficient padding to make it $n \times n$ pixels.
2. Now $n \times n \times 8$ bits of the secret image I_s will be embedded separately in each pixel (byte) of m cover images by using the method of encoding and steganography. If each cover image contains $s \times r$ pixels, then we need m cover images to embed $n \times n \times 8$ bits of secret image where $m = \lceil \frac{n \times n \times 8}{r \times s} \rceil$.
3. Now for each bit b_i; ($i = 1$ to $n \times n \times 8$) from the secret image I_s, each bit will be modified in the following manner:
   Suppose b_i is the original bit and t_i is the modified one where $i = 1$ to $n \times n \times 8$ then,
   $t_1 = b_1 \;\; if \;\; i = 1$
   $t_i = t_{i-1} \oplus b_i \;\; if \;\; i > 1 \; and \; i \leq n \times n \times 8.$
4. For steganography, we have m different cover images. As $n \times n \times 8$ bits to be concealed into $m \times s \times r$ bytes and number of bits from secret image is equal to total number bytes in cover images, we need to insert one bit in each byte (or pixel).
   For each bit t_i from secret encoded image and each byte (pixel) P_i from cover images (where $i = 1$ to $n \times n \times 8$) compute as follows:
   (a) Convert P_i to its 8-bit binary representation $\{p_8 p_7 p_6 p_5 p_4 p_3 p_2 p_1\}_2$.
   (b) Compute the decimal value for $\{p_8 p_7\}_2$ as d_i.
   (c) Insert the secret bit t_i at position $(d_i + 1)$ of the binary representation of P_i. The t_i will replace either p_1 or p_2 or p_3 or p_4.
5. By modifying specific one of the four least significant bits of each pixel of cover images, we achieve m stego-images.

3.2 Extraction and Decoding Phase

We first extract the secret bits from the stego-images, then construct the encoded secret image. After that apply decoding algorithm to retrieve the actual secret image.

1. For each byte (or pixel) P_i ($i = 1$ to $m \times r \times s$) from m stego-images extracts the secret bits t_i as follows:
   (a) Convert P_i to its 8-bit binary representation $\{p_8 p_7 p_6 p_5 p_4 p_3 p_2 p_1\}_2$.
   (b) Compute the decimal value for $\{p_8 p_7\}_2$ as d_i.
   (c) $t_i = p_{d_i+1}$.
2. After extracting $n \times n \times 8$ bits, reconstruct the encoded secret image.
3. For each bit t_i, $i = 1$ to $n \times n \times 8$ from encoded secret image compute the decoded bit b_i as follows:

$b_1 = t_1 \; if \; i = 1$
$b_i = b_{i-1} \oplus t_i \; if \; i > 1 \; and \; i \leq n \times n \times 8$

4. Now, from $b_i (i = 1 \text{ to } n \times n \times 8)$ generate the secret image I_s.

4 Experimental Results

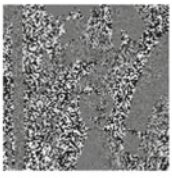
This section deals with the experimental results of the proposed method using MATLAB R2012a. For experiment, we have considered two grayscale cover images (mandril_gray.tif and cameraman.tif) of dimension 256×256 and one grayscale secret image (lena.tif) of dimension 128×128. Since we are going to embed $128 \times 128 \times 8$ bits of secret image in 256×256 pixels cover images, so we need $m = \frac{128 \times 128 \times 8}{256 \times 256} = 2$.

The secret image and two cover images are shown in Fig. 3a–c. After encoding, the encoded image is shown in Fig. 3d. By embedding the encoded secret bits, we get two stego-images as shown in Fig. 4a, b. The encoded image extracted from the stego-images is shown in Fig. 4c. The final decoded secret image is shown in Fig. 4d.

