ISSN: 0067-2904

Concealing a Secret Message in a Colour Image Using an Electronic Workbench

Maisa'a Abid Ali Khodher[1], Ashwaq Alabaichi[2]
[1]*Department of Computer Science/University of Technology-Iraq/Baghdad*
[2]*Biomedical Engineering Department/College of Engineering/Karbala University*

Received: 30/7/2020 Accepted: 2/2/2021

Abstract

Steganography is the art of concealing security data in media, such as pictures, audio, video, text, and protocols. The objective of this paper is hiding a secret message in a colour image to prevent an attacker from accessing the message. This is important because more people use the Internet all the time and network connections are spread around the world. The hidden secret message uses two general algorithms that are embedded and extracted. This paper proposes a new algorithm to conceal a secret message in a colour image in LSB. This algorithm includes three phases: 1) dividing the colour image into a number of blocks, 2) concealing the secret message, and 3) transmitting the stego-image from the sender in a multiplexer network and receiving it through a demultiplexer network using an electronic workbench. The outcome of the new algorithm demonstrates good efficiency, high security, and robustness and is executed quickly. The system is evaluated through the measurements of mean square error, peak signal-to-noise ratio, correlation, histogram, and capacity.

Keywords: Steganography image, secret message, electronic workbench, key secret, synchronous time-division multiplexing.

اخفاء رسالة سرية داخل صورة ملونه باستخدام منضدة عمل الالكترونية

ميساء عبدعلي خضر[1] ،اشواق العبايجي[2]
[1]قسم علوم الحاسوب ، الجامعة التكنولوجية، بغداد، العراق
[2]قسم هندسة الطب الحياتي، كلية الهندسة، جامعة كربلاء، كربلاء، العراق

الخلاصه

إخفاء المعلومات هو فن إخفاء بيانات امنة في الوسائط ، مثل الصور والصوت والفيديو والنص والبروتوكولات. الهدف من هذه الورقة هو إخفاء رسالة سرية في صورة ملونة لمنع المهاجم من الوصول إلى الرسالة. هذا مهم لأن كثيرمن الأشخاص يستخدمون الإنترنت طوال الوقت ، وتنتشر شبكات الاتصال في جميع أنحاء العالم. وتستخدم الرسالة السرية المخفية خوارزميتين عامتينالتضمين والاستخراج. تقترح هذه الورقة خوارزمية جديدة لإخفاء رسالة سرية في صورة ملونة في .LSB تتضمن هذه الخوارزمية ثلاث مراحل: 1) تقسيم الصورة الملونة إلى عدد من الكتل ، 2) إخفاء الرسالة السرية ، و 3) نقل الصورة المخفية من المرسل الى شبكة multiplexer ثم منmultiplexer الى المستلم من خلال شبكة demultiplexer باستخدام منضدة عمل إلكترونية. تظهر نتيجة الخوارزمية الجديدة كفاءة جيدة وأمانًا عاليًا وقوة ويتم تنفيذها بسرعة. يتم تقييم النظام من خلال القياسات التالية: MSE و PSNR و correlation و hiostogram وcapacity.

1.Introduction

*Email: 110044@uotechnology.edu.iq

Digital image handling deals with the processing of other images through a digital computer. Image treatment is the application of a signal treatment method, such as two-dimensional (2D) signals, in photographs or videos. Image treatment typically includes filtering or enhancing a picture using different kinds of functions in addition to other methods to extract data from the image [1].

Image treatment via digital means comprises many branches involving picture recognition, segmentation, compression, and so on. It is essential in many applications, such as pattern recognition and goal identification. Picture treatment normally means digital image treatment [2].

Steganography is a method of hiding data in a carrier file so that it is imperceptible to prohibited parties [3]. Data concealment methods have recently become substantial in sundry application fields. Most issues of the information-hiding method stem from the unsecure carriage medium. The information-hiding method is an innovative kind of mystery communication technology. It comprises embedding data into digital media (image, video, audio, text, and protocol), with a minimum appreciable declination in the steward signal, for the objectives of identification, controlling access to digital media, and copyright [4].

A computer network is a framework where two or more computers and/or suitable calculation devices are interconnected to a portion of interchange data. The computers and other suitable devices are joined by telecommunication devices that can also recall and transfer media, causing the information or data to be transmitted within the network through these devices [5].

Facciolo *et al*. (2014) suggested integrating image impersonation, which is a wonderful idea that allows one to evaluate the sum of picture values in rectangular areas of the image for four processes, regardless of the volume of the areas. It was first suggested under the name of the "summed region table" in the Computer Graphics Society to efficiently change textile maps. It was popularised in the computer community with its use in their real-time topic discovery framework. In this work, it was suggested to depict the integrated image algorithm and study its implementation in the context of block matching. It was used to test trade-offs and the limit of the implementation success with respect to exhaustive block matching [6].

Khodher (2015) suggested an image as a covering to conceal the message using a secret random key. The secret key is a 9×9 array, and random items are selected for the reverse matrix. The reverse matrix is multiplied by a one-dimensional matrix, and the outcome is in a hidden image. This algorithm keeps the image secure through a transformation via a network. Such an operation is defined as a random picture transformation and is regarded as a credible means of hiding. The outcomes obtained from the proposed algorithm rely on the covering image. A secret key is created so that it can be retrieved from the original image after receiving it, without losing any concealed data by the recipient in the network [7].

Pandey *et al*. (2015) suggested image compression in DCT. The quantisation encoding manner of covert coding is widely used in picture treatment methods, but in these, the 2D pictures are split into sub-blocks, and every block is converted separately into prime frequency compositions. The frequency compositions (DC and AC) are decreased to zero over the operation of quantisation, which is a lossy operation. The result of the proposed manner applies to all the images, and its performance is analysed in terms of lowering the picture volume. The difference in picture quality between the original picture and the reconstructed picture is measured using the PSNR value with different quantisation matrices [8].

