PeerJ Computer Science   Manuscript to be reviewed

New deep data hiding and extraction algorithm using multi-channel with multi-level to improve data security and payload capacity

Hanan Hardan [1] , **Ali Alawneh** [Corresp., 1] , **Nameer El-Emam** [1]

[1] Philadelphia University, Amman, Jordan

Corresponding Author: Ali Alawneh
Email address: aalawneh@philadelphia.edu.jo

The main challenge in steganography algorithms is balancing between the size of the secret message (SM) that is embedded in the cover image (CI) and the quality of the stego-image (SI). This manuscript proposes a new steganography algorithm to hide a large size of secret messages in cover images with a high degree of non-perception in the resulting images. The proposed algorithm applied a multi-channel deep data hiding and extraction algorithm (MCDHEA) based on modified multi-level steganography (MLS) approach. It used a new modification of the least significant bits (NMLSB) to make it hard to extract a secret message from attackers. The secret message is distributed among n-blocks; each block is hidden into a sub-channel that includes multi-level hiding and flows into the main channel. Different grayscale images are used through the levels of each sub-channel and using the color image in the last level of the main channel. The image size of the multi-level is expanded from one level to the next level, and at each level, lossless image compression using the Huffman coding algorithm has been applied to enable the size of the data hiding at the next level. In addition, the encryption of secret messages and intermediate cover images based on the XOR encryption algorithm is applied before the hiding process. Finally, the number of bits to be replaced at each level for both sub and main channels is 4 bits per byte except at the last level of the main channel based on a new approach using a non-uniform number of bits replacements. This algorithm's performance is evaluated using various measures. The results show that the proposed technique is effective and better than the previous works concerning imperceptibility and robustness. Furthermore, the results show that the maximum peak signal-to-noise ratio (PSNR) of 61.2 dB for the payload of 18,750 bytes, the maximum video information fidelity(VIF) of 0.95 for the payload of 19,660 bytes, and the maximum structural similarity index measure (SSIM) of 0.999 for the payload of 294,912 bytes.

New Deep Data Hiding and Extraction Algorithm Using Multi-Channel with Multi-Level to Improve Data Security and Payload Capacity

Hanan Hardana[1], Ali Ahmad Alawneh[2], Nameer N. EL-Emam[3]

[1]Computer Science Department, Faculty of Information Technology, Philadelphia University, Amman, Jordan

[2]Management Information Systems Department, Faculty of Information Technology, Philadelphia University, Amman, Jordan

[1]Computer Science Department, Faculty of Information Technology, Philadelphia University, Amman, Jordan

Corresponding Author:
Ali Ahmad Alawneh[2]
Philadelphia University- Amman-Jordan
P. O. Box (1) Philadelphia, 19392- Amman – Jordan:
Email address: aalawneh@philadelphia.edu.jo

Abstract:

The main challenge in steganography algorithms is balancing between the size of the secret message (SM) embedded in the cover image (CI) and the quality of the stego-image (SI). This manuscript proposes a new steganography algorithm to hide a large size of secret messages in cover images with a high degree of non-perception in the resulting images. The proposed algorithm applied a multi-channels deep data hiding and extraction algorithm (MCDHEA) based on modified multi-level steganography (MLS) approach. It used a new modification of the least significant bits (NMLSB) to make it hard to extract a secret message from attackers. The secret message is distributed among n-blocks; each block hid into a sub-channel that includes multi-level hiding and flows into the main channel. Different grayscale images are used through each sub-channel's levels and the color image in the last level of the main channel. The image size of the multi-level is expanded from one level to the next level. At each level, lossless image compression using the Huffman coding algorithm has been applied to enable the size of the data hiding at the next level. In addition, the encryption of secret messages and intermediate cover images based on the XOR encryption algorithm is applied before the hiding process. Finally, the number of bits to be replaced at each level for both sub and main channels is 4 bits per byte except at the last level of the main channel based on a new approach using a non-uniform number of bits replacements. This algorithm's performance is evaluated using various measures. The results show that the proposed technique is effective and better than the previous works concerning imperceptibility and robustness. Furthermore, The results show that the best PSNR

41 and MSE are obtained as 67.3 dB and 0.012, respectively, for the payload of 25000 bytes. The
42 best VIF and NCC are obtained as 0.96 and 1, respectively, for the payload of 19,660 bytes.
43 Finally, the best SSIM is obtained as 0.999 for the payload of 294,912 bytes.

45
46

48 ***Keywords***: Multi-level steganography, Deep data hiding, Deep data extraction, Least significant bit (LSB),
49   Steganalysis, Huffman algorithm, XOR encryption.

Introduction

53 The rapid growth in communication and information technology with the unlimited use of the
54 Internet has made information security the most important factor daily to protect information
55 from attackers. There are two different approaches to information security. The first is
56 Cryptography, and the second is steganography, where both techniques are used to protect
57 confidential data from attacks. Furthermore, these two methods provide a higher security level
58 and confuse attackers.

60 Steganography is one of the essential techniques to hide secret data in different media like color
61 or gray images, audio files, video files, and text files. The objectives of the steganography
62 algorithm are:
63   - Hiding a high capacity of confidential data.
64   - Make an invisible of hiding data.

65 The hiding process of secret messages on gray or color images called cover images (CI) is
66 performed. In contrast, the image hiding information is called stego-image (SI). (Subramanian,
67 N.et al., 2021; Rehman, A. et al., 2018).

68 Image steganography applies in the frequency or spatial domain (Liao, X. et al.,2018). Both
69 environments have weaknesses and strengths; they hide information in the spatial domain much
70 better with lower computational, simplicity, and load capacity.

71

72 Many applications use various techniques based on spatial domain (Ghosal, S. et al., 2021;
73 Wang, J. et al., 2020; Kim, P. et al., 2020). These techniques are:
74   - Least Significant Bits (LSB),
75   - Laguerre transforms (LT),
76   - Exploiting Modification Direction (EMD),
77   - Pixel Value Difference (PVD),
78   - Pixel Pair Matching (PPM),
79   - Multi-Base Notation System (MBNS),
80   - Gray Level Modification (GLM).

81

82 Recently, many researchers developed analytical techniques to extract crucial hidden information
83 from the stego-image. In this work, the proposed hiding technique works against visual and

84   statistical attacks (Kang, Y. et al., 2019; Yang, C. et al., 2020; Jin, Z. et al., 2020). The main
85   challenge in steganography algorithms is balancing between the size of the secret message (SM)
86   that is embedded in the cover image (CI) and the quality of the stego-image (SI). This
87   manuscript proposes a new algorithm to hide a large-sized secret message in images with a high
88   degree of non-perception of secret data hiding in images.

89

90   The rest of the manuscript includes the following: the second section presents the related work,
91   and the motivation and objectives are shown in the third section. The fourth section presents a
92   multi-channel deep data hiding and extraction algorithm (MCDHEA) based on the modified
93   deep data hiding and extraction algorithm. The results discussions are shown in the fifth section,
94   and the sixth section offers the conclusions and future scope.

95

96

97   **Related Works**

98   Researchers modified several techniques based on single-level steganography (SLS) to ensure
99   preservation from various attacks using classical or modified LSB method (Arun, C. Murugan,
100   S. 2018). The other techniques use multi-level steganography (MLS) to enhance security and
101   increase the payload capacity.

102

103

104   Elshare, S., El-Emam, N. (2018) proposed a deep data hiding and extraction algorithm (DHEA)
105   to hide extensive secret data in multi-level color images. This algorithm improves the multi-level
106   steganography technique (MLS) and enhances the security and payload capacity. The best Peak
107   signal-to-noise ratio (PSNR), Structural Similarity (SSIM), and Euclidean norm ratios were
108   obtained as 63.2 dB for the payload of 2500 bytes, 0.9998 for the payload of 7864 bytes, and 205
109   for the payload of 7864 bytes, respectively. The advantage of the algorithm is that it is simply
110   due to the use of one channel with uniform levels. In contrast, the drawback of the algorithm is
111   that the payload capacity is limited due to the slight compression ratio. In addition, using one
112   channel instead of a multi-channel makes the hiding process performed sequentially instead of in
113   parallel.

114   Hacimurtazaoglu, M., and Tutuncu, K. (2022) proposed a deep data hiding algorithm using a
115   video steganography application. This algorithm is based LSB technique with a poly-pattern
116   block matrix (KBM) as the key. This key is a 64×64 pixel block matrix comprising 16 sub-
117   pattern blocks with a pixel size of 16×16. This technique was applied to improve robustness,
118   imperceptibility, and payload capacity. The best Mean square error (MSE), SSIM, and PSNR
119   values were obtained as 0.00066, 0.99999, and 80.01458 dB for the payload of 43827 bytes and
120   0.00173, 0.99999, and 75.72723 dB for the payload of 111616 bytes, respectively. The
121   advantage of the algorithm increases the unpredictability and resistance against statistical and
122   visual attacks. In contrast, the drawback of this algorithm is required a large size of the stego
123   video stream, and the number of video cover images is easy to detect by attacks. Moreover, this
124   algorithm uses a maximum payload of 184320 bytes, which does not have large enough.

125

Xue, P. et al. (2018) proposed a multi-dimensional steganographic method based on (MLS-ATDSS&NS) technique. This technique works under two steganography layers (audio and network steganography layers).   This technique is used to improve the security of covert communication based on the new multi-layer steganographic method (MLSATDSS&NS). As a result, the best PSNR and NC were obtained as 96.15 dB and 1 for the payload of 43069, respectively. The advantage of this technique is that it can achieve anti-detectability and robustness. The drawback of this technique is that using two layers in one channel is insufficient to embed high payload capacity and can not confuse the attackers.

Zhang, C. et al. (2020) proposed a novel universal deep data hiding (UDH) meta-architecture to hide and extract the encoding of a secret image from a cover image. This architecture performs extensive analysis and validates that the achievement of deep steganography can be accredited to a frequency difference between the cover image and the encoded secret image. Furthermore, this technique improves the dependent deep hiding (DDH) pipeline to produce a novel universal deep hiding (UDH) meta-architecture. The best results of PSNR, APD (average pixel discrepancy), Perceptual Similarity (PS), and SSIM were obtained as 39.18, 1.98, 0.0001, and 0.992 for the payload of 512 bytes respectively. The advantage of a novel universal deep hiding (UDH) meta-architecture is to disentangle the encoding of the secret image from the cover image and decode the secret image using high hiding capacity with visual quality. However, using one channel with deep data hiding is insufficient to increase the capacity and speed of processing.

 Ahmad, M. et al. (2021) constructed an improved deep data hiding and extraction algorithm (IDHEA) working on color images. This algorithm develops the hiding process by enhancing the security level and payload capacity by using a small size of the Cover-Image at the first level and gradually increasing the size of the Cover-Image from one level to the next according to the enlargement ratio. As a result, the best PSNR, Signal-to-Noise Ratio (SNR), MSE, and Euclidean norm ratios were obtained as 65.8 dB for the payload of 2500 bytes, 55.395, 0.0687 for the payload of 395310 bytes, and 155 for the payload of 78643 bytes. The advantage of the algorithm is that it is simply due to the use of one channel. In contrast, the drawback of the algorithm is that the security level is limited due to the use of one channel, and this approach makes the hiding process performed sequentially instead of in parallel.

 Dhall, S. et al. (2020) developed a multi-level security algorithm that uses quantum encryption of the texts. This algorithm improves the encryption and compresses the texts using the Huffman algorithm at two levels of security. The best PSNR, entropy, and correlation were obtained as 94.7, 6.3, and 0.99994 for the payload of 36 bytes, respectively. The advantage of the algorithm is based on respectable security due to applying the Huffman algorithm. In contrast, the drawback of the algorithm is that using two levels is inappropriate for confidential data to be incomprehensible.

162

Sayed, M., and Wahby, T. (2017) proposed a data hiding algorithm to enhance MLS. This algorithm enhanced LSB to hide secret data in BMP images using two levels (LSB-L1 and LSB-L2). As a result, the best PSNR and MSE were obtained as 67.91 and 0.01 for the payload of 270 bytes, respectively. The algorithm's advantage is that two enhancements of LSB are applied in data hiding. In contrast, the drawback of the algorithm using two levels is inappropriate for secret data.