(a) Secret Image

(b) Cover Image-1

(c) Cover Image-2

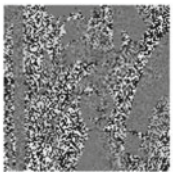


(d) Encoded image before embed

Fig. 3 Secret image (**a**), cover images (**b**), (**c**) and encoded image before embed (**d**)

(a) Stego Image-1

(b) Stego Image-2



(c) Extracted encoded image

(d) Final decoded image

Fig. 4 Stego-images (**a**), (**b**), extracted encoded image (**c**), and final decoded image (**d**)

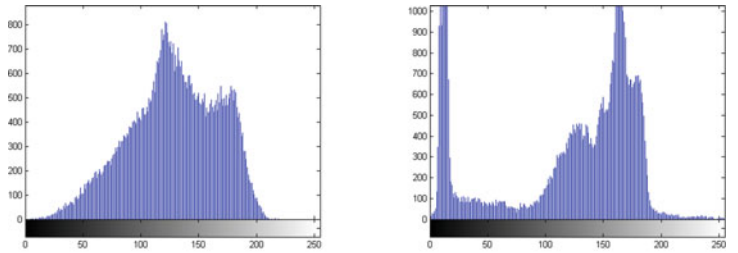
5 Analysis of Results

The cover images—mandril_gray.tif and cameraman.tif—are shown in Fig. 3b, c, whereas the corresponding stego-images are shown in Fig. 4a, b. The histograms of cover-image1 and stego-image1 (for mandril_gray.tif) are shown in Fig. 5a, c. Similarly, the histograms of cover-image2 and stego-image2 (for cameraman.tif) are shown in Fig. 5b, d. The stego-image and the cover image are compared to verify the quality of the obtained stego-image in the proposed scheme as follows.

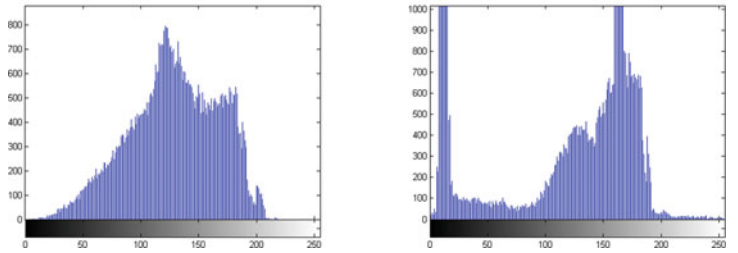
5.1 Mean Square Error (MSE)

The mean square error between the cover image $g(x, y)$ and stego-image $\hat{g}(\hat{x}, \hat{y})$ can be represented as:

$$MSE = \frac{1}{M \times N} \sum_{n=1}^{M} \sum_{m=1}^{N} [\hat{g}(n, m) - g(n, m)]^2$$



(a) Histogram of cover-image-1 (b) Histogram of cover-image-2



(c) Histogram of stego-image-1 (d) Histogram of stego-image-2

Fig. 5 Comparison of histogram of cover images and stego-images

The MSE values computed for mandril_gray.tif and cameraman.tif are 3.02 and 2.90, which is low considering other traditional steganography schemes means very little distortion induced to the stego-images by our algorithm.

5.2 Peak Signal-to-Noise Ratio (PSNR)

The quality of the image better represented by PSNR (as MSE having strong dependency image intensity scaling which does not effect PSNR). The PSNR can be calculated from MSE as:

$$PSNR = 10 \log_{10} \frac{S^2}{MSE}$$

where S is the maximum pixel value and result is measured in decibels (dB). The PSNR values computed for mandril_gray.tif and cameraman.tif are 43.36 and 43.55 dB, which is high considering other traditional steganography schemes means high quality of stego-images.

5.3 Structural Similarity Index Metric (SSIM)

SSIM index is used to find dissimilarities between two images. SSIM index value is within the range from 0 to 1. A value 0 presents two images that are all dissimilar and 1 means the images are identical. If two images are X and Y, the SSIM is defined as:

$$SSIM(X, Y) = \frac{(2\mu_X\mu_Y + C_1)(2\sigma_{XY} + C_2)}{(\mu_X^2 + \mu_Y^2 + C_1)(\sigma_X^2 + \sigma_Y^2 + C_2)}$$

where μ_X and μ_Y are the mean intensity of X and Y;
σ_X^2 and σ_Y^2 are the variance of X and Y;
σ_{XY} is the covariance between X and Y;
$C_1 = (k_1L)^2$, $C_2 = (k_2L)^2$ are two variables to stabilize the division with weak denominator and L is the dynamic range of the pixel values chosen as $L = 255$. The value of $k_1(\ll 1)$ and $k_2(\ll 1)$ are chosen as $k_1 = 0.01$, $k_2 = 0.03$.