Barapatre *et al*. (2017) suggested a survey of three rising velocity technologies, which are X.25, frame relay, and ATM and compared them. Frame relay and ATM are variations of the requisite X.25 technologies. Based on the different execution metrics, the comparison survey explained that ATM has a lower retard contrast as compared to the X.25 and frame relay, and

therefore is effective for carrying real-time data. The result of ATM uses constant volume packets (53 bytes) for telecommunication. The frame relay uses changing packet volumes that rely on the kinds of data to be transmitted. The frame relay is used to join local area networks (LAN), and it is not executed in a single area network, whereas the data in ATM are within a single LAN. In addition, ATM is designed to be suitable for hardware execution and thus, the cost is higher compared to frame relay, which is software controlled [9].

Shirur (2018) suggested a wireless criterion frame status that is executed for time-critical signals (voice and video) and datum signals based on user priority in version 802.11. This proposed action is designed in such a way that forthcoming data are prioritised and integrated into Ethernet frames by tagging. Then, they are mapped to access categories. Based on user priorities, various queues are formative for every access category and difference for the channel differentiation. To support service quality, an enhanced distributed channel access is used, which was based on 802.11e [10].

Bandyopadhyay (2018) stated that the hiding of all information is a challenge in the field of safety and that security methods try to preserve privacy, safety, and availability. A steganography system includes two functions, namely embedding and extraction. The goal of the proposed action is to design robust algorithms that generate stego media and can load a large capacity of secure data without lowering the imperceptibility [11].

2. Electronic Workbench

The Electronic Workbench (EWB) is a designing instrument that supplies the user with all the components and tools to conduct board-level designing on a personal computer [12]. The EWB includes two kinds of data connections: 1) multiplexer (MUX) and 2) demultiplexer (DEMUX). A multiplexer is a circuit that accepts numerous inputs but gives only one output. A demultiplexer task is precisely the inverse of a multiplexer; that is, a demultiplexer accepts only one input and gives numerous outputs. In general, a multiplexer and demultiplexer are used jointly because the connection systems are bi-directional [13], as shown in Figure 1 a, b**.**

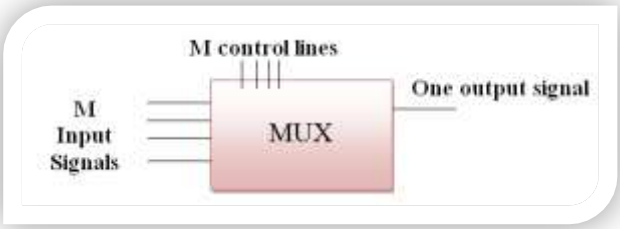


Figure 1a-Multiplexer pin diagram.

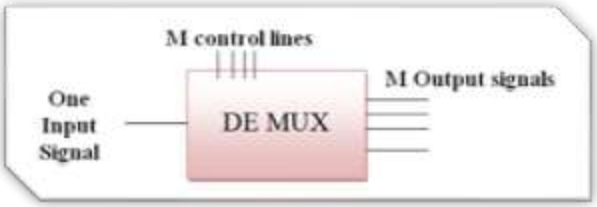


Figure 1b- Demultiplexer pin diagram**.**

3.Steganography

In information hiding, i.e. steganography, the data are concealed in the covering media. The covering medium can be in the form of images, script, video, or auditory files. Information hiding is defined as the science or technique of concealing the message into some covering medium. The word "steganography" comprises two words of old Greek origin: *steganos,* which means 'covering, concealed, or protected' and *graphical,* meaning 'lettering' [14].

Information hiding is a secure message embedded into the points of the load content, either by changing or replacing data [15]. It realises good imperceptibility and full capacity that can be realised comparatively faster than in the frequency domain, but with poor robustness. Alternatively, in frequency domain methods, the secret message is embedded inside the features of the load media after a certain transformation; however, this offers high robustness at the price of complexity and treatment time [16]. Information hiding uses two main algorithms, namely the embedded and extracted algorithms between the sender and receiver [17], as shown in Figure 2.

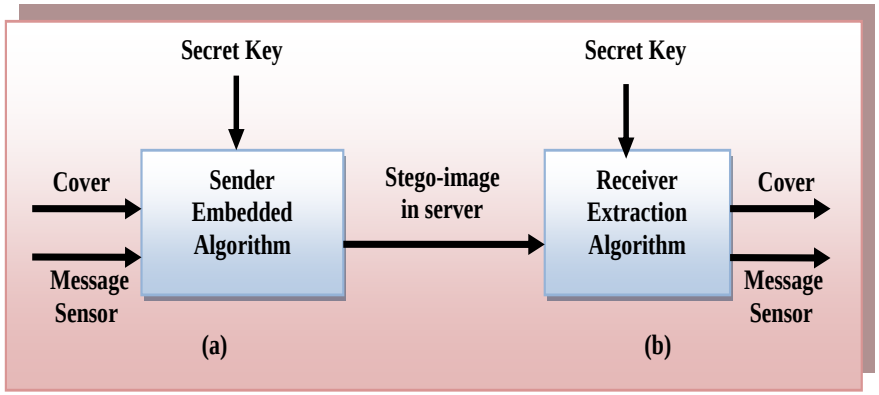


Figure2-Two major algorithms: (a) embedded algorithm and (b) extracted algorithm.

4.Evaluation System Performance

We applied the mean square error (MSE), peak signal-to-noise ratio (PSNR), correlation, and histogram [18] for the evaluation of the system performance.

4.1 Mean Square Error

MSE is calculated by comparing the bytes of two images. A pixel comprises 8 bits, and thus, 256 levels are available to represent various gray levels. MSEs are valuable when the bytes of an image are compared with the corresponding bytes of another image. Equation (1) is used to compute MSE [18, 19].

$$MSE = \frac{\sum_{M,N}[I1(M,N)-I2(M,N)]}{M \times N}. \quad (1)$$

where M and N represent row and column, respectively, in Figures 1 and 2 to obtain the value of MSE.