Bhowal, K. (2019) presented multi-level audio steganography to describe a new hidden communication model in secret communication technology. This algorithm improved MLS using at least two embedding methods, so the second method is used the first method as a carrier. The best SNR was obtained as 92.54 dB for the payload of 44100 byte. The advantage of this algorithm is to increase the level of security while transmitting secure data over community channels and also can be used to deliver two or more data hiding solutions instantaneously. In contrast, the drawback of the algorithm using two levels with one channel is inappropriate for secret data.

Objectives and Motivation

The objectives of the proposed algorithm are to develop and improve several fundamental approaches for access to secure data. Among these approaches that have been developed are the Least Significant Bit (LSB) technology, the multi-level steganography algorithm, and the image and text segmentation to hide secret data randomly.
The Internet has a means available to give specific people legal permission to see confidential information. However, unfortunately, other people can access this confidential data who do not have legal permission. Data encryption is the most traditional strategy for preserving information, but this method has become easy for attackers. So the alternative way to encrypt data is to hide secret data and not arouse suspicion of its existence; this technique is often called data steganography.

The proposed steganography algorithm uses a multi-channel deep data hiding and extraction (MCDHEA) technique. This technique is applied to improve the previous work based on the (IDHEA) algorithm (Ahmad, M. et al., 2021) by using two types of channels. The main channel is the first type, whereas the sub-channel is the second type. The hiding algorithm suggested in this work is based on a new modified least significe bit (NMLSB) algorithm with Huffman compressing and XOR encryption techniques.

The proposed hiding algorithm aims to:
- achieve better hiding performance with the high payload capacity,
- confuse visual and statistical attackers to misleading where the blocks of SM have existed in the main channel and sub-channels,
- make the number of sub-channels and the number of levels at each channel unknown to attackers,

203   • make the stego-image (SI) at the last level of the main channel to closely match its
204   corresponding cover image (CI).
205 In the section "**Result and Discussions,**" we discussed all the above aims and confirmed that all
206 aims had been satisfied.

207 The motivation for proposing multi-channels instead of a single channel in this work is to avoid
208 sequential processing (hiding confidential data from one level to the next sequentially).
209 However, sequential processing needs much time if we hide a large amount of secret data.
210 Therefore, in this paper, we proposed a new approach based on multi-channels with multi-levels
211 at each channel to reduce the time of hiding a high payload capacity that can be working on
212 distributed systems.
213
214

The Suggested Hiding and Extraction Algorithm

216 This paper constructs a new data hiding and extraction technique to achieve high imperceptible
217 secret data in the stego-image. The proposed technique is preserving the superiority of the image
218 based on the new modification of least significant bits (NMLSB) discussed in the "Data hiding
219 algorithm" section.

220 Furthermore, this technique is based on deep data hiding and extraction algorithm working on a
221 multi-channel (MCDHEA).   This algorithm is the extended version of the old techniques such as
222 Multi-Level Steganography (MLS) (Mahdi, M. et al., 2019), deep data hiding and extraction
223 algorithm (DHEA) (Elshare, S., EL-Emam, N. 2018), and improved deep data hiding and
224 extraction (IDHEA) (Ahmad, M. et al., 2021). The proposed algorithm (MCDHEA) has been
225 implemented in two phases. The first phase applied a multi-channel deep data hiding algorithm
226 (MCDHA). In contrast, the second phase applied a multi-channel deep data extraction algorithm
227 (MCDEA).
228

Multi-channel deep data hiding algorithm (MCDHA)

230 The MCDHA is the modified version of the previous work (Ahmad, M. et al., 2021) by dividing
231 a secret message SM into n blocks {SM1, SM2, …, SMn}, and distributing these blocks on a
232 multi-channel. Where SMi is the ith secret message hidden into a cover image of the selected
233 channel index and level number at this channel randomly. Encryption and compression have
234 been applied to the outputs of the hiding process to generate encryption and compression stego-
235 image (ECSI). The process of hiding is continued through a sequence of cover images at the
236 specific channel until the hiding process has reached the main channel. Multi-level images have
237 been applied with progressive enlargement in image size to ensure that security and hidden data
238 are not perceptible (see Figure1).
239

Figure 1. Multi-channels deep data hiding

241
242 The secret message (SM) is divided into a uniform size of (n)-blocks; each block is hidden in one
243 channel. The hiding process is performed after being encrypted by the XOR key and compressed
244 by the Huffman coding algorithm. Then, the blocks are distributed randomly among channels
245 using the Fibonacci algorithm (Bommala, H. et al., 2020). Finally, the process of hiding is

246 applied using a new approach (NMLSB) based on Least significant bit (LSB). The proposed
247 hiding algorithm is applied to grayscale and color images, using the image size's expansion ratio
248 through the channel's level, see Figures 2-3.

249 | Figure 2: Distributed a secret message randomly among channels |
250

251 | Figure 3. Deep data hiding at the ith sub-channel |
252

253 The deep data hiding approach has been applied using the main channel containing N levels. For
254 each level (i) at the main channel, the cover image at the level (i) is divided into two parts; the
255 first part contains the hiding bits from the stego-image of the main channel at the level (i-1). In
256 contrast, the second part contains the hiding bits from a stego-image of a sub-channel. This
257 process continues until the main channel's level (N-1). The proposed hiding algorithm is based
258 on the new approach using a modified LSB (NMLSB) method with encryption and compression
259 algorithms. Finally, the two parts are joined together to generate a new stego-image created at
260 level (i), see Figure.4.

261 | Figure 4. Data Hiding of two parts into cover-image at the main channel using join process |
262

263 *The new modification of least significant bits (NMLSB)*

264 The hiding algorithm is carried out within the chain of levels of the main and sub-channels. This
265 process aims to produce a series of stego-images. The last level of the main channel includes a
266 color cover image (RGB image components). This image is used to hide the stego-image from
267 the penultimate level with the last block of the secret message to produce the last stego-image
268 SI_{MN}, see Figure 5.
269

270 | Figure. 5: Data hiding in the last level of the main channel using RGB cover-image |
271

272 Furthermore, the new modification of least significant bits (NMLSB) is based on the continuous
273 equation to find the number of hidden bits at ith byte(i) (Nbpbi). It is calculated according to Eq.
274 (1). Thus, it appears that the maximum value of (Nbpbi) is reached to 3 bits per byte if the
275 condition $\left(\sigma^{(\,(WSize-1)\,\times\,(WSize-1)\,)} > 18 \quad or \quad ED^{(WSize\,\times\,WSize)} > 250 \right)$ is satisfied.
276

$$
Nbpb_i = \begin{cases} 1 & if \ \left(\sigma^{(WSize\,\times\,WSize)} \leq 6 \right) \\ 2 & if \ \left(\sigma^{(WSize\,\times\,WSize)} > 6 \ and \ \sigma^{(WSize\,\times\,WSize)} \leq 18 \right) \\ 3 & if \ \left(\sigma^{(\,(WSize-1)\,\times\,(WSize-1)\,)} > 18 \ or \ ED^{(WSize\,\times\,WSize)} > 250 \right) \end{cases} \tag{1}
$$

277

278 Where $\left(\sigma^{(WSize\,\times\,WSize)} \right)$ is the standard deviation of window size (Wsize) at the cover image
279 when the (WSize=3), see Eq. (2).

$$
\sigma^{(WSize\,\times\,WSize)} = \left(\sqrt{\frac{1}{(WSize\,\times\,WSize)} \sum_{i=1}^{(WSize\,\times\,WSize)} \left(CI_i - \mu_i^{(WSize\,\times\,WSize)} \right)^2} \right) \tag{2}
$$

280

281   and ($\mu_i^{(WSize \times WSize)}$) is the mean of window (3x3) at the cover image around the ith location,
282   see Eq. (3).

$$\mu_i^{(WSize \times WSize)} = \frac{1}{WSize \times WSize}\sum_{j=1}^{WSize \times WSize} CI_j \tag{3}$$

284   The metric $(ED^{(WSize \times WSize)})$ is the edges detection filter calculated by using Sobel edge
285   detection filter (Tian, R. et al., 2021) with window size (WSize = 3), see Eqs. (4-6).

$$ED_{x,\,CI} = \sum_{i=0}^{WSize-1}\sum_{j=0}^{WSize-1} S_j D_i * CI_{ji} \tag{4}$$

$$ED_{y,\,CI} = \sum_{i=0}^{WSize-1}\sum_{j=0}^{WSize-1} S_i D_j * CI_{ji} \tag{5}$$

$$ED^{(WSize \times WSize)} = \sqrt{\left(ED_{x,\,CI}\right)^2 + \left(ED_{y,\,CI}\right)^2} \tag{6}$$

289   Where the two variables ($ED_{x,\,CI}$ and $ED_{y,\,CI}$) are calculated based on the Sobel edge detection
290   technique based on horizontal (x-axis) and vertical (y-axis) convolution of a cover image. The
291   Sobel operator for the x-axis is combined with optimal smoothing along the y-axis (S_j) with
292   optimal differencing along the x-axis (D_i), see Eq. (4), while the Sobel operator for the y-axis is
293   combined with optimal smoothing along the x-axis (S_i) with optimal differencing along the y-
294   axis (D_j), see Eqs. (7-10)

$$S_i = \frac{(WSize-1)!}{((WSize-1)-i)!} \quad , \quad S_j = \frac{(WSize-1)!}{((WSize-1)-j)!} \tag{7}$$

$$D_i = P_{i,WSize-2} - P_{i-1,WSize-2} \tag{8}$$

$$D_j = P_{j,WSize-2} - P_{j-1,WSize-2} \tag{9}$$

$$P_{s,r} = \begin{cases} \frac{r!}{(l-s)!\,*\,s!} & \text{if } s \geq 0 \ \ s \leq l \\ 0 & \text{Otherwise} \end{cases} \tag{10}$$

299   Where ($P_{s,r}$) is Pascal's triangle that gives sets of coefficients for a smoothing operator.

Data hiding algorithm

301   The proposed data hiding algorithm (MCDHA) is described in the following steps:

302   **Main-Algorithm: MCDHA**
303   /*
304   *Let SM be a secret message;*
305   *Let N be the depth of the main channel;*
306   *Let S be the depth of each sub-channel;*
307   *Let n be the number of channels;// where n channels are used; one main-channel and n-1 sub-*
308   *channels;*
309   *Let EK be the encryption key using the XOR approach;*

310 *Let SI be stego-image;*
311 *Let CSI be a compressed stego-image;*
312 *Let Ch_St_image be a stego-image from any channel;*
313 *Let M_Ch_St_Image be stego-image from the main channel;*
314 *Let RGB_CI be the color cover image;*
315 *Let RGB_SI be Color stego-image;*
316 *Let CI be a cover image;*
317 *Let Nbpb be the number of bits per byte;*
318 **/*
319 Step 1: Input N, S;
320 Step 2: Compute n= N-1;
321 Step 3: Divide the SM into (n) blocks {SM1, SM2, …, SMn}; //*number of blocks=number of*
322   *channels that include the main*
323   *and sub-channels.*
324 Step 4: Let i←0; // i is the block's index SMi.
325 Step 5: Set SM←SMi;
326 Step 6: Compute i←i+1;
327 Step 7: Input CI, EK;
328 Step 8: Call HidingInLevel (SM, EK, CI), which returns CSI; //*hiding in level 1 at the main*
329   *channel.*
330 Step 9: Set SM← CSI;
331 Step 10: Set M_Ch_St_Image ← SM;
332 Step 11: For (level ←2 to N-1) Do   // *Passing M_Ch_St_image to the next level of the main*
333   *channel starting from (level 2).*
334   Step 11-1: Set SM←SMi;
335   Step 11-2: Compute i←i+1;
336   Step 11-3: Call HidingInChannel (SM, S) which returns Ch_St_Image;
337   Step 11-4: Input CI;
338   Step 11-5: Input EK;
339   Step 11-6: Call JoinStegoImagesInMainChannel (M_Ch_St_Image, Ch_St_Image, CI,
340   EK) which returns a new stego-image; // *Passing Ch_St_Image to the main*
341   *channel.*
342   Step11-7: Set M_Ch_St_Image= CSI;
343   End for.
344 Step 12: Input RGB_CI, EK, Nbpb; // *calculate Nbpb according to Eq.(1).*
345 Step 13: Call HidingInRGB-Image (M_Ch_St_Image, RGB_CI, EK, Nbpb,) which Return SI;
346   // *passing M_Ch_St_Image to HidingInRGB-Image.*
347 End MCDHA.
348
349 **Sub-Algorithm 1: HidingInChannel(.)**

350 Step 1: input SM, S
351 Step 2: Do
352   Step 2-1: Input CI
353   Step 2-2: Input EK;
354   Step 2-3: Call HidingInLevel (SM, EK, CI) which return CSI;
355   Step 2-4: Set SM← CSI;   // passing CSI to the next level of sub-channel.