SSIM index between cover image and stego-image calculated for mandril_gray.tif is 0.9879 and cameraman.tif is 0.9568, which implies that the stego-images are almost similar of the cover images.

6 Conclusion

In this paper, we have proposed a steganography scheme to conceal a secret image within multiple cover images. In proposed work, we have considered grayscale images only. But the scheme can be easily extended for color images, if we repeat the algorithm for each of the three color planes (RGB images). Before hiding, the secret image has encoded first using bitwise XOR operations (computationally low-cost operation) and then the encoded bits are inserted into multiple cover images. We have used a modified LSB technique which will select a bit position out of least significant four bits of a pixel of a cover image. For this scheme, we may need more than one cover image as each single bit from the secret image after encoding will be inserted in one byte (or one pixel) of the cover image. So, if the cover images are of less dimensions, then we may need more than one cover images. Then from those stego-images, we first extract the encoded secret image and decode it to regenerate the original secret image.

References

1. Fridrich, J.: Applications of data hiding in digital images. In: 5th International Symposium on Signal Processing and Its Applications (ISSPA). IEEE, Brisbane, Queensland, Australia (1999)
2. Nin, J., Ricciardi, S.: Digital watermarking techniques and security issues in the information and communication society: the challenges of noise. In: 27th International Conference on Advanced

Information Networking and Applications Workshops, pp. 1553–1558. IEEE, Barcelona, Spain (2013)
3. Kumari, S.: A research paper on cryptography encryption and compression techniques. Int. J. Eng. Comput. Sci. **6**(4), 20915–20919 (2015)
4. Huang, Q., Wong, D.S., Yang, G.: Heterogeneous signcryption with key privacy. Comput. J. **54**(4), 525–536 (2011)
5. Petitcolas, F.A.P., Anderson, R.J., Kuhn, M.G.: Information hiding a survey. Proc. IEEE **87**(7), 1062–1078 (1999)
6. Cachin, C.: An information-theoretic model for steganography. Inf. Comput. **192**(1), 41–56 (2004)
7. Kaur, N., Behal, S.: A survey on various types of steganography and analysis of hiding techniques. Int. J. Eng. Trends Technol. **11**(8), 388–392 (2014)
8. Samidha, D., Agrawal, D.: Random image steganography in spatial domain. In: International Conference on Emerging Trends in VLSI. Embedded System, Nano Electronics and Telecommunication System (ICEVENT), pp. 1–3. IEEE, Tiruvannamalai, India (2013)
9. Sheidaee, A., Farzinvash, L.: A novel image steganography method based on DCT and LSB. In: 9th International Conference on Information and Knowledge Technology (IKT), pp. 116–123. IEEE, Tehran, Iran (2017)
10. Surse, N.M., Vinayakray-Jani, P.: A comparative study on recent image steganography techniques based on DWT. In: International Conference on Wireless Communications. Signal Processing and Networking (WiSPNET), pp. 1308–1314. IEEE, Chennai, India (2017)
11. Wang, R.-Z., Lin, C.-F., Lin, J.-C.: Hiding data in images by optimal moderately-significant-bit replacement. Electron. Lett. **36**(25), 2069–2070 (2000)
12. Chan, C.-K., Cheng, L.M.: Hiding data in images by simple LSB substitution. Pattern Recognit. **37**, 469–474 (2004)
13. Karim, S.M.M., Rahman, M.S., Hossain M.I.: A new approach for LSB based image steganography using secret key. In: 14th International Conference on Computer and Information Technology (ICCIT), pp. 286–291. IEEE, Dhaka, Bangladesh (2011)
14. Sapra, P.S., Mittal, H.: Secured LSB modification using dual randomness. In: International Conference on Recent Advances and Innovations in Engineering (ICRAIE), pp. 1–4. IEEE, Jaipur, India (2016)
15. Blue, J., Condell, J., Lunney, T.: Identity document authentication using steganographic techniques: the challenges of noise. In: 28th Irish Signals and Systems Conference, pp. 1–6. IEEE, Killarney, Ireland (2017)
16. Pathak, P., Chattopadhyay, A.K., Nag, A.: A new audio steganography scheme based on location selection with enhanced security. In: First International Conference on Automation, Control, Energy and Systems (ACES), pp. 1–4. IEEE, Hooghy, India (2014)