4.2 Peak Signal to Noise Ratio

PSNR is a parameter used to measure the amount of imperceptibility in decibels. It measures the quality between the two images. A large PSNR value indicates that a small difference exists between two images. By contrast, a small PSNR value indicates a huge distortion between two images. Equation (2) is used to compute PSNR [18, 19].

$$PSNR = \frac{1 - Log_{10} R^2}{MSE}. \quad (2)$$

where R is the maximum number of fluctuation in the input image data type.

4.3 Correlation Coefficient

The correlation coefficient *r* is the measurement of the range and trend of the linear group of two random variables. If two variables are closely related, the correlation coefficient is close to the value of 1. If the coefficient is close to 0, the two variables are not related. The coefficient *r* can be calculated using equation (3) [20] .

$$r = \frac{\sum_i (X_i - X_m)(Y_i - Y_m)}{\sum_i \sqrt{\sum_i (X_i - X_m)^2} \sqrt{\sum_i (Y_i - Y_m)^2}}. \quad (3)$$

where X_i is the pixel intensity of the original image, X_m is the mean value of the original image intensity, Y_i is the pixel intensity of the stego-image, and Y_m is the mean value of the stego-image intensity [21, 22].

4.4 Histogram

An image histogram is a diagram displaying how many pixels there are at every scale or at every index for the indexed colour image. The histogram includes data that are necessary for image equalisation, where the image pixels are stretched to give a sensible dissimilarity [22, 23]. With the histogram, the equalisation method can evolve. Equalization stretches the scale range of the pixel level to the full range to improve the contrast of the given image. To use this technique, the equalised new pixel value is redefined using equation (4) [23].

$$p(m,n) = \frac{numberofpixelswithscalelevel \leq (m,n)}{Totalnumberofpixels} x(maximumscalelevel) \quad (4)$$

where m and n represent row and column, respectively in image p. which are applied in equation (4) to obtain the histogram.

5. The Proposed System

The proposed system uses colour images to conceal a secret message inside an image in three phases: 1) image blocks, 2) secret message, and 3) image transmission, as shown in the block diagram of the proposed system in Figure 3.

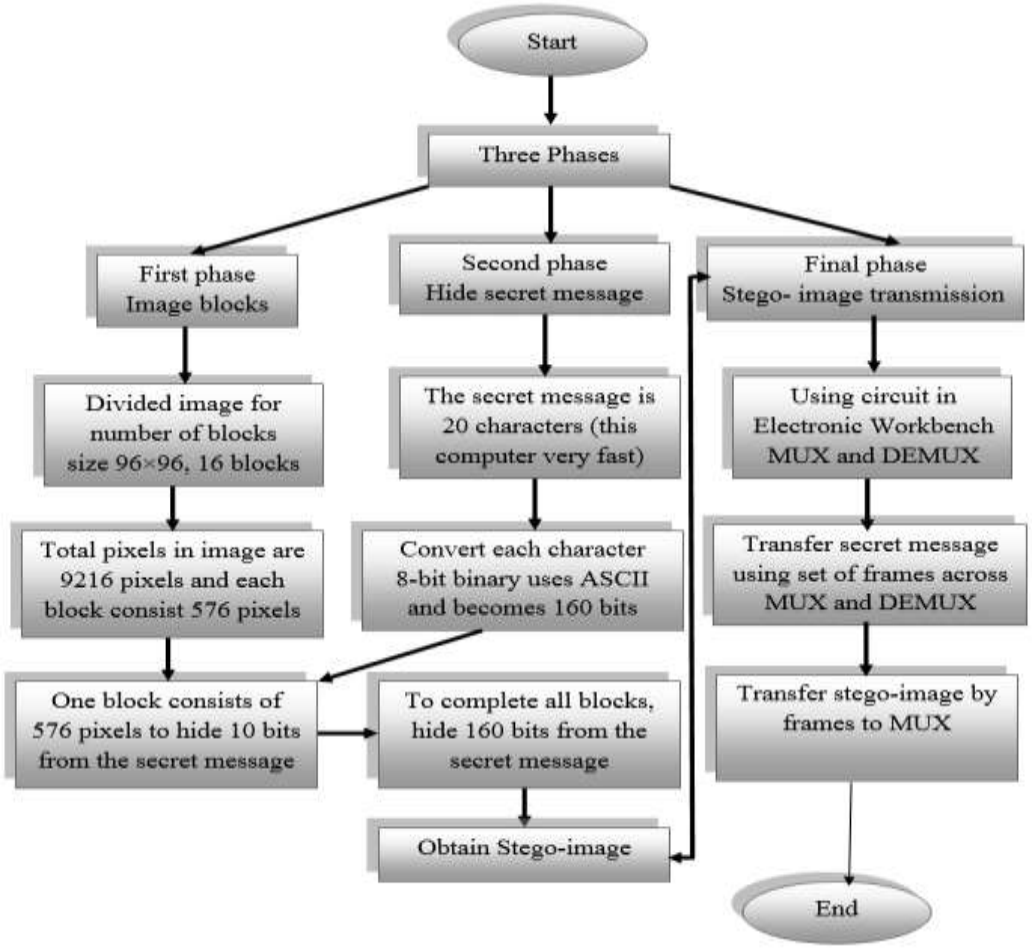


Figure 3-The proposed system in three phases to conceal secret message.

5.1 First Phase: Image Blocks

This phase divides a colour image of any format into a number of blocks, as shown in the original image in Figure 4. The size of the image is 96×96 for 16 blocks. Figure 5 starts from 0 to 23 for block 1, from 24 to 47 for block 2, from 48 to 71 for block 3, and from 72 to 96 for

block 4. Each block consists of 576 pixels and hides 10 bits of binary code, where every 50 pixels hide one bit from the secret message in the same block.

Figure 4-Original image cut.