356   Step 2-5: Compute S← S-1;
357   While (S≠0);
358 Step 3: Find Ch_St_Image;
359 End HidingInChannel.
360

361 **Sub-Algorithm 2: HidingInLevel(.)**
362 Step 1: input SM, EK, CI;
363 Step 2: Check the type of SM, whether it is a text or an image;
364 Step 3: Convert SM into integer value representation;
365 Step 4: Find total hiding pixel and total hiding data to ensure sufficient hiding space;
366 Step 5: Encrypting SM using EK;
367 Step 6: Hiding data in CI using NMLSB Algorithm and return SI;
368 Step 7: Compressing SI using Huffman coding algorithm, which returns CSI;
369 Step 8: Output CSI;
370 End HidingInLevel.
371

372 **Sub-Algorithm 3: JoinStegoImagesInMainChannel(.)**
373 Step 1: Input M_Ch_St_Image and Ch_St_Image, CI, EK;
374 Step 2: Divide CI into 2 parts {part1, part 2};
375 Step 3: Hiding M_Ch_St_Image in part1 and Ch_St_Image in part2 using NMLSB and return a
376   new SI;
377 Step 4: Compressing SI using Huffman coding algorithm, which returns CSI;
378 Step 5: Passing a new CSI to the next level in the main channel;
379 End JoinStegoImagessInMainChannel.
380

381 **Sub-Algorithm 4: HidingInRGB-Image(.)**
382 Step 1: input M_Ch_St_Image, RGB_CI, and EK;
383 Step 2: Hide the M_Ch_St_Image using an (R, G, B) order along the rows moving from left to
384   right using the NMLSB algorithm based on Nbpb;// see Eq. (1)
385 Step 3: Return SI;
386 End HidingInRGB-Image.
387

388 ***Multi-channel deep data extraction algorithm (MCDEA).***

389 The main channel contains N levels; these are used to hide and extract (n) blocks of a secret
390 message (SM) beside a sequence of intermediate stego-images. The extraction process has been
391 implemented back-word from level (N) to level (1) for the main channel and from level S to
392 level 1 from each sub-channel., see Figure 6.

393

394 | Figure. 6: Data Extraction from the main and sub-channels |
|---|

395 The extraction process at the ith level of the main channel produces two parts; the first part
396 contains the stego-image of the $(i-1)^{th}$ level. In contrast, the second part contains the stego-image
397 of the sub-channel at the specific level (i), see Figure 7.

398 | Figure 7. Data Extraction from two channels

399 The secret message is extracted according to the proposed NMLSB after decompression by
400 Huffman coding algorithm and decryption by the XOR key for the main channel and each sub-
401 channel. See Figure 8.

402 | Figure.8: Data Extracting in many levels of one sub-channel

403 The (n) blocks of secret messages extracted from the main channel and sub-channels are joined
404 together after reordering blocks' indexes from random distribution into ascending order of
405 blocks' indexes using the Fibonacci algorithm21 to obtain a required secret message SM, see
406 Figure 9.

407 | Figure 9: Data Extracting from main and sub-channels to find SM

408

409 *Data extraction algorithm*

410 The description of the suggested extraction algorithm (MCDEA) appears in the following
411 algorithm steps:

412 **Main-Algorithm: MCDEA Algorithm**
413 */**
414   *Let SM be a secret message;*
415   *Let N be the depth of the main channel;*
416   *Let S be the depth of each sub-channel;*
417   *Let n be the number of channels;// where n channels are used; one main-channel and n-1*
418   *sub-channels;*
419   *Let DK be the decryption key using the XOR approach; // DK=EK*
420   *Let SI be stego-image;*
421   *Let CSI be a compressed stego-image;*
422   *Let Ch_St_Image be a stego-image from any channel;*
423   *Let M_Ch_St_Image be stego-image from the main channel;*
424   *Let RGB_CI be the color cover image;*
425   *Let RGB_SI be color stego-image;*
426   *Let CI be a cover image;*
427   *Let Nbpb be the number of bits per byte;// using Eq.(1)*
428 **/*
429 Step 1: input CSI-RGB, DK, N, S Nbpb;
430 Step 2: Call ExtractFromRGB (RGB_SI, DK) which return Stego-Image; // Retrieve the CSI
431   from RGB_SI at the last level.
432 Step 3: Call Extraction (Stego-Image, DK, N, S) returns the SM; // Retrieve the CSI from SI for
433   the levels N-1 to 1.
434 Step 4: Extract text message from SM;
435 Step 5: Send a text message to the output file;
436 End MCDEA.
437

438   **Sub-Algorithm1: ExtractFromRGB (.)**
439   Step 1: input RGB_SI, and DK, Nbpb;
440   Step 2: Return the CSI by scanning RGB_SI using row-wise scanning from left to right using the
441   NMLSB algorithm;
442   Step 3: Return CSI;
443   End ExtractFromRGB.
444
445   **Sub-Algorithm2: Extraction (.)**
446   Step 1: Input CSI, DK, N, S
447   Step 2: Decompress of CSI to find SI;
448   Step 3: If (N=1) then
449   Step 3-1: T=Decode (SI, DK);
450   Else If (N=2) then
451   Step 3-1: t1=Decode (SI, DK);
452   Step 3-2: T=Decode (t1, DK);
453   Else // Divided the SI into two parts to retrieve the secret message from each part.
454   Step 3-1: sub1=SplitGray (SI);
455   Step 3-2: Y2=Decode (sub1 {1, 1}, DK);
456   Step 3-3: C2=Decode (sub1 {2, 1}, DK);
457   Step 3-4: T2=Extraction (C2, DK, 2, S);
458   Step 3-5: T1=Extraction (Y2, DK, N-1, S);
459   Step 3-6: T=Strcat (t1, t2); //Merging retrieved messages from sub-channels and
460   the main channel.
461   End If.
462   End If.
463   Step 4: Return the SM;
464   End Extraction.
465
466   **Sub-Algorithm3: Decode (.)**
467   Step 1: Input SI, DK;
468   Step 2: Return the encrypted message, whether it is a text or image (stego-image);
469   Step 3: Message decrypted using same symmetric XOR DK;
470   Step 4: Return SM;
471   End Decode.
472

473   *Implementation of multi-channel deep data hiding algorithm (MCDHA)*

474   Suppose that one byte from stego-image SI is used in the 4th level of the main channel ($SI_{M,4}$).
475   Next, we select one byte from stego-image in the sth level of the ith sub-channel ($Si_{i,s}$). These
476   bytes are used to perform hiding into the cover image in the 5th level of the main channel ($CI_{M,5}$).
477   In this algorithm, hiding a sequence of bits from each byte into the cover image ($CI_{M,5}$) is applied
478   to generate the corresponding stego-image ($SI_{M,5}$). The proposed algorithm uses four bits to be
479   hidden into each byte at the cover image. As a result, it generates a stego-image at the next level
480   of the main channel ($SI_{M,5}$). Thus, the cover image used for hiding bits is partitioned into two
481   parts; the first part holds the hiding bits from the previous stego-image ($SI_{M,4}$). In contrast, the

482   second part holds the hiding bits from the stego-image in the sth level of the sub-channel ($SI_{i,s}$),
483   see Figure 10.

484   Figure. 10: Implementation of the hiding process in the main channel

485

486

Result and Discussions

488   In this section, the experimental results are applied to evaluate the performance of the suggested
489   algorithm. Many experiments have been performed using grayscale and color images with the
490   size (512×384 and 384×512) pixels from the UCID v2 database (Schaefer, G., Stich 2004). In
491   addition, standard-test-images datasets such as (Barbara, Baboon, Peppers, and Airplane) with
492   the size (512×512) are used to compare with the previous works. Furthermore, in this paper,
493   various measures have been discussed in the following sections to justify the security level and
494   payload capacity.

Payload capacity vs. image quality

496   The mean square error (MSE), Peak signal-to-noise ratio (PSNR), and Normalized Cross-
497   Correlation (NCC) are defined in Eqs. (11-14), and they are used to evaluate the performance of
498   the suggested hiding algorithm.

499
$$PSNR = 10 * \log_{10} \frac{255 * 255}{MSE} \tag{11}$$

500
$$MSE = \frac{MSE_R + MSE_G + MSE_B}{3} \tag{12}$$

501   where MSEi for $i \in \{R, G, B\}$ are the mean square error for the Red, Green, and Blue image
502   colors.

503
$$MSE_k = \frac{1}{m*n} \sum_{i=1}^{m} \sum_{j=1}^{n} (CI_{ij} - SI_{ij})^2 \ ; k \in \{R,G,B\} \tag{13}$$

504   where (i, j) is the pixel at the cover image and stego-image.

505
$$(NCC)_{i,j} = \frac{\sum_{i}^{m} \sum_{j}^{n} ((CI_{ij} - \mu_{CI}) \times (SI_{ij} - \mu_{SI}))}{\sqrt{\sum_{i}^{m} \sum_{j}^{n} (CI_{ij} - \mu_{CI})^2} \sqrt{\sum_{i}^{m} \sum_{j}^{n} (SI_{ij} - \mu_{SI})^2}} \tag{14}$$

506   Where (μ_{CI}, and μ_{SI}) are the average pixels of cover and stego-images, respectively.

507   The proposed MCDHEA algorithm aims to make the value of (MSE) low, the value of (PSNR)
508   high, and the value of (NCC) is closed to one. These scale values are necessary to make it
509   difficult for the visual or statistical attacks to notice changes in the cover image. The proposed
510   hiding algorithm is based on bit replacement using NMLSB. This algorithm is compared with

511   previous works such as the MDLSB algorithm by (Elshare, S., EL-Emam, N. 2018), the MLSB
512   algorithm by (Ahmad, M. et al. 2021), reversible data hiding by (Ou, B. et al., 2015), and the
513   noise-like binary image blocks by (Li, J. et al., 2013), see Table 1.
514

515 | Table 1. Performance of the proposed algorithm MCDHEA. |

516   Moreover, the metrics MES, PSNR (dB), and NCC are calculated at the last level of the main-
517   channel $SI_{M,N}$ of the proposed deep data hiding algorithm. According to these metrics ' results,
518   different payload capacities on three stego-images (from the standard-test-images) are applied to
519   show the system performance. Furthermore, the proposed approach results have been compared
520   with the previous works (Elshare, S., El-Emam, N. 2018; Ahmad, M. et al., 2021; Ou, B. et al.,
521   2015; and Li, J., et al., 2013). As a result, the average PSNR for the three images using the
522   proposed hiding algorithm is better than the results of the previous algorithms for the same
523   images with the same data hidden capacity. Moreover, the suggested hiding algorithm that
524   generates the "Barbara" stego-image is better than the previous works mentioned above by
525   approximately 8.17%, N/A, 12.51%, and 14.05%, respectively. Furthermore, the Baboon stego-
526   image generated by the proposed algorithm is better than the previous works by approximately
527   12.37%, 9.40%, 15.57%, and 15.35%, respectively. Finally, the "Peppers" stego-image generated
528   by the suggested algorithm is better than the previous works by approximately 11.28%, 8.08%,
529   15.92%, and 16.30%, respectively. However, the present work results show the highest average
530   of PSNR is 63.8(dB), which appears in the "Peppers" stego-image. In contrast, the lowest
531   average of PSNR is 63.18 (dB) in the "Baboon" stego-image. Accordingly, the present work
532   results illustrate that when the payload sharply increases, the PSNR gradually declines.
533   Moreover, the proposed hiding algorithm results confirm that the maximum and the minimum
534   averages of MSE for the three stego-images are 0.037 and 0.0304 for the "Barbara" and
535   "Peppers" stego-images, respectively. In addition, the highest average of Normalized Cross-
536   Correlation NCC results of the three stego-images is 0.99998 for the "Baboon" stego-image.
537   Accordingly, the suggested hiding algorithm achieves the best performance for all payload
538   capacities.
539

540   In addition, the difference (Diff) between the secret message before hiding (SM^H) and the secret
541   message after extraction (SM^E) is checked in Table1. The results of Diff approved that the
542   suggested algorithm can extract the same secret message before the hiding process by evaluating
543   the difference according to Eq. (15).

544   $$\text{Diff} = \sum_{i=1}^{|SM|} \left| SM_i^H - SM_i^E \right|$$ (15) where (SM_i^H) is the ith character of

545   the secret message before the hiding process. Furthermore, Figure 11 shows the PSNR values
546   obtained by the suggested algorithm and RDH algorithm by (Li, J. et al. 2013) for the first 50
547   images in the UCID database with the payload capacity of 250×10^3 bit. Results settle that the
548   suggested algorithm has a more considerable PSNR value for all images. The maximum
549   difference between the two algorithms equals 10.266 (dB). Furthermore, it appears in the image
550   index (32). In contrast, the minimum difference between the two algorithms equals 8.547 (dB),
551   appearing in the image index (37).
552

553   Figure 11. The PSNR values of the first 50 images in the database UCID with payload capacity
554   $250×10^3$ bit. Using the Orange line for (Li, et al., 2013) and the Blue line for the
555   proposed algorithm MCDHEA.

556

557

558   ***Structural similarity index measure (SSIM)***

559   The structural similarity index measure (SSIM) is a model of comparison metric to check the
560   structural similarity between two images. It is calculated using Eq. (16).

561
$$\text{SSIM(CI, SI)} = \frac{\left(2\mu_{\text{CI}}\mu_{\text{SI}} + ((2^{24}-1)*0.01)^2\right)\left(2\sigma_{\text{CI, SI}} + ((2^{24}-1)*0.03)^2\right)}{\left(\mu_{\text{CI}}^2 + \mu_{\text{SI}}^2 + ((2^{24}-1)*0.01)^2\right)\left(\sigma_{\text{CI}}^2 + \sigma_{\text{SI}}^2 + ((2^{24}-1)*0.03)^2\right)} \tag{16}$$

562   where μ_{Ic} and μ_{Is} metrics represent the average of the cover and stego images, respectively,
563   σIcIs metric represents the covariance between the cover and the stego images, and $(\sigma_{\text{Ic}}^2, \sigma_{\text{Is}}^2)$
564   represents the variance between the cover and the stego images (Elshare, S., El-Emam, N. 2018).

565   Structural similarity index measure (SSIM) is introduced in this study to check the image quality
566   and attack resistance by calculating the similarity between the cove-images and corresponding
567   steg-images. Comparisons with the previous hiding algorithms (Elshare, S., EL-Emam, N. 2018)
568   and (Li, J., et al., 2013) have been made by using fifty color images selected randomly within the
569   sizes (512×384 and 384×512) from the UCID v2 database for three payload capacities (20%,
570   30%, and 40%). It found that the suggested hiding algorithm achieved excellent performance see
571   Table 2.

572
573   Table 2. The Average values of SSIM by different steganography algorithms
574
575   Figure 12. The SSIM values of the first 50 images in the database UCID with payload capacity
576   $250×10^3$ bit.

577   Figure 12 shows the SSIM values obtained by the suggested algorithm for the first 50 images in
578   the UCID database with a payload capacity of $250×10^3$ bit. Results show that the maximum
579   SSIM equals 0.9998, appearing in the image indexes (46-48, 49-50).

580   ***Euclidean norm test***

581   The Euclidean norm is defined in Eq. (17); this test demonstrates that the suggested algorithm
582   works well against visual attacks. The distance (D) between the corresponding color {R, G, B}
583   of both cover and stego-images is calculated.

584
$$D = \sqrt{(R_{\text{CI}} - R_{\text{SI}})^2 + (G_{\text{CI}} - G_{\text{SI}})^2 + (B_{\text{CI}} - B_{\text{SI}})^2} \tag{17}$$

585 Results of Euclidean norm (D) appeared in Figures (13-14) for two-color images with image size
586 (512 × 512) with the payload percentages are 10%, 30%, and 40%. The purpose of the suggested
587 algorithm is to compare the results with the previous works: the MDLSB algorithm (Elshare, S.,
588 EL-Emam, N. 2018), and (El-Emam, N. Al- Zubidy, R. 2013).

589

590 | Figure. 13: Euclidean norm testing of Baboon's image. Using the Blue color (El-Emam N.,
591 | 2013), the Green color (Elshare, S. 2018), and the Yellow color for the proposed algorithm
592 | MCDHEA.

593

594

595 | Figure. 14: Euclidean norm testing of Peppers' image. Using the Blue color (El-Emam N., 2013),
596 | the Green color (Elshare, S. 2018), and the Yellow color for the proposed algorithm MCDHEA.

597

598 The Euclidean norm distances of two images have been calculated individually; the minimum
599 and the maximum average of the norm for three payloads are 392 and 413 at the "Peppers" and
600 "Baboon" images, respectively. In addition, the smallest and the most significant difference
601 between the average norm of the proposed algorithm and the others are 137 and 203 at the
602 "Baboon" image for the works (Elshare, S., EL-Emam, N. 2018) and (El-Emam, N. Al- Zubidy,
603 R. 2013) respectively.

604 Furthermore, the most significant difference in the Euclidean norm reached D=360.35 at the
605 image "Pepper," with a load ratio of 40%. It appeared between the proposed algorithm and the
606 previous work (El-Emam, N. Al-Zubidy, R. 2013). At the same time, the slightest difference in
607 the Euclidean norm reached D=9.51 at the image "Baboon" with a load ratio of 10%. It appeared
608 between the proposed algorithm and previous work (Elshare, S., EL-Emam, N. 2018).
609
610 ***The difference between adjacent pixels***

611 The difference between adjacent pixels of a cover image and its corresponding stego image was
612 calculated by using Eqs. (18-19), where the scales ($D_{i,j}^{cI}$ and $D_{i,j}^{sI}$) represent the absolute
613 difference in the adjacent horizontal pair to CI and SI (El-Emam, N. 2015).

$$D_{i,j}^{CI} = |CI_{i,j} - CI_{i,j+1}| \qquad (18)$$

$$D_{i,j}^{SI} = |SI_{i,j} - SI_{i,j+1}| \qquad (19)$$

616 Where ($CI_{i,j}$ and $SI_{i,j}$) are two pixels at the location (i, j) in the cove-image and the
617 corresponding stego-images, respectively.   In this test, three-color stego-images with size (512 ×
618 512) from the last level of the main channel with a payload capacity equal to 40% of the image
619 size are used. The difference values ($D_{i,j}^{CI}$ and $D_{i,j}^{SI}$) belong to the interval [-255, +255], and the
620 frequency of each of these different values was counted. Figures (15-16) illustrate a graph of the

621   pixel difference value on the X-axis and the frequency on the Y-axis. Results show that the
622   difference value between the stego-image and the cover image is closed.

623   Figure. 15: Dissimilarity between adjacent pixels of Peppers image with a payload of 40%, using
624   Red color for the cover image and Blue color for the stego-image of the proposed algorithm
625   MCDHEA.

626

627   Figure. 16: Dissimilarity between adjacent pixels of Baboon image with a payload of 40%, using
628   Red color for the cover image and Blue color for the stego-image of the proposed algorithm
629   MCDHEA.

630
631
632   ***Using the visual information fidelity (VIF) model***

633   The VIF test is used to assess the loyalty of the stego-image to the corresponding cover image.
634   This test is based on the reference field (RD), natural scene statistics NSS, and the mixture of
635   Gaussian scale (GSM) with the image distortion (ID) and the human visual system (HVS) (Han
636   et al. 2013) and (El-Emam 2015).   VIF test is calculated using Eq. (20), where this equation
637   includes two mutual information measures. The first measure of the VIF test is based on the
638   information exchanged between inputs and outputs of HVS channels without channel distortion.
639   In contrast, the second measure of the VIF test is based on the information exchanged between
640   the inputs and the outputs of the distorted HVS channels. The output of the HVS channels is a
641   stego-image

642

$$\text{VIF} = \frac{\sum_{j \in \text{sub\_band}i \in \text{block}} \log_2\left(\frac{\left(\sigma_{ji}^{CI,SI}\right)^2}{\left(\sigma_{ji}^{SI}\right)^2 \times \left(\sigma_{ji}^{CI}\right)^2 - \left(\sigma_{ji}^{CI,SI}\right)^2 + \sigma_\mu^2 \times \left(\sigma_{ji}^{CI}\right)^2} + 1\right)}{\sum_{j \in \text{sub\_band}i \in \text{block}} \log_2\left(\frac{\left(\sigma_{ji}^{CI}\right)^2}{\sigma_\mu^2} + 1\right)} \qquad (20)$$

643

644   where(σ_{ji}^{CI} and σ_{ji}^{SI}) are the standard deviation of the cover image (CI) and stego-image (SI) in
645   the ith block at the jth sub-band, respectively. The covariance of CI and SI in the ith block at the
646   jth sub-band is defined in ($\sigma_{ji}^{CI,SI}$) is, see (Han et al., 2013).

647   Table 3: The average values of VIF for three stego-images
648
649   In Table 3, the VIF measure is reported to demonstrate visual information fidelity. In this work,
650   testing on three images from the database of the standard color images (Imtiaz M. S.) with the
651   sizes (256×256) pixels are applied. The proposed hiding process is studied using the payload
652   capacities and the VIF metric. The measurement of results confirmed that the suggested

653   algorithm is better than the typical reference (El-Emam, 2015). The suggested algorithm is
654   working adeptly.

655

656

657

658   ***Testing Chi-square ($\chi 2$) attack***

659   The primary purpose of the suggested hiding algorithm is to hide a secret message SM in the
660   color image without realizing the presence of hidden data. Chi-square test is used in this situation
661   to check color uniformity in stego-images by verifying how the expected (E_i) and observed (O_i)
662   frequencies of stego pixels are structured (Ahmad, M. et al. 2021).

663

664 $$\chi_{s-1}^2 = \sum_{i=0}^{s-1} \frac{(O_i - E_i)^2}{E_i} \tag{21}$$

665   where (s) is the number of classes in the stego-image, (s-1) is a degree of freedom, and (E_i) is the

666   expected frequency of (i^{th}) pair see Eq. (22).

667 $$E_i = \frac{1}{2} \operatorname*{fr}_{\forall\,color} \{P_{2i}, P_{2i+1}\}, \forall i = 0,...,s-1 \tag{22}$$

668   where, $\{P_{2i}, P_{2i+1}\}$ is the ith pair of pixels $\{P_0, P_1,...,P_{255}\}$. The frequency observed at the (i^{th})
669   color is shown in Eq. (23).

670 $$O_i = fr(C_i) \quad \forall i = 0,...,s-1 \tag{23}$$

671   The probability ($Pr_{\chi^2, s-1}$) based on Chi-square value (χ^2) with (s - 1) degree of freedom is

672   calculated using Eq. (24).

673 $$Pr_{\chi^2, s-1} = \left(2^{\frac{s-1}{2}} \Gamma\left(\frac{s-1}{2}\right)\right)^{-1} \int_{\chi^2}^{\infty} (X)^{\frac{s-1}{2}-1} e^{-\frac{X}{2}} dX \tag{24}$$

674   Where the Gamma ($\Gamma(.)$) that appears in Eq.(24) is a factorial function, see Eq. (25).

675 $$\Gamma(Z) = \int_0^\infty X^{Z-1} e^{-X} dX \tag{25}$$

676   The Chi-square attack on a stego-image with randomly distributed secret messages was studied.
677   The proposed hiding algorithm verified comparisons between the two cover images (Baboon and
678   Peppers) and their corresponding stego-images. The probability (Pr) values at the beginning of
679   the block at the color image are irregular. With the block size increasing, the Pr value eventually
680   drops to zero.
681   Figure 17(A-D) illustrates the probabilities' results concerning the block sizes. The maximum
682   block size reached 20 and 25 for the Baboon image and 25 and 50 for the Peppers image when
683   the secret message length equals 25% and 50%, respectively.

684 Therefore, steganalysis cannot detect SM due to the identical Pr for the stego-images and their
685 corresponding cover images.