	023	2447	48 71	72 96
0 23	BLOCK 1 576 pixels	BLOCK 2 576 pixels	BLOCK 3 576 pixels	BLOCK 4 576 pixels
24 47	BLOCK 5 576 pixels	BLOCK 6 576 pixels	BLOCK 7 576 pixels	BLOCK 8 576 pixels
48 71	BLOCK 9 576 pixels	BLOCK 10 576 pixels	BLOCK 11 576 pixels	BLOCK 12 576 pixels
72 96	BLOCK 14 576 pixels	BLOCK 14 576 pixels	BLOCK 15 576 pixels	BLOCK 16 576 pixels

Figure5- Block image cuts.

5.2 Second Phase: Hide the Secret Message

The secret message comprises 20 characters 'This computer is very fast', and each character is represented as ASCII in 8 bits. For the secret message, every 10 bits hide in one block. For 20 characters times 8 bits in ASCII, that is equal to 160 bits hiding in the image of 96×96 pixels in 16 blocks. This system can hide more than 20 characters. As shown in Figure 6a, there are 16 blocks in the image, and Figure 6b shows the readout for block 1 in the block image. The pixels hide one bit in LSB after converting this pixel to binary in 137, 89, 76, 108, 208, 219, 225, 209, 215, and 223, and it resets LSB in each pixel, adding one bit from the secret message. In each of the 50 locations, one bit hides from 0 to 49 and continues in 50 to 99 to *n* blocks, hiding 10 bits in each block. In all, the image hides 160 bits.

Figure 6a- Block image cut into 16 blocks.

242	206	210	209	198	201	199	197	212	209	207	202	196	193	192	194	207	208	205	202	198	197	194	197	201	206	209	173
214	165	156	152	136	135	132	132	138	138	141	141	139	139	138	140	142	142	137	135	134	134	133	138	147	153	156	126
191	125	104	100	85	82	81	87	79	81	86	88	88	87	86	86	92	90	86	85	85	86	89	92	100	108	112	90
188	111	83	85	79	77	75	87	94	95	97	95	94	89	86	85	79	79	78	77	79	80	80	80	90	100	103	89
202	118	89	92	87	83	78	88	81	80	79	76	73	71	70	69	75	75	78	78	81	79	76	75	84	93	94	89
213	130	98	97	89	82	72	76	81	81	80	79	80	82	82	84	74	75	79	82	83	82	79	76	64	76	75	80
202	125	94	90	83	81	72	73	74	75	78	79	80	80	80	80	83	82	83	87	90	91	92	91	69	79	74	83
180	108	80	79	77	83	78	79	86	90	92	93	92	90	87	83	85	83	84	87	92	97	99	99	101	107	95	97
210	116	83	94	80	83	95	75	90	82	80	87	88	80	78	80	76	79	86	90	91	94	95	97	98	99	85	87
216	198	208	208	208	194	209	214	208	206	208	211	210	203	198	196	199	203	211	216	219	222	221	221	218	219	220	219
203	214	219	211	237	227	227	234	227	230	230	220	211	207	201	196	194	199	209	217	221	222	221	220	203	219	225	219
218	216	201	206	219	225	210	211	224	227	218	198	183	181	180	173	176	183	193	202	206	206	204	202	213	216	217	216
228	229	223	249	212	225	219	231	236	242	238	222	211	212	210	203	201	207	218	225	228	228	224	221	216	200	207	230
240	231	220	240	200	217	221	236	212	219	223	224	223	223	220	214	209	212	220	226	228	226	223	219	217	214	219	232
253	242	219	206	220	225	222	219	209	207	207	211	212	209	206	203	208	210	215	220	219	218	214	211	209	223	211	206
206	226	221	179	242	219	200	183	220	203	189	188	186	181	181	184	176	174	178	181	180	177	174	170	172	179	170	190
227	203	208	227	226	192	223	215	171	173	200	168	218	218	230	217	216	202	207	224	230	218	208	206	204	204	211	225
xcx209	223	212	207	198	213	210	153	153	128	153	232	187	220	213	234	199	211	223	218	215	220	219	212	205	206	215	229
171	180	160	163	133	155	173	176	170	168	136	124	164	194	182	212	197	212	222	216	212	220	222	218	212	215	221	234
217	167	120	133	138	155	176	203	176	108	132	129	182	164	190	190	189	182	186	201	209	203	197	199	195	196	198	207

Figure 6b-Block 1 image before hiding the secret message.

Secret message “This computer very fast”
T in ASCII is 84= 01010100 , i in ASCII is105 = 01101001

							MSB				Pixel 137				LSB
...	141	139	139	138	140	142	142	1	0	0	0	0	1	0	0	1

Reset LSB pixel

1	0	0	0	0	1	0	0	0

Add one bit from secret message

1	0	0	0	0	1	0	0	0

The pixels become 136, 88, 77,108, 209, 218, 225, 208, 215, and 222. There is no effect on the colour image. The operation is repeated in ten locations from 137 to 223 in block 1 and is repeated in all blocks to hide all parts of the secret message in all image blocks before sending the image (Figure 7). Each block can hide a character and two bits from the next character. After embedding the secret message as shown in Figure 8, we have the stego-image.