686 Figure 17: A-Probability of hiding a secret message (SM) of length 25% of the Baboon
687 image size, B-Probability of hiding a secret message (SM) of length 50% of the
688 Baboon image size, C-Probability of hiding a secret message (SM) of length
689 25% of the Peppers image size, D-Probability of hiding a secret message (SM) of
690 length 50% of the Peppers image size, using Blue line for the cover image and
691 using Red line for stego-image of the proposed algorithm MCDHEA.

692
693
694 ***Estimate the probability of detection error (P_E)***

695 The proposed multi-channel based on a deep data hiding algorithm can imperceptibly hide secret
696 data and resist attacks even in largely hidden payloads. The algorithm's performance in data
697 hidden can be checked by calculating the probability detection error (PE) expressed in equation
698 Eq.(26).

699
$$P_E = min\left(\tfrac{1}{2}\left(P_{FA} + P_{MD} \right)\right) \tag{26}$$

700 Let the metrics (#CISI and #SICI) be the number of cover images recognized as stego-images
701 and the number of stego-images recognized as cover images, respectively. Therefore the
702 probability of false alarms (PFA) and miss detection (PMD) are calculated in Eqs(27,28).

703
$$P_{FA} = \frac{\#CI_{SI}}{\#CI} \tag{27}$$

704
$$P_{MD} = \frac{\#SI_{CI}}{\#SI} \tag{28}$$

705 where $P_{FA}, P_{MD} \in [0,1]$

706 The detection error (PE) value range from 0 to 0.5. When PE = 0, discovering secret data is
707 optimal, while PE = 0.5 means perfect security and difficulty accessing secret data.
708 Figure 18 shows the probability detection error (PE) as a function of the payload capacity
709 represented by the number of bits per pixel (bpp). This function measures the area under the
710 curve (AUC), where excellent security is reached when the area of AUC is large. The proposed
711 deep data hiding algorithm result shows that the mean value of PE equals 0.467. This result is
712 better than the previous works (Elshare, S., EL-Emam, N. 2018; Ahmad, M. et al., 2021) by
713 about 3.8% and 2.2%, respectively. Moreover, the excellent security percentage reaches 98%
714 when bpp=0.05, whereas the worst security percentage reaches 86% when bpp=0.4.
715

716 Figure 18. Calculate the probability of detection error P_E as a function of the payload capacity.
717 Using the Orange line for DHEA (Elshare, 2018), the Blackline for IDEA (Ahmad, M. 2021),
718 and the Blue line for the proposed algorithm MCDHEA.

719
720
721
722
723

Conclusion and Future Scope

725 This paper proposes a new steganography algorithm based on a multi-channel deep data hiding
726 and extraction algorithm (MCDHEA). This algorithm is applied to develop the previous works
727 (DHEA) (Elshare, S., EL-Emam, N. 2018) and (IDHEA) (Ahmad, M. et al., 2021). The
728 proposed hiding algorithm is based on the new approach of the modified least significant bit
729 (NMLSB) to enhance data hiding security. However, the proposed hiding and extraction
730 algorithm can confuse attackers because they cannot answer the questions: How many channels
731 are used? How many levels are selected in each channel? Moreover, how is the secret message
732 distributed on multi-channel?
733 The XOR encryption and Hoffman image compression are introduced to raise the security level
734 due to the deep data hiding approach to generate one stego-image. The experimental results
735 show that the proposed algorithm finds the best way to avoid the problem of a high load capacity
736 of secret data. Moreover, results validate that deep dissimilarity is appreciated and obtain a more
737 significant hiding rate. Finally, all benchmark results indicate that attackers cannot detect secret
738 messages SM in the stego-image that appear at the last level of the main channel. The proposed
739 deep data hiding can be enhanced in future work by applying deep learning to perform adaptive
740 distribution of secret message SM among channels. This approach is based on partitioning SM
741 into non-uniform sizes and randomly hiding these partitions on channels, making it hard to
742 detect SM by attacks. This approach aims to enhance the new algorithm's performance according
743 to the evaluation criteria for image steganography. The results show that the best PSNR and
744 MSE are obtained as 67.3 dB and 0.012, respectively, for the payload of 25000 bytes. The best
745 VIF and NCC are obtained as 0.96 and 1, respectively, for the payload of 19,660 bytes. Finally,
746 the best SSIM is obtained as 0.999 for the payload of 294,912 bytes.

747

Acknowledgment

749 The authors thank Dr. Gerald Schaefer and Dr. Michal Stich for publishing a very interested
750 UCID v2 dataset well-suited general benchmark database for evaluating and testing image hiding
751 techniques (Schaefer, G., Stich, M. 2004). Moreover, the authors would like to thank Mr. Imtiaz
752 M. S for permission to use the standard test images database for image processing.

753

References

755 Subramanian, N., Elharrouss, O., Al-ma'adeed, S., Bouridane, A., 2021. Image Steganography:
756   A Review of the Recent Advances. IEEE Access PP(99):1-1 January.
757   DOI:10.1109/ACCESS.2021.3053998.

758   Rehman, A., Saba, T., Mahmood, T., Mehmood, Z., Shah, M., Anjum, A. 2018. Data hiding
759   technique in steganography for information security using number theory. Journal of
760   Information Science, 45(6): pp.767-778.
761   Liao, X., Yin, J., Guo, S., Li, X., Sangaiah, A., 2018. Medical JPEG image steganography based
762   on preserving inter-block dependencies. Computers & Electrical Engineering, 67, pp. 320-
763   329.
764   Ghosal, S., Hossain, S., Sarkar, R., 2021. Exploiting Laguerre transform in image
765   steganography. Computers & Electrical Engineering, 89, pp. 1-14.
766   Wang, J., Yang, C., Wang, P., Song, X., Lu, J. 2020. Payload location for JPEG
767   image steganography based on co-frequency sub-image filtering. International Journal of
768   Distributed Sensor Networks, 16(1), pp. 1-16.
769   Kim, P., Ryu, K., Jung, K. 2020. Reversible data hiding scheme based on pixel-value
770   differencing in dual images. International Journal of Distributed Sensor Networks, 16(7),
771   pp. 1-13.
772   Kang, Y., Liu, F., Yang, C. Xiang, L., Luo, X., Wang, P. 2019. Color image steganalysis based
773   on channel gradient correlation. International Journal of Distributed Sensor Networks,
774   15(5), pp. 1-13.
775   Yang, C., Kang, Y., Liu, F., Song, X., Wang, J., Luo, X. 2020. Color image steganalysis based
776   on embedding change probabilities in differential channels. International Journal of
777   Distributed Sensor Networks, 16(5), pp.1-10.
778   Jin, Z., Yang, Y., Chen, Y., Chen, Y. 2020. IAS-CNN: Image adaptive steganalysis via
779   convolutional neural network combined with selection channel. International Journal of
780   Distributed Sensor Networks, 16(3), pp.1-9.
781   Arun, C. Murugan, S. 2018. Design of image steganography using LSB XOR substitution
782   method. International Conference on Communication and Signal Processing (ICCSP).
783   Chennai, pp. 0674-0677.
784   Elshare, S., El-Emam, N. 2018. Modified Multi-Level Steganography to Enhance Data Security.
785   International Journal of Communication Networks and Information Security (IJCNIS),
786   10(3), pp. 509-525.
787   Hacimurtazaoglu, M., Tutuncu K. 2022. LSB-based pre-embedding video steganography with
788   rotating & shifting poly-pattern block matrix. PeerJ Computer Science 8:e843.
789   https://doi.org/10.7717/peerj-cs.843
790   Xue, P., Liu, H., Hu, J., Hu, R., A 2018. Multi-Layer Steganographic method Based on Audio
791   Time Domain Segmented and Network Steganography. 6th International Conference on
792   Computer-Aided Design, Manufacturing, Modeling and Simulation (CDMMS 2018), pp.
793   020046-1 - 020046-17.
794   Zhang, C., Benz, P., Karjauv, A., Sun, G., Kweon, I., 2020. Universal Deep data hiding for
795   Steganography, Watermarking, and Light Field Messaging. 34th Conference on Neural
796   Information Processing Systems (NeurIPS2020), pp.1-12.
797   Ahmad, M., El-Emam, N., AL-Azawi, A. 2021. Improved Deep data hiding/Extraction
798   algorithm to Enhance the Payload Capacity and Security Level of Hidden Information.
799   International Journal of Communication Networks and Information Security (IJCNIS), 13(3),
800   pp. 459-473.
801   Dhall, S., Sharma, R., Gupta, S., 2020. A multi-level steganography mechanism using quantum
802   chaos encryption. Multimedia Tools and Applications, 79, pp.1987–2012.

803   Sayed, M.,   Wahba, T., 2017. Multi-Level Image Steganography Using Compression
804   Techniques. International Journal of Computer Applications Technology and Research,
805   6(11), pp. 441-450.

806   Bhowal, K. (2019). Multi-level Steganography to Improve Secret Communication. In (Ed.), Digital Image
807   and Video Watermarking and Steganography. IntechOpen. https://doi.org/10.5772/intechopen.8159

808

809   Bommala, H., Kiran, S., Venkateswarlu, T., Sheela, M., 2020. Fibonacci Technique for Privacy
810   and Security to Sensitive Data on Cloud Environment. Int. J. Advanced Networking and
811   Applications, 11 (04), pp. 4374-4377.

812   Tian, R.; Sun, G.; Liu, X.; Zheng, B. 2021. Sobel Edge Detection Based on Weighted Nuclear
813   Norm Minimization Image Denoising. Electronics, 10(6), 655.
814   https:// doi.org/10.3390/electronics10060655

815   Ou, B. Li, X., Zhao, Y., Ni, R. 2015. Efficient Color Image Reversible Data Hiding Based on
816   Channel-Dependent Payload Partition and Adaptive Embedding. Signal Processing; 108, pp.
817   642-657.

818   Li, J., Li, X., Yang, B., 2013. Reversible data hiding scheme for color image based on
819   prediction-error expansion and cross-channel correlation. Signal Processing, 93, pp. 2748–
820   2758.

821   Imtiaz M. S. (2019). The MIT License in the link:
822   https://github.com/mohammadimtiazz/standard-test-images-for-Image-Processing.git

823   El-Emam, N., Al-Zubidy R. 2013. New Steganography Algorithm to Conceal a Large Amount of
824   Secret Message Using Hybrid Adaptive Neural Networks with Modified Adaptive Genetic
825   Algorithm. Journal of Systems and Software, 86(6), pp. 1465-1481.

826   Han, Y., Cai, Y., Cao, Y., Xu, X. 2013. A new image fusion performance metric based on visual
827   information fidelity. Information Fusion, 14(2), pp. 127–135.

828   El-Emam, N. 2015. New Data-Hiding Algorithm Based on Adaptive Neural Networks with
829   Modified Particle Swarm Optimization. Computers & security, 55, pp. 21-45.

830   Schaefer, G., Stich, M. 2004. UCID—an uncompressed color image database, in Proceedings of
831   813 the SPIE Storage and Retrieval Methods and Applications for Multimedia; San Jose, 814
832   CA, USA, pp. 472–480.

833

834

835

Figure 1

Multi-channels deep hiding

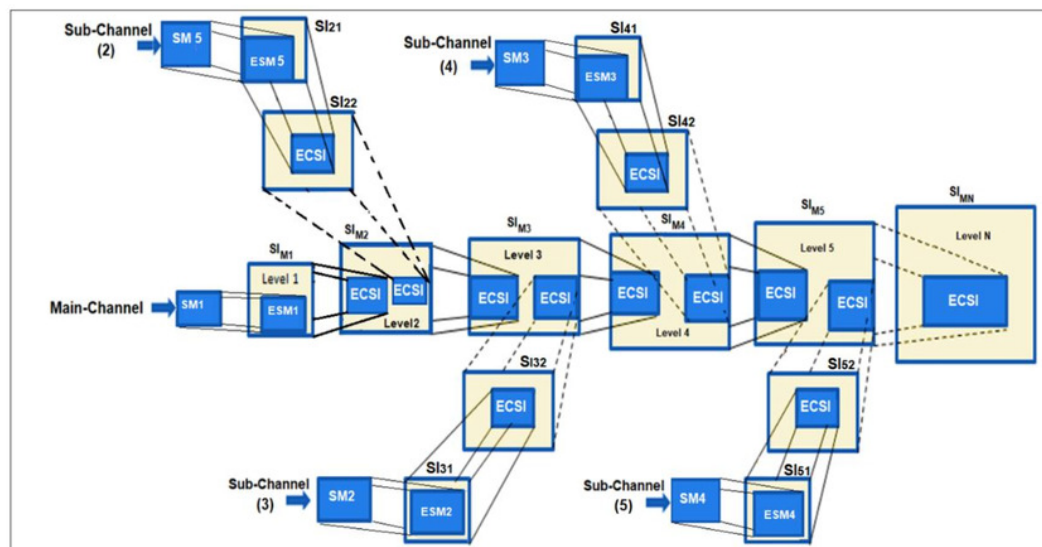



Figure 2

Distributed a secret message randomly among channels

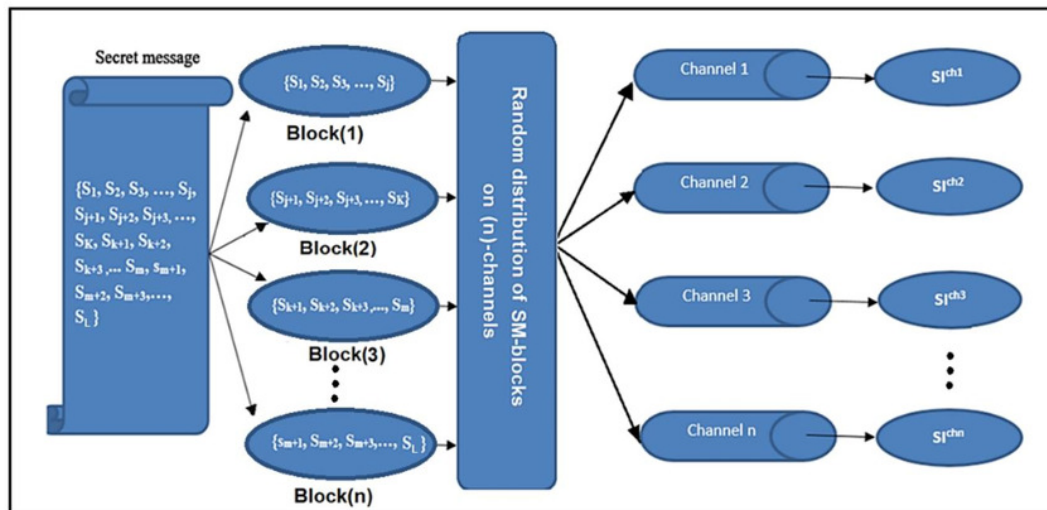



Figure 3

Deep Hiding at the ith sub-channel

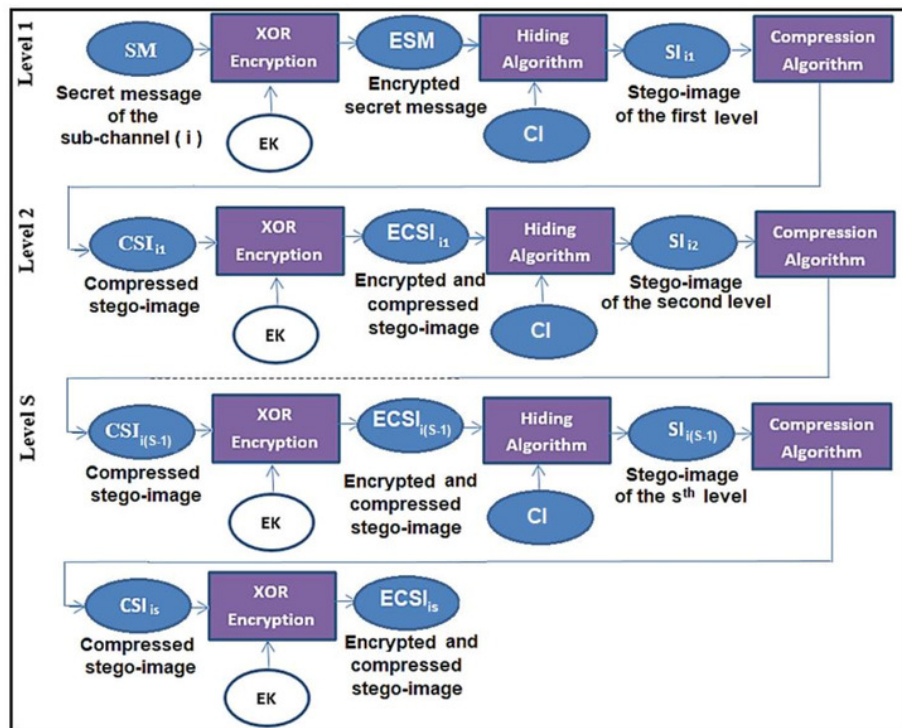



Figure 4

Data Hiding of two parts into cover-image at the main-channel using join process

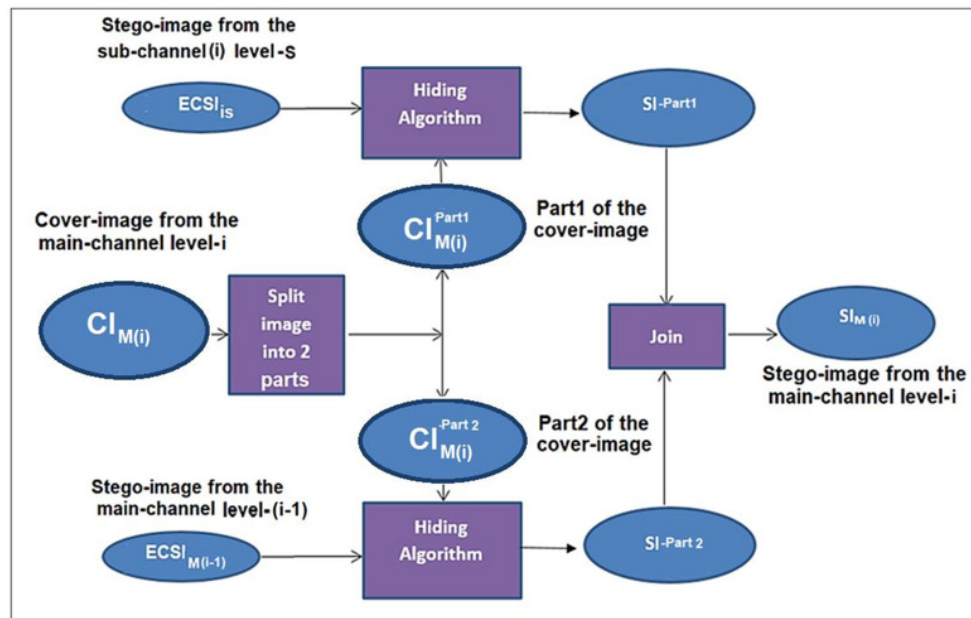



Figure 5

Data hiding in the last level of the main-channel using RGB cover-image

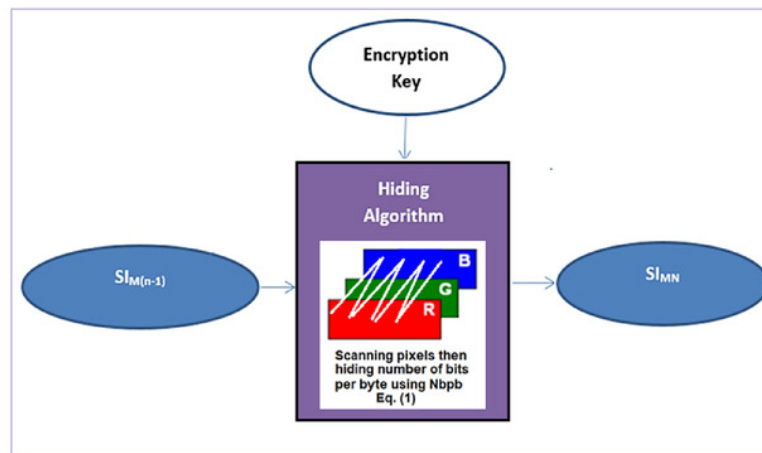



Figure 6

Data Extraction from the main and sub-channels

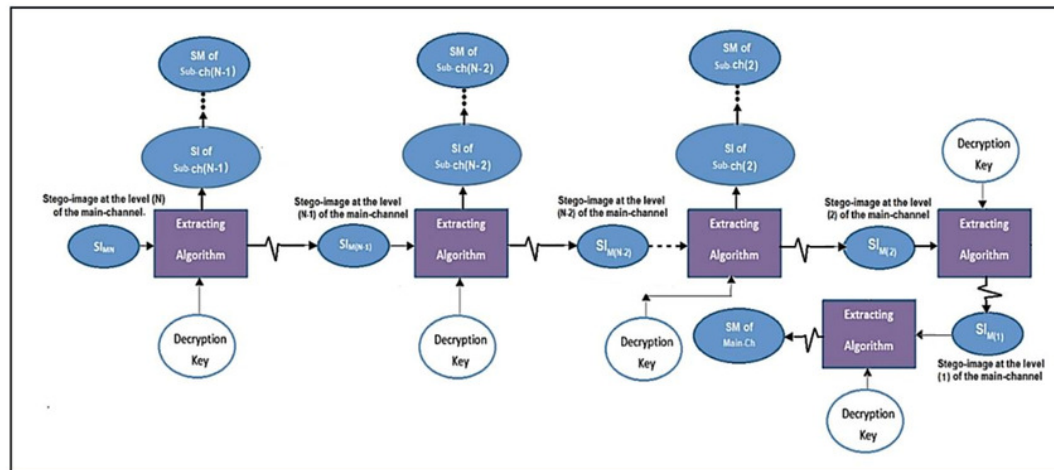