242 206 210 209 198 201 199 197 212 209 207 202 196 193 192 194 207 208 205 202 198 197 194 197 201 206 209 173
214 165 156 152 136 135 132 132 138 138 141 141 139 139 138 140 142 142 136 135 134 134 133 138 147 153 156 126
191 125 104 100 85 82 81 87 79 81 86 88 88 87 86 86 92 90 86 85 85 86 89 92 100 108 112 90
188 111 83 85 79 77 75 87 94 95 97 95 94 88 86 85 79 79 78 77 79 80 80 80 90 100 103 89
202 118 89 92 87 83 78 88 81 80 79 76 73 71 70 69 75 75 78 78 81 79 76 75 84 93 94 89
213 130 98 97 89 82 72 77 81 81 80 79 80 82 82 84 74 75 79 82 83 82 79 76 64 76 75 80
202 125 94 90 83 81 72 73 74 75 78 79 80 80 80 80 83 82 83 87 90 91 92 91 69 79 74 83
180 108 80 79 77 83 78 79 86 90 92 93 92 90 87 83 85 83 84 87 92 97 99 99 101 107 95 97
210 116 83 94 80 83 95 75 90 82 80 87 88 80 78 80 76 79 86 90 91 94 95 97 98 99 85 87
216 198 208 209 208 194 209 214 208 206 208 211 210 203 198 196 199 203 211 216 219 222 221 221 218 219 220 219
203 214 219 211 237 227 227 234 227 230 230 220 211 207 201 196 194 199 209 217 221 222 221 220 203 218 225 219
218 216 201 206 219 225 210 211 224 227 218 198 183 181 180 173 176 183 193 202 206 206 204 202 213 216 217 216
228 229 223 249 212 225 219 231 236 242 238 222 211 212 210 203 201 207 218 225 228 228 224 221 216 200 207 230
240 231 220 240 200 217 221 236 212 219 223 224 223 223 220 214 209 212 220 226 228 226 223 219 217 214 219 232
253 242 219 206 220 225 222 219 209 207 207 211 212 208 206 203 208 210 215 220 219 218 214 211 209 223 211 206
206 226 221 179 242 219 200 183 220 203 189 188 186 181 181 184 176 174 178 181 180 177 174 170 172 179 170 190
227 203 208 227 226 192 223 215 171 173 200 168 218 218 230 217 216 202 207 224 230 218 208 206 204 204 211 225
209 222 212 207 198 213 210 153 153 128 153 232 187 220 213 234 199 211 223 218 215 220 219 212 205 206 215 229
171 180 160 163 133 155 173 176 170 168 136 124 164 194 182 212 197 212 222 216 212 220 222 218 212 215 221 234
217 167 120 133 138 155 176 203 176 108 132 129 182 164 190 190 189 182 186 201 209 203 197 199 195 196 198 207

Figure 7-Block 1 image after hiding the secret message.

Figure 8- Stego-image cut into 16 blocks.

5.3 Final Phase: Stego-image Transmission

The transmission of the stego-image from the multiplexer to demultiplexer uses a circuit in EWB. It can use time-division multiplexing (TDM) and a type of synchronous TDM. This type is used for framing bits for transferring data in the stego-image. The stego-image transfers from block 1 to block 16 (the size of each block is 576 pixels) after concealing the secret message. Each block in the stego-image uses 72 frames, each frame has a capacity of 64 bits or 8 bytes, each byte has slots, and each slot includes one pixel in a decimal number, where each pixel represents 8 bits or one byte. The transmission data for the stego-image of all blocks in a channel are converted for each pixel in a slot to 8 bits across the network multiplexer via one channel, and the secret message is extracted by the receiver to one channel by the demultiplexer. The demultiplexer includes a filter to retrieve all frames and rearrange them block by block for the stego-image. The receiver can extract the secret message using the algorithm as the secret key. As shown in Figure 9, rearrangement of the frames and slots in each block is performed. Figure 10 shows the transmission of stego-image in EWB (MUX and DEMUX). The message is sent block by block using two selectors in MUX and DEMUX, four probability logics 00, 01, 10, and 11 to control the transmission block by block, where, in 00, B1 is sent; in 01, B2 is sent; in 10, B3 is sent; and in 11, B4 is sent. This operation is repeated to complete four blocks (in 00, B5 is sent, in 01, B6 is sent; in 10, B7 is sent; and in 11, B8 is sent), thus completing 16 blocks. The switches 1, 2, 3, and 4 are always active in logic 1 to arrive block to pass off in channel.

Block 1 Fram 1	197	199	201	198	209	210	206	242
Block 1 Fram 2	194	192	193	196	202	207	209	212
Block 1 Fram 3	197	194	197	198	202	205	208	207
.								
.								
.								
.								
Block 1 Fram 72	209	203	197	199	195	196	198	207

Figure 9- Frame in each pixel in Block1**.**

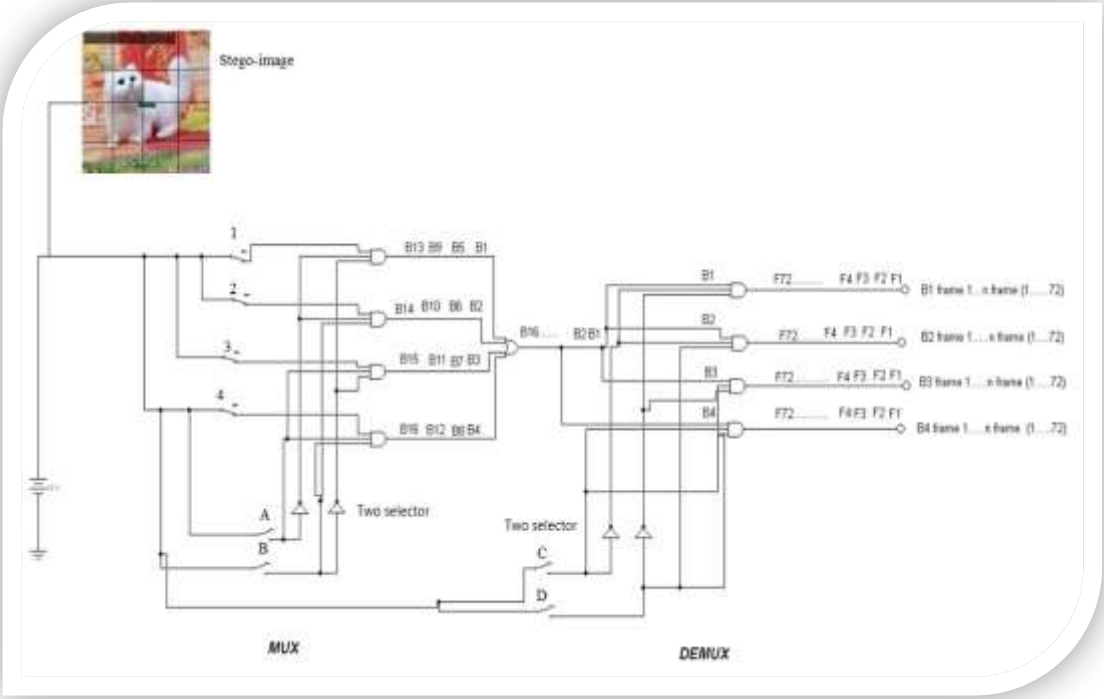


Figure 10- Transmission of stego-image in EWB (MUX and DEMUX).