Figure 7

Data Extraction from two channels

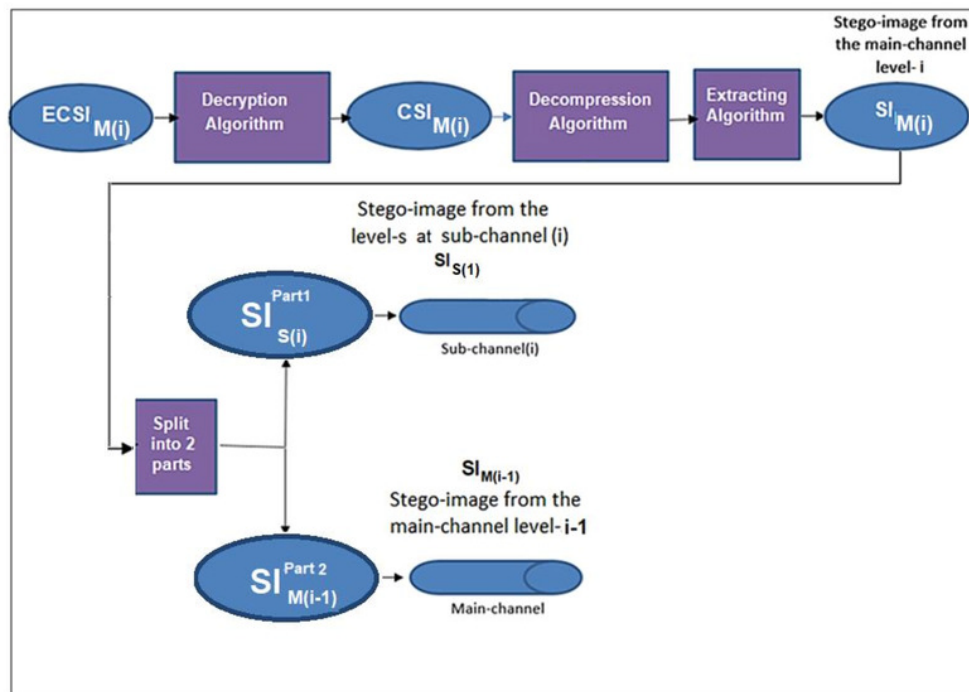



Figure 8

Data Extracting in many levels of one sub-channel

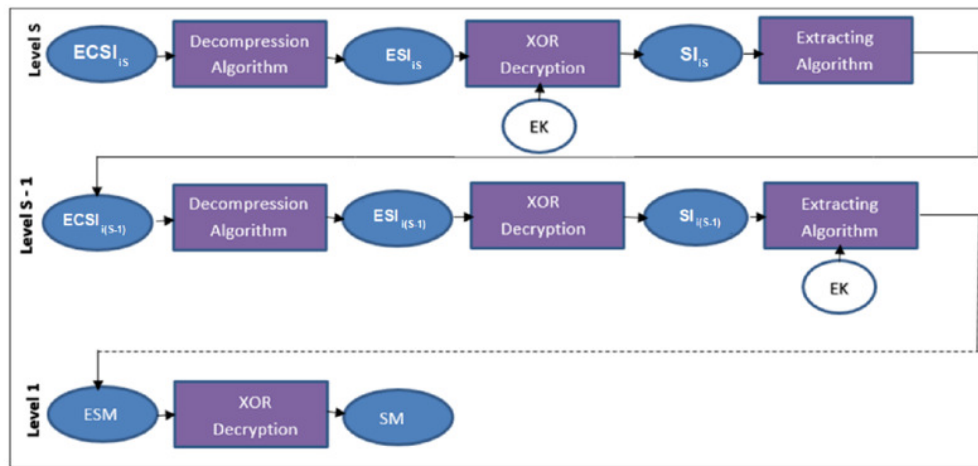



Figure 9

Data Extracting from main and sub-channels to find SM

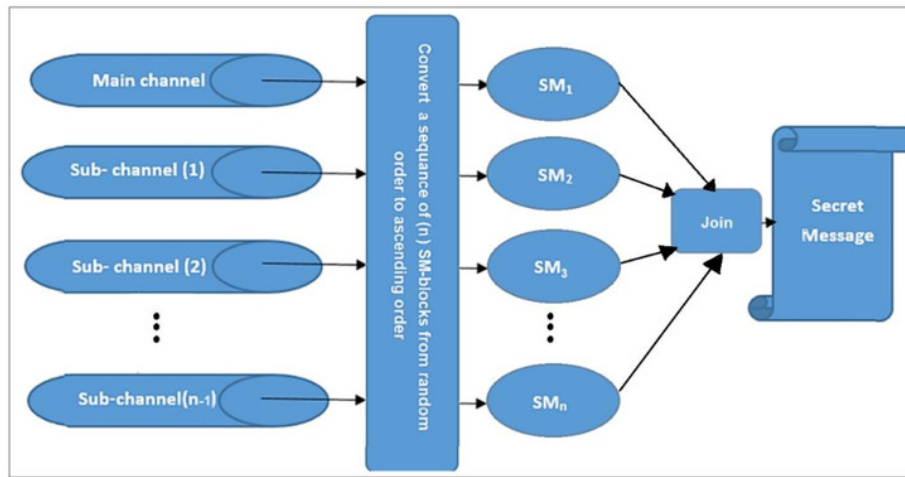



Figure 10

Implementation of the hiding process in the main channel

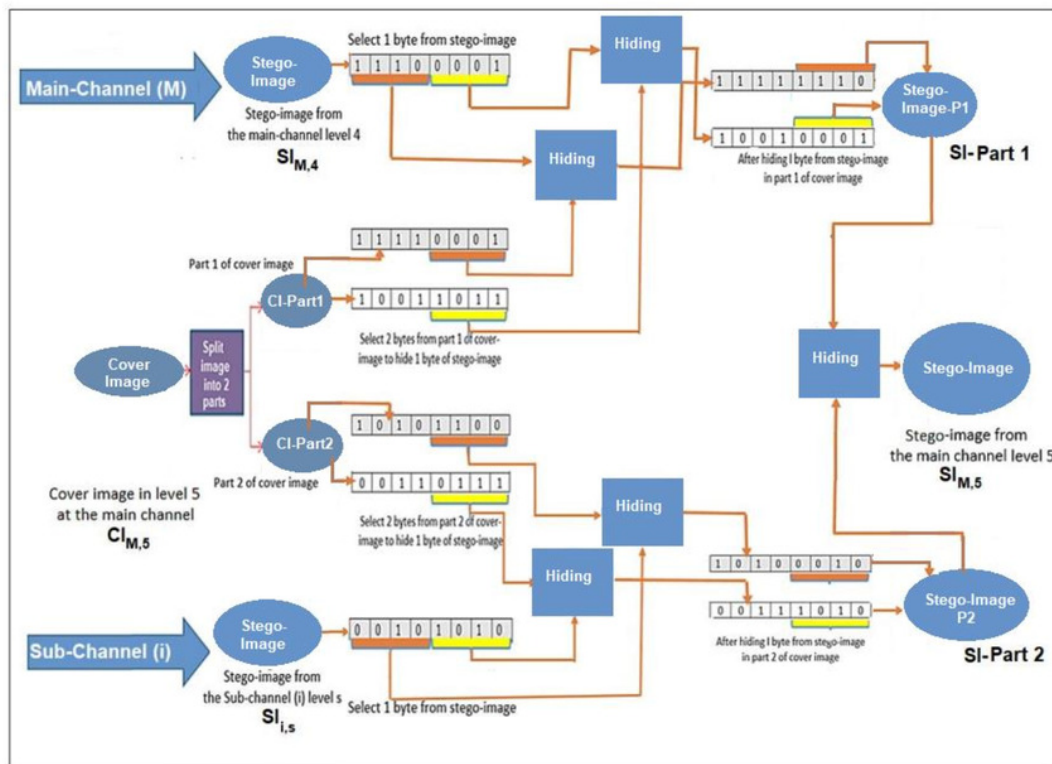



Figure 11

The PSNR values of the first 50 images in the database UCID with payload capacity 250x10^3

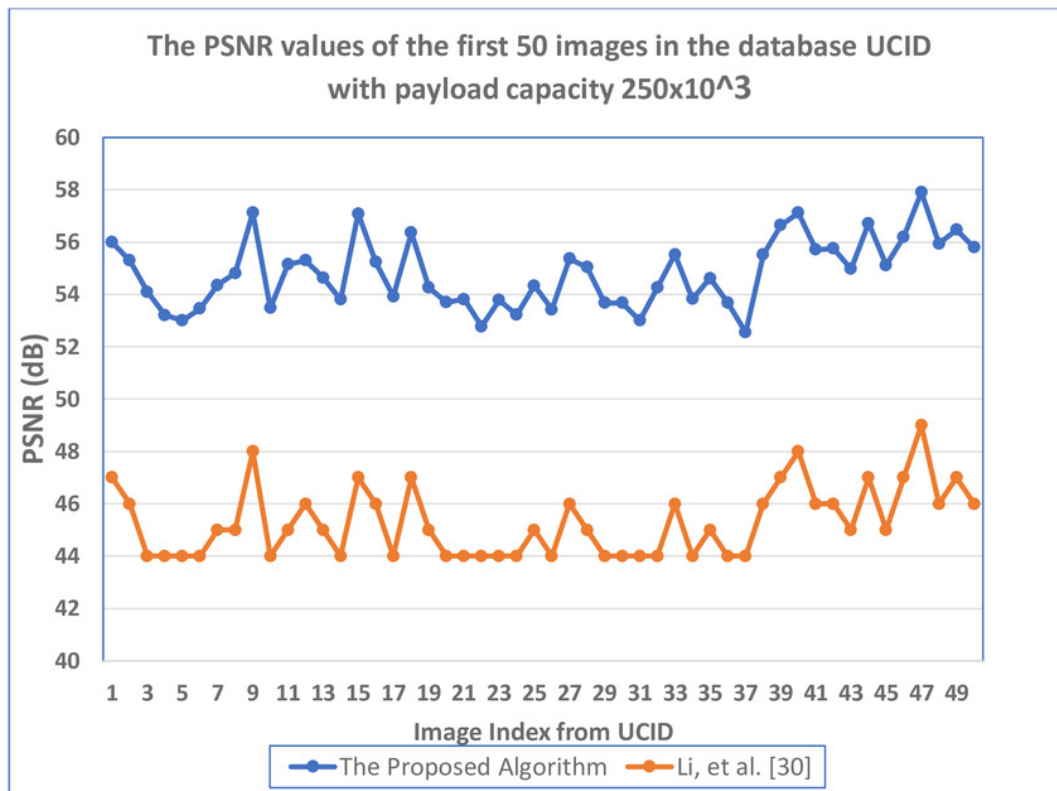



Figure 12

The SSIM values of the first 50 images in the database UCID with payload capacity 250x10^3

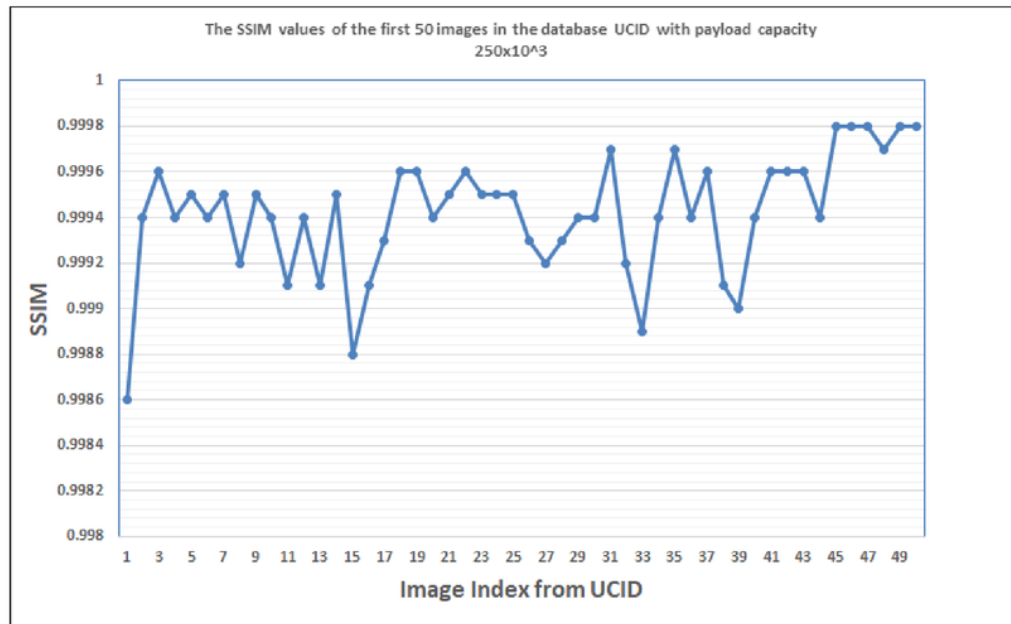



Figure 13

Euclidean norm testing of Lena image

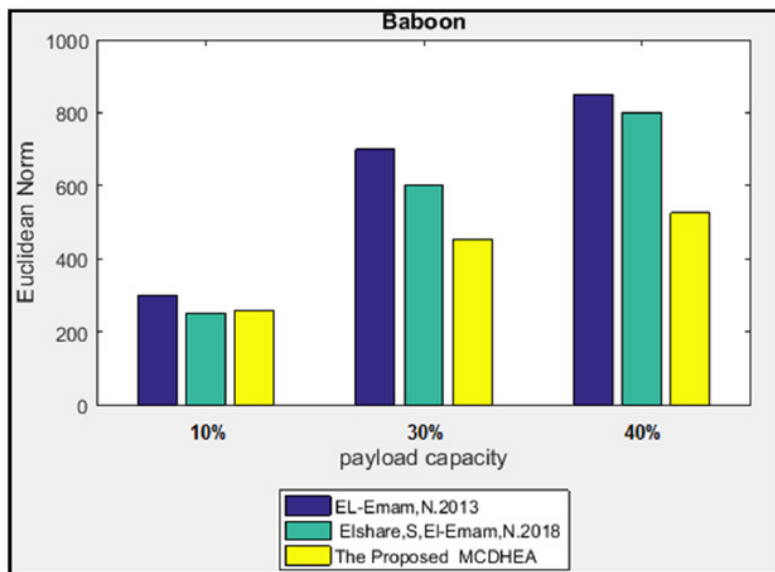



Figure 14

Euclidean norm testing of Baboon image

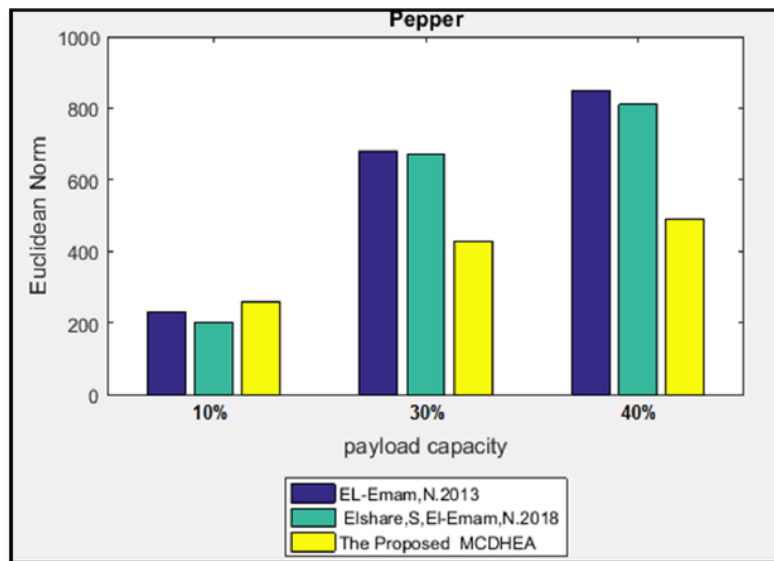



Figure 15

Euclidean norm testing of Peppers image

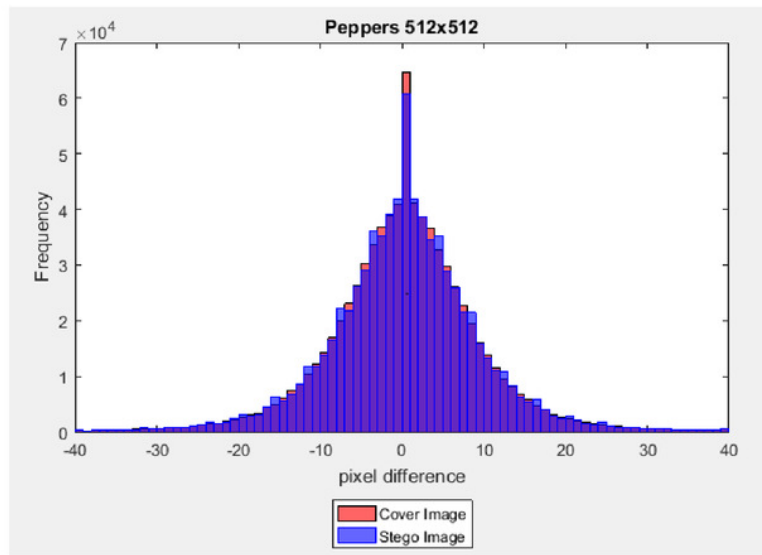



Figure 16

Dissimilarity between adjacent pixels with payload 40%

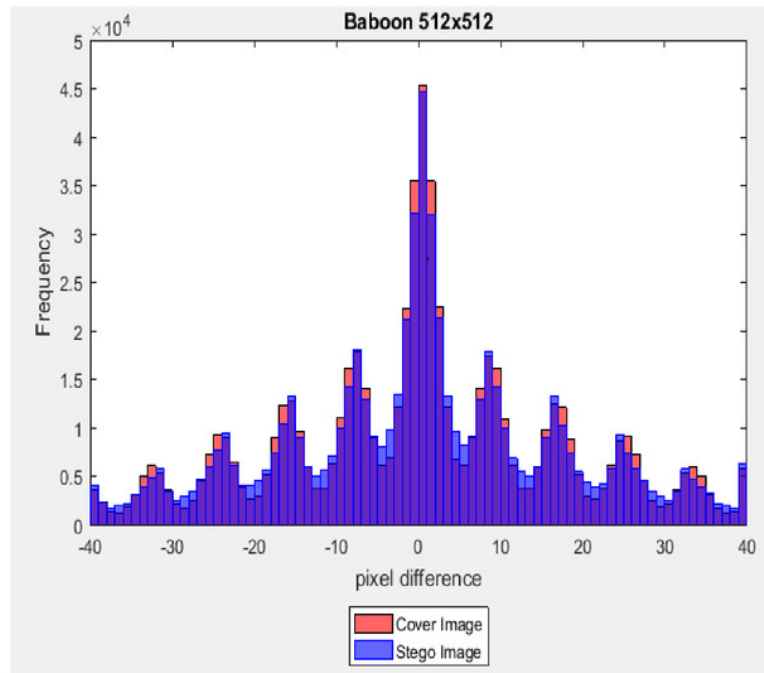



Figure 17

Dissimilarity between adjacent pixels with payload 40%

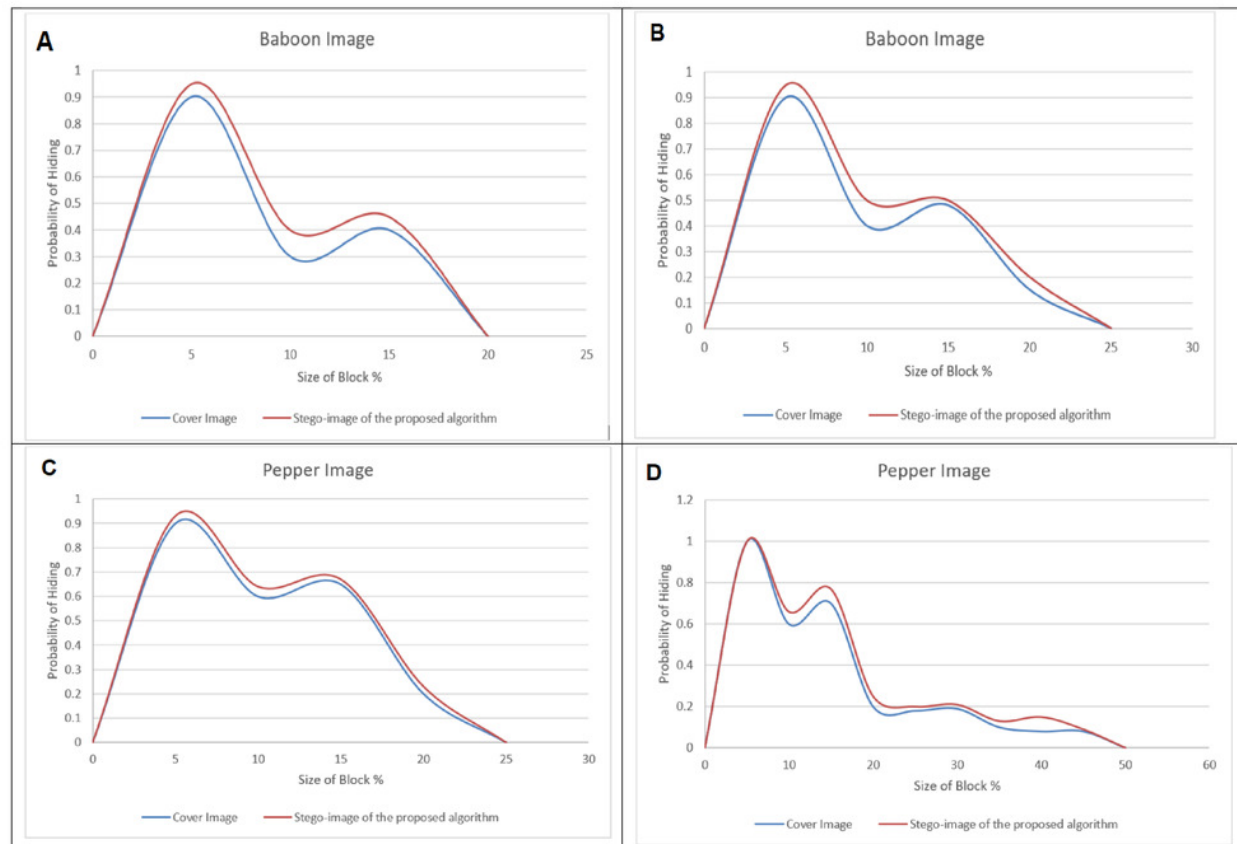



Figure 18

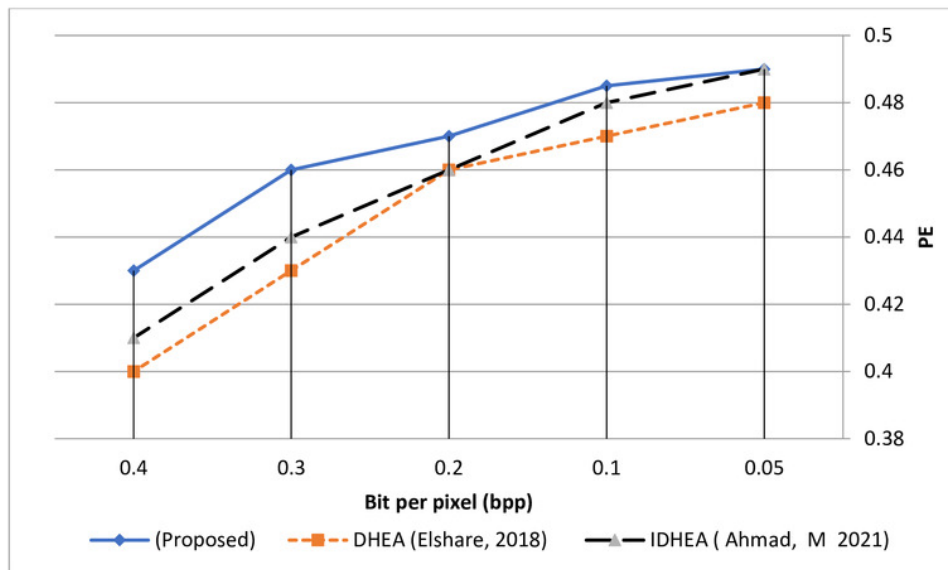
Dissimilarity between adjacent pixels with payload 40%

Performance of the proposed method

Table 1. Performance of the proposed algorithm MCDHEA

Image size 512 x 512	Payload capacity (bits)x10^5	PSNR (dB) using MDLSB Elshare, S. (2018)	**PSNR (dB) Ahmad, M. (2021)**	PSNR (dB) using Ou, B., et al. (2015)	PSNR (dB) using Li, J.(2013)	Proposed MCDHEA using NMLSB			
						MSE (dB)	PSNR (dB)	NCC (dB)	Diff
Barbara (Gray)	2	63.2	N/A	62	59.8	0.0232	65.2	1	0
	5	59.6	N/A	57	55.8	0.0341	64.6	1	0
	7	58.5	N/A	55.1	54.1	0.0361	63.8	0.999986	0
	10	55.9	N/A	53	52.5	0.0404	62.6	0.999966	0
	12.5	54.8	N/A	51.1	51.1	0.0514	61.8	0.999934	0
Baboon (Color)	2	59.2	63.3	56.8	57.1	0.0181	65.6	1	0
	2.8	56.1	57.8	54.9	55.2	0.02504	64.2	1	0
	3.6	54.9	56.1	53.3	53.3	0.03244	63.0	1	0
	4.4	53.2	55.4	51.9	51.9	0.04012	62.1	0.999967	0
	5.6	53.4	53.6	49.8	49.9	0.05118	61.0	0.999933	0
Peppers (Color)	2	61.2	64.9	59.1	57.9	0.01222	67.3	1	0
	4	59.1	59.2	55.5	53.7	0.02122	64.9	0.999967	0
	6	55.3	57.5	53.1	51.8	0.02960	63.4	0.999967	0
	8	53.7	56.7	51.3	50.2	0.03901	62.2	0.999933	0
	10.5	53.7	54.9	49.2	N/A	0.05006	61.2	0.999933	0

The Average values of SSIM by different steganography algorithms

Table 2. The Average values of SSIM . by different steganography algorithms

Payload Capacity	SSIM using MDLSB Elshare, S.[11]	SSIM using Li, J.[30]	SSIM using the proposed algorithm
20%	0.9997	0.9999	0.9999
30%	0.9998	0.9998	0.9997
40%	0.9997	0.9995	0.9996

The average values of VIF for three stego-images

Table 3 - The average values of VIF for three stego-images

Color Stego- image 256x256	Payload Capacity %	ANN_MPSO (ElEmam, 2015)	The proposed approach
Barbara	10%	0.91	0.96
Pappers	20%	NA	0.92
Baboon	30%	0.86	0.90