5.4 Implementation Embedding and Extraction Algorithms

Embedding Process

Embedded Algorithm 1

Process:

Input: Original image 96×96, secret key (number of locations), secret message

Output: secret message (20 characters).

A= Original image.

B= Block image.

C= Secret key (50 pixels).

D=Hide the secret message in each block.

E= Divide each block into the number of frames (each frame has 8 slots).

F= Put the resulting stego-image transmission by MUX in one channel.

Step 1: Load the original image in A.

Step 2: Divide the original image into 16 blocks; each block has 576 pixels in B.

Step 3: Find the location in 16 blocks considering the secret key, select each of the 50 pixels

by 50 pixels in C.
Step 4: Hide 10bitsin binary in LSB in each location in each block using the secret key: 160 bits in D.
Step 5: Divide each block into 72 frames, where each frame has 8 slots in E.
Step 6: Put the result (stego-image) in F and transmit it using multiplexers in one channel.

Extraction Process

Extraction Algorithm 2

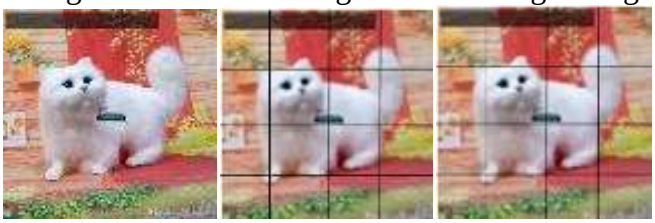
Process:

Input: Stego-image 96×96, secret key (number of locations), number of frames.
Output: Original image.
A= Receive number of frames from DEMUX.
B= Sum all frames and reorder into 16 blocks.
C= Stego-image.
D= Secret key (50 pixels).
E= Retrieve the secret message from each block in the image.
E= Sum the 160 bits in binary from the 16 blocks (20 characters)
F= Put the result (secret message).
Step 1: Load all frames from one channel to DEMUX in A.
Step 2: Sum all frames and rearrange to 16 blocks, each block with 576 pixels, and each block includes72 frames in B.
Step 3: Load stego-image in C.
Step 4: Find the secret key to select the location (every 50 pixels) in all blocks in D.
Step 5: Retrieve 10 bits in binary from LSB in all blocks using the secret key in E.
Step 6: Sum the 160 bits in binary from the 16 blocks in E.
Step 7: Put the results (secret message) in F.

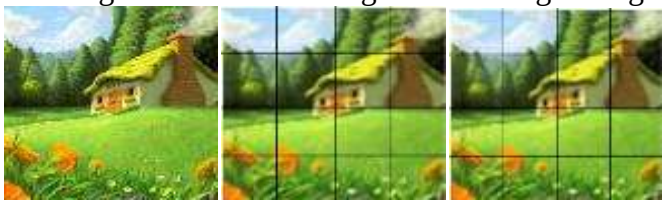
6. Testing the Result

This paper indicates that the outcome in the proposed system is good; it hides the secret message in blocks in an image. The steganography system provides high security and is efficient and robust because it cannot be viewed and changed by attackers. Through the test measurements using PSNR MSE, correlation, and histograms, the outcomes are very good. Figure 11 explains the testing results among the original image, image block, and stego-image.

Original Image Cut Block Image Cut Stego-Image Cut

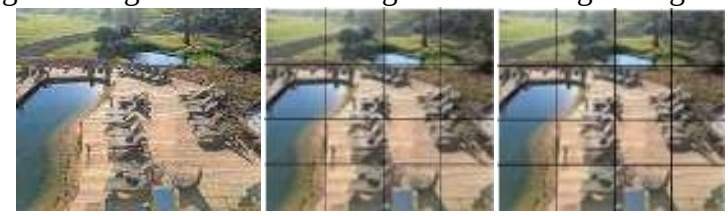


Original Image House Block Image House Stego-Image House



Original Image Nature Block Image Nature Stego-Image Nature

Original Image River Block Image River Stego-Image River



Original Image Tree Block Image Tree Stego-Image Tree

Figure 11-The original, block, and stego-image

6.1 System Analysis

The proposed system is analysed by evaluating the outcome using MSE, PSNR, correlation, and histogram to explain the robustness, efficiency, and security. The system is very powerful in analogous between original image, block image, and stego-image, when concealing the secret message. Table 1 indicates the measurements of MSE, PSNR, and correlation, using equations (1), (2), and (3), respectively, shown in the section on the performance evaluation. Table 2 indicates the histogram of the original image, which varies in the block image and stego-image, where the histogram between the block image and stego-image relies on equation (4) shown in the section on the performance evaluation. This indicates that the system is powerful for concealment.

When MSE, PSNR, and the correlation are run in five tests, the range of MSE is the reverse of the range of PSNR. The range of MSE in the block image and stego-image increases compared with the original image, and the range of the PSNR in the block image and stego-image decreases compared with the original image. When the correlation in the block image and stego-image is relatively equal, as shown in Table 1, this indicates that the proposed system is good for concealing a secret message and can transfer the stego-image using EWB.

Table 1-Measurements of the MSE, PSNR, and correlation

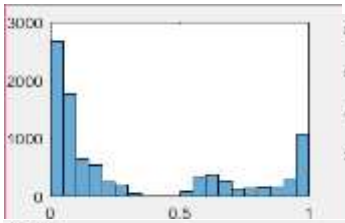
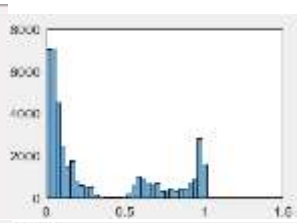
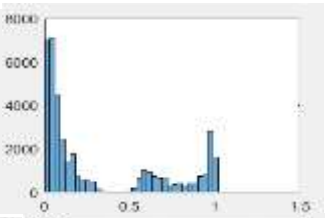
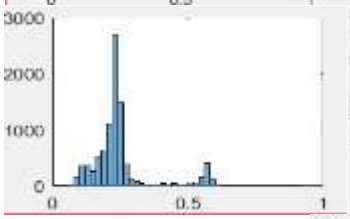
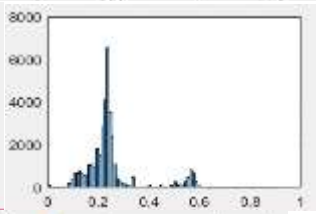
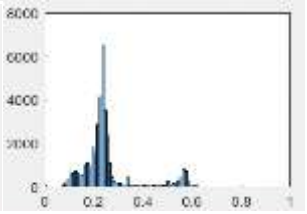
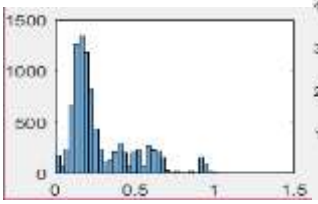
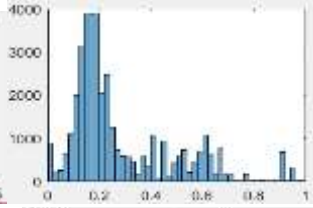
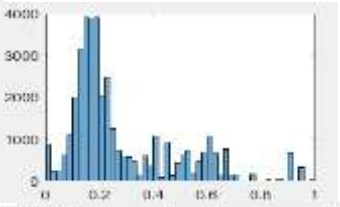
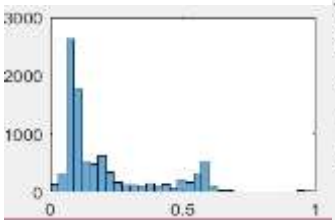
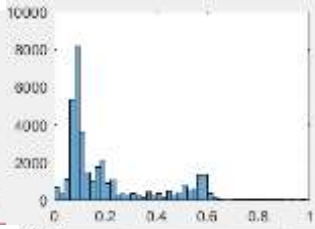
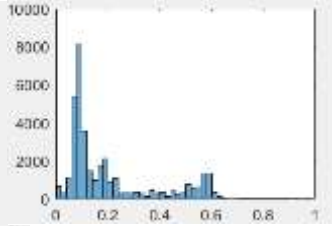
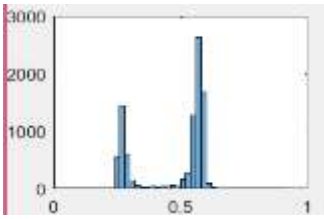
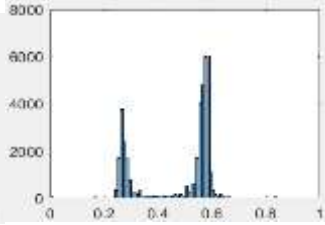
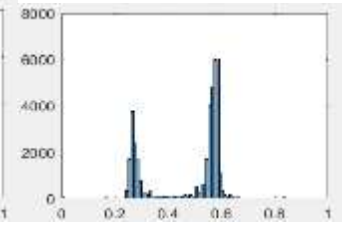
Name of image	Original image	Block image	Stego-image
Cut	MSE=5220.597	MSE=6400.5821	MSE= 6423.6711
	PSNR=2.9463	PSNE=2.6453	PSNR=2.5432
	Correlation=0.9754	Correlation=0.8755	Correlation=0.7959
House	MSE=14751.7461	MSE=14925.1162	MSE=15724.2235
	PSNR=1.5453	PSNE=1.5154	PSNR=1.5123
	Correlation=0.9914	Correlation=0.8280	Correlation=0.7871
Nature	MSE=29882.0757	MSE=30374.5564	MSE=31264.5466
	PSNR=0.9544	PSNE=0.8374	PSNR=0.8056
	Correlation=0.9945	Correlation=0.8178	Correlation=0.8077

River	MSE=14175.5631	MSE=14211.2060	MSE=14332.3060
	PSNR=1.5934	PSNE=1.5904	PSNR=1.5625
	Correlation=1.000	Correlation=0.9549	Correlation=0.9076
Tree	MSE=19859.5830	MSE=19938.3781	MSE=20940.3788
	PSNR=1.9241	PSNE=1.2054	PSNR=1.0063
	Correlation=1.000	Correlation=0.9932	Correlation=0.9250

6.2 Histogram

The histogram displays the accurate appearance of all pixels in the image. Table 2 indicates the histogram of the original image, block image, and stego-image. The histogram shows variation in the proposed system among the original image and stego-image, but also shows the similarity between the block image and stego-image. This indicates that the proposed system is good for hiding a secret message. The similarity between block and stego-images indicates that it prevents the detection of the secret message by attackers.

Table 2- The histogram of the proposed system.

Name of image	Original image	Block image	Stego-image
Cut			
House			
Natur			
River			
Tree			

6.3 High Capacity

The hiding capacity determines the maximum number of bits that can be hidden in the original image (96x96) after dividing 16 blocks for an acceptable quality of the resultant stego-image. The steganography system has better performance if it has a large hiding capacity, equal to 160 bits. In the proposed algorithm, one bit is embedded in each of the 50 pixels of each block. Therefore, the capacity of the hiding rate in the proposed algorithm is equal to the number of characters/size of the image (number of pixels). For 20 characters, it is 160 bit/9216 pixels, equal 0.017361, and for 80 characters, it is 640 / 9216 pixels, equal 0.0694 capacity for hiding data in a colour image.

7. Conclusions

This paper describes a proposed system to hide a secret message inside a block image using LSB. More than 20 characters can be sent in a secret message in this system. Each block image is transformed via EWB, using a circuit of multiplexers and demultiplexers (MUX and DEMUX) and TDM. This method is used to send a secret message across a network Internet. The outcomes of this system show that it is executed quickly, efficiently, robustly, and securely, through the use of TDM and a number of tests shown in table 1 and table 2. It can be used as a secret key by selecting the locations of all 50 pixels to hide one bit in each block image, where ten bits are used without revealing sensitive information to an unauthorised attacker when exchanging a message.

References

[1] S. Padmappriya, and K. Sumalatha, Digital Image Processing Real Time Applications, *International Journal of Engineering Science Invention* (IJESI), One Day National Conference on "Internet of Things - The Current Trend inConnected World", NCIOT-2018, pp. 46-51.

[2] S. V. Khedaskar, M. A. Rokade, B. R. Patil, and P. N. Tatwadarshi, A Survey of Image Processing and Identification Techniques, *Viva-Tech International Journal for Research and Innovation*, Vol.1, No. 1, pp. 1-10,10 October 2018.

[3] M. Cem Kasapbas and W. Elmasry, *New LSB-Based Colour ImageStestegano-graphy Method to Enhance the Efficiency in Payload Capacity, Security and Integrity Check*, Indian Academy of Sciences, 27 April 2018. https://DOI.org/10.1007/s10.12046-018-8048-4

[4] R. A. Watheq, F. Almasalha, and M. H. Qutqut, A New Steganography Technique using JPEG Images, *International Journal of Advanced Computer Science and Applications*, Vol. 9, No. 11, pp. 751-760, 2018.

[5] A. Basu, K. K. Jha, and S. Mohanty, Wide Area Networking using FrameRelay Cloud, *International Journal of Computer & Mathematical Sciences*,Vol. 4, No. 7, pp. 1-7, July 2015.

[6] G. Facciolo, N. Limare, and E. Meinhardt, Integral Images for Block Matching, *Image Processing Online*, Vol. 4, pp. 344-369,16December2014.

[7] M. Abid Ali khodher, A Proposal of Steganography Algorithm by Random Image Transformation, *Journal of AlRafidain University College*, Issue No.35, pp. 246-265, 2015.

[8] S.S.Pandey, M. P. Singh, and V. Pandey, Block Wise Image Compression & Reduced Blocks Artifacts Using Discrete Cosine Transform, *International Journal of Scientific and Research Publications*, Vol. 5, No. 3, pp. 1-10, March-2015.

[9] K. R. Barapatre, N. R. Barapatre, S. M.Lichade, and R. Lanjewar, A Performance Comparison of X.25, Frame Relay and ATM in High Speed Networks: A Review, *International Journal of Innovative Research in Computerand Communication Engineering*, Vol. 5 No. 3, March 2017.

[10] Y. J.M. Shirur, Wireless Local Area Network Frame Classification to AccessCategories based on UserPriority, *International Journal of Innovative Researchin Science, Engineering and Technology*, Vol. 7, No. 6, pp. 6966-6974, June 2018.

[11] S. K. Bandyopadhyay, A Proposed Method for Image Steganography, *Research in Medical & Engineering Sciences*, vol. 3 No. 4, pp. 253-256, 15 February 2018.doi:10.31031 /RMES. 2018.03.000569

[12] F. Morstatter, L. Wu, U. Yavanoglu, S. R. Corman, and H. Liu, IdentifyingFraming Bias in Online News, *ACM Transactions on Social Computing*, Vol. 1, No. 2, Article 5. June 2018, pp. 5:1-5:18.

[13] S.V. Wunnava, T. Marcus, R. Romer, and M. Heimer, Electronic Work Bench and PSpice Can Be Used for DesignExtensions along with the Simulations, *Fourth International Latin American and Caribbean Conference for Engineering and Technology (LACCET'2006)*, 21-23 June 2006.

[14] K. Joshi, S. Gill, and R.Yadav, A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel inthe Gray Scale Image, *Journal of Computer Networks and Communications*,Vol. 2018, pp. 1-10.

[15] M. A. Fadhil Al-Husainy, H. Abbass, A. Al-Sewadi, Full Capacity Image Steganography Using Seven-Segment Display Pattern as Secret Key, *Journal ofComputer Science*, Vol. 14, No. 6, 2018 pp. 753-763. doi:10.3844/jcssp.2018.753.763

[16] Z. K. AL-Ani, A. A. Zaidan, B.B. Zaidan, and H.O.Alanazi, Overview: MainFundamentals for Steganography, *Journal of Computing*, Vol. 2, No. 3, pp. 158-165, March 2010.

[17] H. A. Jalab, A. A. Zaidan, and B. B. Zaidan, New Design for Information Hiding with in Steganography Using Distortion Techniques, *International Journal of Engineering and Technology*, Vol. 2, No.1, pp. 72-77, February 2010.

[18] N. P. Kamdar, D. G. Kamadar, and D. N. Khandhar, Performance Evaluation ofLSB Based Steganography for Optimization of PSNR and MSE, *Journal of Information, Knowledge and Research in Electronics and Communication Engineering*, Vol.2, Issue 2, No.12, pp. 505-509, 13 Oct2013.

[19] M. Ghebleh and A. Kanso, A robust chaotic algorithm for digital image steganography, *Communications in Nonlinear Science and Numerical Simulation*, Vol. 19, pp. 1898-1907, 2014.

[20] M. R. Islam, A. Siddiqa, M. P. Uddin, A. K. Mandal, and M. D. Hossain, An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography, *2014 International Conference on Informatics, Electronics & Vision*, pp. 1-62014.

[21] F.C. Crow, Summed-area tables for texture mapping, *ACM SIGGRAPH Computer Graphics*, pp. 207,1984{212. http://dx.doi.org/10.1145/964965.808600.

[22] P. Viola and M.J. Jones, Robust real-time face detection, *International Journal of ComputerVision*, vol.57, pp. 137{154. , 2004. http://dx.doi.org/10.1023_/B:VISI.0000013087.49260.fb.

[23] Ashwak ALabaichi, Maisa'a Abid Ali K. Al-Dabbas, and Adnan Salih, Image steganography using least significant bit and secret map techniques, *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 10, No. 1, pp. 935~946, February 2020.